

**UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS**  
**UNIDADE ACADÊMICA DE GRADUAÇÃO**  
**CURSO DE DIREITO**

**PHILIPPE AUGUSTO DE MATTOS MACHADO**

**PROTEÇÃO DE DADOS PESSOAIS:**  
**Boas práticas e adequação à Lei Geral de Proteção de Dados**

**São Leopoldo**  
**2021**

PHILIPPE AUGUSTO DE MATTOS MACHADO

**PROTEÇÃO DE DADOS PESSOAIS:**

**Boas práticas e adequação à Lei Geral de Proteção de Dados**

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais, pelo Curso de Direito da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientadora: Profa. Dra. Têmis Limberger

São Leopoldo

2021

Aos meus avós, agradeço por todo o carinho, suporte e incentivo.

Aos meus pais, agradeço o incentivo, desde muito cedo, ao hábito da leitura.

A minha filha, Beatriz, eu agradeço por ser meu tudo, minha luz, meu raio de sol.

A minha esposa, Débora, agradeço por me dar o melhor presente de todos, minha “flor do dia”. Agradeço por escolher dividir a vida comigo, pelos melhores conselhos, pelos melhores momentos e pelas melhores risadas.

Agradeço a todos pela paciência e compreensão, por serem minha base e minha força, amo muito todos vocês.

## **AGRADECIMENTOS**

Primeiramente, eu gostaria de agradecer a minha mãe, por todo o carinho e dedicação, pelo suporte, por toda a paciência e compreensão, mesmo nos momentos mais difíceis. Obrigado por todos os ensinamentos e, mesmo estando longe, por sempre estar disponível para conversar, obrigado pelo incentivo e por todo o cuidado dedicado a mim e a minha filha.

Agradeço, ao meu pai, por todo o carinho e diálogo, por ter me acolhido e cuidado, desde muito cedo.

Agradeço aos meus avós por todo o incentivo, por serem meu chão e minha base e por todo o suporte nessa reta final.

Agradeço a minha esposa, Débora, pelo amor empregado, por todo carinho e dedicação, por ter me ouvido por horas e ter me dado todo o suporte necessário, por ter acreditado em mim e me incentivado a não desistir.

A minha filha, Beatriz, eu agradeço por tudo, por ser uma criança incrível e me compreender nesse momento difícil, por me tornar uma pessoa melhor, por ser a razão de todo meu esforço e do meu viver.

Agradeço aos meus amigos, aqueles que estiveram comigo nesse momento e me deram suporte e incentivo.

Agradeço ao Ariel, por toda a trajetória e parceria na faculdade e, principalmente, por ter sido a minha “orientação paralela” durante a elaboração desse trabalho.

Agradeço a todos os professores, por terem compartilhado sua experiência e saber e, principalmente, a minha orientadora, pela confiança e paciência.

Agradeço a UNISINOS, por ter me proporcionado um ambiente incrível de aprendizado e de crescimento pessoal e profissional.

Espero um dia poder retribuir, pelo menos em parte, tudo o que fizeram por mim.

*If you should go skating  
On the thin ice of modern life  
Dragging behind you the silent reproach  
Of a million tear-stained eyes  
Don't be surprised when a crack in the ice  
Appears under your feet  
You slip out of your depth and out of your mind  
With your fear flowing out behind you  
As you claw the thin ice*

*The thin ice,*  
Pink Floyd, The Wall, 1980.

## RESUMO

As tecnologias da informação têm adentrado nas diversas esferas da vida e alterado profundamente as relações sociais, impactando na forma como nos relacionamos com outros indivíduos. Assim, verificamos que a influência digital, apesar das diversas facilidades e comodidades, trouxe à tona casos cada vez mais frequentes de violações ao direito à privacidade. Nesse contexto, violações ao direito à privacidade e vazamentos de dados, dos usuários das redes, têm se tornado episódios cada vez mais corriqueiros, frente às novas tecnologias de captação, processamento e transmissão de dados. Dessa maneira, os ordenamentos jurídicos tradicionais, têm encontrado desafios cada vez mais complexos, em se aperfeiçoar e encontrar instrumentos capazes de fiscalizar e coibir a prática de ilícitos no meio virtual. Assim como, as organizações, em implementar boas práticas de governança de dados, adequadas à essa realidade digital. O presente estudo será pautado em métodos investigativos, que incluem fundamentações teóricas extraídas de artigos científicos, monografias, dissertações, teses e livros. Serão abordados conceitos e inovações trazidos pela LGPD, aplicáveis às operações de tratamento de dados. Assim, esta pesquisa busca contribuir para o debate e para compreensão do tema, acerca da necessidade de implementação de boas práticas de governança de dados e de adequação dos preceitos e práticas existentes, à luz dos fundamentos e exigências impostas pela Lei n. 13.709/2018. Compreende-se, assim, que esta abordagem é tema urgente, para todas as organizações e instituições responsáveis pelas operações de tratamento de dados pessoais. Devido às imposições e as sanções já estarem em vigor e representarem, para além dos impactos econômicos, impostos pelas sanções administrativas, grande risco à imagem e à confiabilidade das organizações, que não se adequem às exigências impostas pela LGPD. Sendo assim, primeiramente, será analisado o contexto histórico de surgimento do direito à privacidade, para além do seu conceito tradicional, de respeito à intimidade e à vida privada, ressaltando-se a necessidade do reconhecimento de um direito fundamental autônomo à proteção de dados pessoais. Em seguida, será analisada a Lei Geral de Proteção de Dados (LGPD), seus fundamentos, princípios e bases legais, relacionando-os às práticas de governança e à implementação e adequação dos princípios e conceitos

trazidos pela Lei. Assim, depreendemos que esta Lei surgiu, nesse contexto, com a finalidade de resguardar os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade das pessoas naturais, bem como, em assegurar o equilíbrio entre os direitos fundamentais dos titulares e a preocupação com o desenvolvimento econômico e tecnológico. No entanto, compreendemos que apenas a lei não é suficiente para a efetividade dos direitos dos titulares. Assim, verificou-se que as organizações devem promover o fortalecimento da cultura organizacional de proteção e de boas práticas de governança de dados, diante da constitucionalização do direito fundamental à proteção de dados e das imposições relativas à LGPD. Dessa maneira, constatamos a importância de que as empresas tenham uma política interna e externa bem definidas, de proteção das informações sensíveis, por meio da adoção de medidas preventivas e de mitigação dos riscos e de boas práticas, que transbordem a todos os níveis organizacionais.

**Palavras-chave:** proteção; dados pessoais; tratamento de dados; boas-práticas; governança, adequação; LGPD;

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>9</b>
<b>2. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS .....</b>	<b>14</b>
2.1. Contextualização, fundamentos legais e históricos acerca do Direito à Privacidade e à Proteção de Dados Pessoais .....	14
2.2. Privacidade e proteção de dados .....	18
2.2.1. O sistema europeu de proteção de dados pessoais .....	27
2.3. Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709/2018 e seus fundamentos.....	36
2.3.1. O respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem, o direito à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião .....	37
2.3.2. O direito ao desenvolvimento econômico e tecnológico e à inovação, à livre iniciativa, à livre concorrência e a defesa do consumidor.....	39
2.3.3. Os direitos humanos, como o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, a liberdade de expressão, de informação, de comunicação e de opinião .....	40
<b>3. GOVERNANÇA E TRATAMENTO DE DADOS PESSOAIS .....</b>	<b>41</b>
3.1. Objetivos e aplicabilidade da LGPD .....	42
3.1.1. Conceitos .....	45
3.1.1.1. Dados pessoais e dados pessoais sensíveis .....	45
3.1.1.2 Tratamento de dados pessoais e de dados pessoais sensíveis .....	47
3.1.1.3 Tratamento de dados pessoais de crianças e adolescentes.....	50
3.1.1.4 Tratamento de dados pelo poder público .....	51
3.2. Princípios aplicáveis às operações de tratamento de dados.....	52
3.2.1. Princípio da Finalidade, da Adequação, da Necessidade e da Prevenção .....	53
3.2.2. Princípio do livre acesso, da transparência, da segurança e da qualidade dos dados .....	57
3.2.3. Da não-discriminação e da prestação de contas ( <i>accountability</i> ).....	60
3.2.4 Consentimento e o legítimo interesse.....	62
3.3. Agentes de tratamento de dados pessoais.....	68

3.3.1. Controlador e operador .....	69
3.3.2. Encarregado (DPO) .....	71
4. ADEQUAÇÃO, RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS.....	72
4.1. Adequação <i>das operações de tratamento</i> à LGPD .....	73
4.2. Direitos dos titulares de dados .....	78
4.2.1. Direito à titularidade dos dados pessoais, à confirmação de existência de tratamento, de acesso aos dados e de requerer a correção de dados incompletos, inexatos ou desatualizados.....	78
4.2.2. Direito à anonimização, bloqueio ou eliminação dos dados.....	81
4.2.3. Direito de petição, de oposição e à revisão das decisões tomadas unicamente com base em tratamento automatizado de dados.....	82
4.2.4. Direito à portabilidade dos dados, a revogar o consentimento, a ser informado sobre a possibilidade de não consentir.....	83
4.3. Autoridade Nacional, responsabilidade e sanções na LGPD.....	84
4.3.1. Autoridade Nacional de Proteção de Dados (ANPD) e estrutura regulatória.....	84
4.3.2. Incidentes em segurança e prestação de contas ( <i>accountability</i> ).....	91
5 CONSIDERAÇÕES FINAIS .....	97
REFERÊNCIAS.....	102

## 1 INTRODUÇÃO

O presente estudo será pautado em métodos investigativos, que incluem fundamentações teóricas extraídas de artigos científicos, monografias, dissertações e teses. Assim como, entendimentos doutrinários extraídos de livros que tratem sobre a temática, articulando a teoria com a análise dos processos de evolução dos conceitos abordados e, consubstanciando, a análise histórica com a realidade empírica, por meio de reflexões acerca das perspectivas e desafios enfrentados pelo tema em análise na atualidade. Devido à necessária interdisciplinaridade na pesquisa jurídica, será utilizado, preponderantemente, a pesquisa por meio de ampla revisão bibliográfica sobre o tema e análise histórica dos fenômenos sociais advindos com a transformação digital da sociedade, a fim de contribuir com o debate doutrinário sobre a temática.

Dessa forma, devido à complexidade do tema pesquisado e da interdisciplinaridade que assume no contexto atual, é necessário que a pesquisa jurídica utilize métodos de abordagem e métodos de procedimentos sistemáticos que considere os fenômenos sociais correlatos. Sendo assim, a fim de se obter o resultado pretendido, qual seja, de investigação das implicações jurídicas advindos com a transformação digital da sociedade e das suas consequências práticas, será utilizado um método dedutivo, de análise dos fenômenos estudados por meio dos estudos sobre a disciplina.

Isto posto, verifica-se que com a globalização e os processos de transformação do mundo físico em mundo digital, novos modelos de negócios têm sido viabilizados em face dos avanços tecnológicos e as tecnologias da informação têm adentrado, cada vez, as mais diversas áreas da vida cotidiana e alterado profundamente as relações sociais, de trabalho, de consumo etc. Devido a isso, violações ao direito à privacidade e vazamentos de dados dos usuários das redes têm se tornado episódios cada vez mais corriqueiros. Uma vez que, as novas tecnologias de captação, processamento e transmissão de dados trouxeram à luz a urgência de uma necessária regulamentação por parte dos ordenamentos jurídicos. Assim como, do aperfeiçoamento de instrumentos capazes de fiscalizar as práticas de ilícitos, ou seja, das instituições criarem meios capazes de coibir as práticas e punir os responsáveis.

Dessa maneira, este trabalho objetiva demonstrar a necessidade da inserção da temática, sobre a Proteção de Dados, como objeto das já existentes e consolidadas políticas de adequação organizacional e dos programas de *compliance* (adequação). Nesse sentido, primeiramente, será realizada uma análise dos movimentos históricos e algumas mudanças ocorridas no último século. Bem como, a análise de alguns conceitos e fundamentos importantes à disciplina que trata da proteção dos dados pessoais propriamente dita e sua distinção, para além das concepções tradicionais de direito à privacidade e à vida privada. Assim, a fim de analisar essa nova realidade social, este trabalho fará uma breve análise do reconhecimento de um direito fundamental autônomo à proteção de dados pessoais, a fim compreender como os avanços tecnológicos e a transformação digital têm impactado em sua proteção e regulamentação.

Em vista disso, verifica-se que, ao redor do mundo, surgem legislações que buscam conferir maior proteção do titular de dados, diante das novas tecnologias de captação, processamento e transmissão de dados. Nesse sentido, cita-se o Regulamento Europeu (RGPD), aprovado em 2016, e a Legislação do Estado da Califórnia, nos Estados Unidos da América, aprovado em 2018, como marcos normativos relevantes em âmbito internacional. Diante desse movimento internacional, em maio de 2018, foi promulgada, no Brasil, a Lei Geral de Proteção de Dados – Lei n. 13.709, que dispõe sobre o tratamento de dados pessoais de pessoas naturais, coletado em território nacional.

Diante disso, esta pesquisa teve como intuito contribuir para o debate e para compreensão do tema, sobre a necessidade de implementação de boas práticas de governança de dados pessoais e de adequação, dos preceitos e práticas já existentes, à luz dos fundamentos e exigências impostas pela Lei n. 13.709/2018. Além disso, objetivou-se compreender os desafios impostos pelas novas tecnologias e as inovações trazidas pela LGPD. Dessa forma, foram analisados seus fundamentos, princípios e bases legais. Assim como, a sua estrutura regulatória e outros elementos capazes de contribuir para a implementação e/ou adequação das já existentes práticas em segurança da informação.

Assim, finalmente, serão analisadas novidades trazidas pela LGPD, seus conceitos relacionando-os com as boas práticas de governança de dados e adequação às normas protetivas de dados pessoais. Nesse sentido, os agentes

de tratamento, o controlador e o operador, responsáveis pelo tratamento de dados pessoais nas organizações, devem ter vista a observância a padrões éticos e probos de conduta, sob pena de sofrer as sanções administrativas impostas pela Lei, que estão em vigor desde 1º de agosto de 2021.

Para atingir essa finalidade, serão analisadas as legislações e regulamentações que envolvam o tema pesquisado e o seu processo histórico de consolidação e transformação, identificar práticas existentes e consolidadas, aptas a lidar com a nova realidade digital e analisar os desafios e novidades impostas pela nova legislação, que possam contribuir na implementação de um sistema eficiente de governança em privacidade, por meio da estrita observância às normas técnicas de segurança da informação e das legislações sobre proteção de dados.

A justificativa acadêmica dessa pesquisa reside na importância que a proteção de dados adquiriu nos últimos anos e tem como finalidade contribuir no debate sobre a necessidade da promoção de uma cultura organizacional de boas práticas de governança de dados, nesse contexto de transformação digital, por regulamentos internacionais de proteção de dados e normas e padrões éticos de conduta e de segurança informacional.

Dessa maneira, é possível afirmar que o Regulamento Geral sobre Proteção de Dados da União Europeia e outras legislações, não menos importantes, contribuem para uma cultura global de reconhecimento do direito à proteção de dados e influenciam diretamente no surgimento de legislações sobre o tema ao redor do mundo, que culminaram com o surgimento, no ordenamento jurídico brasileiro, na Lei Geral de Proteção de Dados, Lei n. 13.709, de abril de 2018 (LGPD). Esta pesquisa busca contribuir para o debate e para compreensão do tema, acerca da necessidade de implementação de boas práticas e da adequação dos preceitos e práticas existentes, à luz dos fundamentos e exigências impostas pela Lei n. 13.709/2018. Assim como, dos desafios impostos pelas novas tecnologias de captação, processamento e transmissão de dados. Assim, compreende-se que, a abordagem deste assunto, é tema urgente para todas as organizações, entidades jurídicas de direito público e privado, responsáveis pelas operações de tratamento de dados pessoais. Considerando que às imposições e as sanções já estão em vigor e representam, para além dos impactos econômicos impostos pelas sanções

administrativas, grande risco à imagem das organizações que não se adequarem às exigências impostas pela Lei.

Assim, este trabalho se propôs a analisar o reconhecimento do direito à proteção de dados pessoais, como um direito fundamental autônomo e sua necessária constitucionalização. Nesse contexto, verificou-se que o reconhecimento da existência de direito fundamental à proteção de dados está intrinsecamente relacionado ao princípio da dignidade humana, na medida em que as informações representam uma extensão da personalidade dos indivíduos, ao exprimirem hábitos e predileções precisas do comportamento. Sendo assim, o reconhecimento de um direito fundamental autônomo à proteção de dados, não como uma mera decorrência do direito à privacidade e do resguardo à intimidade e à vida privada, é de extrema relevância para a sua plena concretização.

Nesse sentido, verificamos que o STF reconheceu a importância do tema, em recente julgado, implementando um novo paradigma à tutela constitucional deste direito fundamental, ao trazer um conceito ampliado de dado pessoal. e fazer a diferenciação da esfera da proteção de dados, dos conceitos tradicionais de privacidade e vida privada. Além do mais, a preocupação legislativa com o tema demonstrou um viés mais protecionista com a aprovação da Proposta de Emenda à Constituição n. 17/2019, em 20 de outubro de 2021. Desse modo, após a promulgação da PEC n. 17/2019, a disciplina acerca da proteção de dados adquirirá novos contornos, ao incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, previstos no art. 5º da Constituição.

Além disso, observou-se que os ordenamentos jurídicos tradicionais, os operadores do direito, os órgãos de fiscalização e regulamentação, as organizações de direito público e privado e diversos setores da sociedade enfrentam grandes dificuldades em avaliar os efeitos da utilização das novas tecnologias, frente a todo um universo amplo, complexo e dinâmico experimentados na *internet*. Diante da sua imprevisibilidade e rápida transformação, o direito e a sociedade precisam se atualizar e se reinventar na mesma medida e velocidade experimentadas no ciberespaço.

Nesse sentido, compreendemos que o Regulamento Europeu implicou em efeitos relativos à proteção de dados que ultrapassaram os limites da União Europeia, por meio do estabelecimento de parâmetros de proteção a serem observados por todos os países que cogitem estabelecer relações comerciais com

o bloco europeu.

Assim, depreendemos que a Lei Geral de Proteção de Dados surgiu, nesse contexto, com a finalidade de resguardar os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade das pessoas naturais, bem como, em assegurar o equilíbrio entre os direitos fundamentais dos titulares e a preocupação com o desenvolvimento econômico e tecnológico.

No entanto, compreende-se que apenas a lei não é suficiente para a efetividade dos direitos dos titulares, assim, verificou-se que as organizações devem promover o fortalecimento da cultura organizacional de proteção e de boas práticas de governança de dados. Assim, diante da constitucionalização do direito fundamental à proteção de dados, compreendemos a importância de que as empresas tenham uma política interna bem definida, de proteção das informações sensíveis, por meio da adoção de medidas preventivas e de mitigação dos riscos e de boas práticas que transbordem a todos os níveis organizacionais.

Sendo assim, compreendemos que a organização deve promover práticas pautadas em princípios éticos e probos, em estrita observância às boas práticas em governança de dados e segurança da informação, as quais devem ser atualizadas constantemente, diante de novos regulamentos, normas e padrões técnicos disponíveis e adequados. Além do mais, importa às organizações oferecer treinamento e aperfeiçoamento qualificados ao seu quadro funcional, conforme as normas e os procedimentos mais adequados à complexidade e ao risco das operações. Assim, ressaltamos que as organizações que já possuam, em suas operações técnicas, a promoção de boas práticas de governança em privacidade e uma cultura organizacional protetiva das informações dos clientes, terão menos dificuldades em se adequarem às novas legislações a respeito do tema.

Nesse sentido, verificamos a adoção de procedimentos técnicos já existentes e de normas técnicas setoriais, como aquelas da família ISO 27000, normas técnicas procedimentais que adotam padrões internacionais em segurança da informação. Especificamente a norma ISO 27701, alinhada como as inovações trazidas pela LGPD e o Regulamento Europeu. Portanto, é possível afirmar que, ao adotar ferramentas eficazes e promover uma cultura de proteção de dados, as organizações estarão um passo à frente em atender às necessidades de adequação impostas pela LGPD, resultando em maior confiabilidade e

competitividade.

Compreendemos, assim, que a adequação digital é capaz de reduzir as dificuldades impostas e a sobrecarga de trabalho por parte dos agentes de tratamento. Ao promover um ambiente mais simplificado e eficaz. Sendo assim, ressalta-se que as consequências da não adequação podem ocasionar danos, não apenas de cunho pecuniário, mas também, à imagem da organização, por meio da perda de confiabilidade, de clientes e de oportunidades de negócio. Dessa maneira, compreendemos que, a médio e longo prazo, a adequação empresarial e organizacional, tende a trazer inúmeros benefícios às organizações, ao conferir maior confiabilidade e segurança jurídica aos titulares de dados, assim como, da simplificação dos procedimentos de conformidade, resultando, assim, em maior competitividade e confiança à organização.

## **2. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS**

### **2.1. Contextualização, fundamentos legais e históricos acerca do Direito à Privacidade e à Proteção de Dados Pessoais**

Primeiramente, antes de se aprofundar no objeto desta pesquisa, compreendemos que cabe a análise de alguns termos e conceitos. Os quais, serão fundamentais para o entendimento acerca do fenômeno referente à proteção de dados e à privacidade no meio digital. Nesse sentido, verificamos que a compreensão dos direitos fundamentais e a sua importância para o ordenamento jurídico, parte do reconhecimento do princípio da dignidade da pessoa humana, conceito jus filosófico, que decorre da própria condição humana, como um fundamento do estado democrático de direito. Conforme preleciona Andrade<sup>1</sup> “No centro do direito encontra-se o ser humano.” Dessa maneira, é possível afirmar que o fundamento do direito e de todo o ordenamento jurídico é o homem e as suas relações estabelecidas em sociedade. Além do mais, o autor afirma o seguinte “Um indivíduo, pelo só fato de integrar o gênero humano, já é detentor de

---

<sup>1</sup>ANDRADE, André Gustavo Corrêa de. O princípio fundamental da dignidade humana em sua concretização judicial. *In*: Tribunal de Justiça do Rio de Janeiro, Rio de Janeiro, 2004. Disponível em: [http://www.tjrj.jus.br/c/document\\_library/get\\_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe](http://www.tjrj.jus.br/c/document_library/get_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe). Acesso em: 29 out de 2021

dignidade.”<sup>2</sup>

Cumpra salientar que, a Constituição Federal da República Federativa do Brasil, de 1988, representa a lei máxima do ordenamento jurídico brasileiro ao traçar os parâmetros a serem observados por todo o sistema de normas infraconstitucionais. Dessa maneira, em seu artigo 1º, inciso III, estabelece-se, entre um dos fundamentos, da República Federativa do Brasil e do Estado Democrático de Direito, o reconhecimento da dignidade da pessoa humana como um dos princípios fundamentais para o estabelecimento da ordem social e democrática.

Dessa forma, compreendemos que o reconhecimento de um direito fundamental à proteção de dados, está intrinsecamente relacionado ao princípio da dignidade humana, nessa toada, Sarlet<sup>3</sup> preceitua o seguinte:

As conexões entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção dos dados pessoais são intensas, embora nem sempre compreendidas do mesmo modo no âmbito das diferentes ordens jurídicas. Os dois principais pontos de contato, todavia, são o princípio autonômico (autodeterminação) e os direitos de personalidade, representados aqui, por sua vez, pelo direito (de natureza geral) ao livre desenvolvimento da personalidade e os direitos especiais à privacidade e à autodeterminação informativa, igualmente conectados entre si, mas que não esgotam o leque de alternativas.<sup>3</sup>

Além do mais, o autor afirma o seguinte:

[...]no caso do direito à proteção dos dados pessoais, o princípio da dignidade da pessoa humana pode e deve ser acionado, seja para a justificação da fundamentalidade daquele direito, seja para a determinação de parte de seu conteúdo, com destaque para a identificação de alguns pontos de contato com outros princípios e direitos fundamentais.<sup>4</sup>

Assim, o reconhecimento, na ordem constitucional, dos direitos e garantias fundamentais e a limitação do poder estatal estão entre os elementos que

---

<sup>2</sup>ANDRADE, André Gustavo Corrêa de. O princípio fundamental da dignidade humana em sua concretização judicial. *In*: Tribunal de Justiça do Rio de Janeiro, Rio de Janeiro, 2004. Disponível em: [http://www.tjrj.jus.br/c/document\\_library/get\\_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe](http://www.tjrj.jus.br/c/document_library/get_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe). Acesso em: 29 out de 2021

<sup>3</sup>SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021;

<sup>4</sup>SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021;

fundamentam toda a ordem democrática e o Estado de Direito. Nesse contexto, depreendemos que a evolução histórica dos direitos fundamentais está intrinsecamente relacionada aos diferentes momentos históricos e aos anseios de determinada sociedade em determinado tempo. Nesse sentido, Mendes e Branco<sup>5</sup> afirmam que, a distinção entre gerações de direitos é estabelecida com a finalidade de situar os diferentes momentos em determinados grupos de direitos surgiram, como anseios sociais relevantes, acolhidos pela ordem jurídica. Assim, referente às gerações de direitos fundamentais, Pinho afirma o seguinte “a sucessão de gerações não significa dizer que os direitos previstos num momento tenham sido suplantados por aqueles surgidos em instante seguinte.”<sup>6</sup>

Assim, verifica-se que os direitos fundamentais estão relacionados às seguintes características gerais, quais sejam: I) a historicidade: pois são produtos da evolução histórica e das sucessivas conquistas de determinadas sociedades, em determinado contexto histórico-cultural; II) a sua inalienabilidade: uma vez que são inerentes à condição humana e, portanto, como atributos inatos, são intransferíveis e inegociáveis; III) a sua imprescritibilidade: o que significa dizer que a pretensão, de respeito e estrita observância, aos seus preceitos e da sua concretização não se esgota com o decurso do tempo; IV) a sua irrenunciabilidade: novamente, em vista de atributo inato à condição humana, não podem ser renunciado por nenhum ser humano; V) a sua universalidade: da mesma maneira, dizem respeito a uma categorias de direitos advindo e referente à condição humana, motivo pelo qual englobam a todos os indivíduos, sem exceções, pertencentes à espécie humana, independentemente da sua nacionalidade, da sua raça, do seu gênero biológico, de sua orientação política, sexual, religiosa ou filosófica; VI) a sua relatividade: compreendemos que nenhum direito fundamental é absoluto, no que diz respeito possibilidades de sofrerem limitações ou mitigações, diante da colisão com outros direitos fundamentais como, por exemplo, o interesse público ou do direito individual de outros seres da espécie humana.

Além do mais, no que se refere à eficácia dos direitos fundamentais, sua

---

<sup>5</sup>MENDES, Gilmar Ferreira; BRANCO, Paulo Gonet. Série IDP - Linha Doutrina - Curso de direito constitucional. São Paulo: Editora Saraiva, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553618088/>. Acesso em: 09 jun. 2021

<sup>6</sup>PINHO, Rodrigo Cesar Rebello. Sinopses Jurídicas v 17 - direito constitucional - teoria geral da constituição e direitos fundamentais. São Paulo: Editora Saraiva, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553619627/>. Acesso em: 12 jun. 2021;

compreensão perpassa pelo reconhecimento dos seus sentidos, quais sejam, o subjetivo e o objetivo. Nesse contexto, sua dimensão subjetiva refere-se à capacidade dos indivíduos, titulares do direito, de exigirem a sua concretização ou, ainda, a abstenção por parte do poder estatal. Na sua dimensão objetiva, diz respeito ao modo de cumprimento pelo poder estatal e aos limites impostos pela ordem constitucional à atuação estatal.

Em vista disso, verifica-se que as revoluções liberais, movimento político-social da segunda metade do século XVIII, que foi responsável pelo surgimento das democracias modernas. Nesse contexto, a Revolução Americana, em 1776, desencadeou a declaração de independência dos Estados Unidos da América, pautada em ideias de liberdades individuais e abstenção e intervenção mínima do Poder Estatal na esfera individual. Além do mais, podemos citar a Revolução Francesa, em 1799, que pôs fim ao regime absolutista naquele país, fundada em ideais iluministas de “Liberdade, Igualdade e Fraternidade” (*Liberté, Egalité, Fraternité*). Assim, compreendemos que suas conquistas impulsionaram ideais de liberdade em todo o mundo ocidental, com fundamento na limitação do poder estatal, o respeito à liberdade e aos direitos de prestações negativas, ou seja, um direito de não interferência estatal na esfera individual e na vida particular.<sup>78</sup>

Embora tenham representado de forma efetiva, naquele momento, a defesa da dignidade humana, dos direitos de liberdade e de defesa da privacidade, por meio da abstenção estatal na vida privada, as constituições de cunho liberal tornaram-se insuficientes, frente às desigualdades sociais advindas no contexto de pós-guerra. Dessa maneira, devido aos fortes anseios sociais, surgiram as primeiras constituições sociais, a saber, a Constituição de Weimar, de 1919 e a Constituição do México, de 1917. As quais trouxeram, em seu bojo, conceitos inéditos de prestação positiva por parte do estado, ou seja, de imposição à intervenção estatal na ordem econômica e social, a fim de garantir condições mínimas existenciais aos cidadãos, pautada em princípios de justiça social, pela prestação do direito à saúde, à educação, ao trabalho, à previdência social dentre outros direitos.<sup>8</sup>

---

<sup>7</sup>COMPARATO, Fábio Konder. A afirmação histórica dos direitos humanos. 11. ed. São Paulo: Editora Saraiva, 2017. p. 111.

<sup>8</sup>MENDES, Gilmar Ferreira; BRANCO, Paulo Gonet. Série IDP - Linha Doutrina - Curso de direito constitucional. São Paulo: Editora Saraiva, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553618088/>. Acesso em: 09 jun. 2021

Desse modo, compreendemos que o surgimento de novos direitos está intrinsecamente relacionado aos novos anseios sociais, à evolução da sociedade e aos desafios impostos pela ordem social. Neste contexto, as novas tecnologias e os seus impactos, principalmente, a partir da segunda metade do século XX, causam profundas transformações na sociedade em velocidade e intensidade inimagináveis anteriormente. Em vista disso, o avanço tecnológico experimentado no último século, acentuado pelo progressivo desenvolvimento da informática, exprimem novos desafios aos ordenamentos jurídicos de todo o mundo e a toda a ordem social. Nesse contexto, surgem novos anseios sociais relacionados à tutela e à promoção da dignidade humana, ao direito de acesso à informação, à proteção da privacidade, ao resguardo à intimidade e à vida privada e à proteção dos dados pessoais dos usuários das complexas redes de comunicação estabelecidas no ciberespaço.

## 2.2. Privacidade e proteção de dados

O surgimento do conceito tradicional de privacidade, em um primeiro momento, no século XIX, estava relacionado ao desenvolvimento da imprensa, ao surgimento de meios de transporte mais eficientes e aos problemas relacionados à violação da privacidade e à difamação realizadas pelos veículos de imprensa e as suas inferências na vida privada da classe política. Nesse sentido, é amplamente referenciado, nos estudos sobre privacidade, a origem do seu conceito tradicional relacionada à publicação do artigo intitulado *Right to privacy*, em 1890, por Samuel Warren e Louis Brandeis. Estes estudos analisaram precedentes judiciais da Suprema Corte norte-americana, no que se refere à propriedade, aos direitos autorais e à difamação realizada por veículos de imprensa. Dessa maneira, diante da sua preocupação com a divulgação de informações referentes à vida privada e às novas tecnologias da imprensa, aduziram o chamado “direito de estar só” (*right to be alone*).<sup>91</sup>

No entanto, a partir da segunda metade do século XX e, com maior

---

<sup>91</sup>VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito, Estado e Sociedade: Políticas Públicas e Democracia), Universidade Nacional de Brasília (UNB). Brasília, 2007. Disponível em: [https://repositorio.unb.br/bitstream/10482/3358/1/2007\\_TatianaMaltaVieira.pdf](https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf). Acesso em: 09 jun. 2021.

intensidade e dimensão, a partir das primeiras décadas do século XXI, novas ameaças nas redes e violações ao direito fundamental à privacidade tornam-se cada vez mais frequentes, com o uso globalizado da *internet*, com o desenvolvimento de computadores de alta performance, com o aprimoramento de tecnologias da informação e com o aumento da capacidade de processamento e transmissão de dados. Sendo assim, o debate, quanto à importância da proteção de dados dos usuários da rede, adquiriu contornos mais complexos e urgentes, para além dos tradicionais conceitos de privacidade e as suas garantias negativas, de não interferência estatal na privacidade, na vida privada e ao sigilo das comunicações<sup>11</sup>.

Além do mais, nas últimas décadas, têm-se fomentado ampla discussão na sociedade em geral, na jurisprudência e na doutrina constitucional, quanto à imprescindibilidade de não apenas reconhecer o direito à proteção de dados como um direito fundamental autônomo, mas sim, como protegê-los e garantir sua efetividade, em face das constantes e aceleradas mudanças tecnológicas. Dessa forma, verificamos que o conceito tradicional de privacidade sofreu profundas transformações, diante das novas tecnologias da informação e dos meios de transmissão da informação, em face das complexas redes de informação estabelecidas na *internet*, que permitem um fluxo de dados<sup>1012</sup> de maneira muito mais eficiente e dinâmica. Embora essas inovações tecnológicas possibilitem novas formas de se relacionar, consumir, vender e se comunicar, em contrapartida, representam inúmeros desafios à regulamentação e ao controle, por parte dos ordenamentos jurídicos tradicionais. Dessa maneira, proporcionam grande insegurança aos usuários nas redes e, ainda, de princípios e fundamentos relacionados à própria higidez do Estado Democrático de Direito.<sup>11</sup>

---

<sup>10</sup>Nesse contexto, fluxo de dados refere-se ao seguinte: “à operação de correlação lógica acerca do trânsito dos dados em programas e hardwares presentes nos sistemas de um agente de tratamento. O processo de determinação do fluxo de dados geralmente engloba as transformações às quais os dados estão sujeitos, bem como a definição de quem tem acesso aos mesmos, onde estão armazenados e o que é feito. Relaciona-se ao ciclo de vida dos dados. Assim, uma instituição, por exemplo, pode apresentar, por meio de um diagrama de fluxo de dados, como certo dado é coletado por um software, como o dado é tratado e refinado junto a outro software em conjunto com um hardware e como este dado é armazenado nas bases de servidores da instituição.” Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getúlio Vargas - São Paulo: CEPI-FGV Direito SP, 2021.

<sup>11</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021

Nesse sentido, Sarlet<sup>14</sup> afirma que, a dinamicidade e a complexidade das relações estabelecidas no meio digital põem à prova a capacidade, dos ordenamentos jurídicos tradicionais, em lidar com os impactos causados pelos avanços tecnológicos na sociedade. Ressalta que, os ordenamentos jurídicos enfrentam grandes dificuldades em avaliar os efeitos da utilização das novas tecnologias, diante da sua imprevisibilidade e rápida transformação, uma vez que compreendem um universo amplo e complexo<sup>12</sup> Assim, é possível afirmar que a dinamicidade e complexidade das relações estabelecidas no meio digital representam verdadeiros desafios aos operadores do direito, aos órgãos de regulamentação e de fiscalização e à sociedade em geral, que precisam se atualizar e se reinventar na mesma medida e velocidade experimentadas nesse meio.

Além do mais, as novas tecnologias de captação, processamento, armazenamento e transmissão de dados pessoais, como o *Big Data*<sup>13</sup>, põem à prova a capacidade dos sistemas jurídicos de garantir a proteção da privacidade e da intimidade dos usuários nas redes e de assegurar a proteção dos seus dados pessoais. Assim, torna-se urgente a necessidade de aperfeiçoamento e utilização de instrumentos jurídicos capazes de fiscalizar o uso de dados pessoais, bem com apontar e investigar casos de violação do direito à privacidade na *internet*, diante do uso indevido das informações pessoais dos usuários.

Assim, com o uso de tecnologias da informação, sobretudo a partir do surgimento das redes sociais e do aumento exponencial da auto exposição individual, os escândalos de vazamento de dados pessoais e de violação do direito à privacidade têm se tornado cada vez mais corriqueiros. Podemos citar, como exemplo, a captação e compartilhamento, de informações de cunho pessoal, dos dados de mais de 50 (cinquenta) milhões de usuários do *Facebook*, promovido pela *Cambridge Analytica* para fins manipulação eleitorais e de opinião política, nas eleições norte-americanas de 2016. Ressalta-se que, este é um fato notório, amplamente divulgado, em março de 2018, por veículos de mídia

---

<sup>12</sup>SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: Tratado de proteção de dados pessoais/coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021

<sup>13</sup>Pode-se conceituar Big Data como “ativos de informação de alto volume, alta velocidade e alta variedade que exigem formas inovadoras e econômicas de processamento de informações para uma melhor percepção e tomada de decisão.” Tradução nossa: In *Gartner Glossary. Big Data*: Disponível em: <http://www.gartner.com/it-glossary/big-data>. Acesso em: 03 nov. 2021

tradicional, como o *The New York Times*<sup>14</sup> e o *The Guardian*<sup>15</sup>.

O direito à autodeterminação, das informações pessoais, diz respeito ao atributo inato do ser humano em decidir sobre sua vida particular e, por conseguinte, aos dados que dizem respeito à sua personalidade, hábitos e predileções, os quais podem ser utilizados indiscriminadamente como moeda de troca, com a finalidade de traçar perfis de consumo e comportamentais<sup>16</sup>. Assim, o direito à autodeterminação informativa, conforme refere Peixoto e Erhardt<sup>17</sup>, se relacionam com a dimensão informacional, na medida em que o modo de viver de uma pessoa pode ser exprimido em dados, que representam uma extensão da sua personalidade, que deve ser protegida contra divulgações indevidas ou não autorizadas. Dessa maneira, referem que:

A proteção da privacidade em sua dimensão decisional tem um ponto de encontro com a dimensão informacional. Muitos dos assuntos que dizem respeito ao modo de viver da pessoa acabam virando dados, os chamados dados sensíveis, cuja proteção é uma das principais preocupações na chamada sociedade da informação.<sup>18</sup>

Nesse sentido, Sarlet afirma, no que tange à autodeterminação informativa, o seguinte:

[...]direito à autodeterminação informativa, ou seja, o direito de cada indivíduo poder controlar e determinar (ainda não de modo absoluto) o acesso e o uso de seus dados pessoais. Da mesma forma, quando se trata de fiscalizar a legitimidade de restrições ao direito à proteção

<sup>14</sup>GRANVILLE, Kevin. Facebook and Cambridge Analytica: What You Need to Know as Fallout Widen. *In* NY Times. Nova Iorque, 2018. Disponível em: <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>. Acesso em: 03 nov. 2021.

<sup>15</sup>*Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. In The Guardian*, Londres, 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 03 nov. 2021.

<sup>16</sup>Perfilamento ou profiling implica o tratamento de dados pessoais com a finalidade de traçar perfil dos titulares de dados, envolvendo operações como cruzamento, agregação e enriquecimento de bases de dados. Nesse sentido, cita-se, por exemplo, os *cookies*, que por meio do armazenamento de dados de navegação gera publicidade a partir das predileções de navegação dos usuários das redes. Adaptado de: Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo: CEPI-FGV Direito SP, 2021;

<sup>17</sup>PEIXOTO, Erick Lucena Campos; ERHARDT JÚNIOR, Marcos. Os Desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. *Revista Jurídica Luso-Brasileira*. Ano 6, 2020. n. 2. Disponível em: [https://www.cidp.pt/revistas/rjlb/2020/2/2020\\_02\\_0389\\_0418.pdf](https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf). Acesso em: 13 jun 2021;

<sup>18</sup>Idem;

de dados, o manejo do instituto da ponderação e respectivas técnicas, como é o caso dos critérios da proporcionalidade.<sup>19</sup>

Para fins de compreensão do conceito, cumpre salientar que o direito à autodeterminação informativa teve seu marco jurisprudencial em decisão do Tribunal Constitucional Federal da Alemanha ocidental, em 1983, no caso da Lei do Censo. No qual, declarou-se inconstitucional uma lei que havia determinado o recenseamento da população, para fins de coletar e realizar o processamento de dados pessoais dos usuários. Assim como, este instrumento normativo previa a possibilidade de comparação, dos dados levantados, com registros públicos pré-existentes e, ainda, sua transmissão a repartições públicas, sob a justificativa de otimização das políticas públicas<sup>20</sup>.

Além disso, quanto à decisão do Tribunal Constitucional Federal da Alemanha ocidental, Sarlet, ressalta o seguinte:

[...] o Tribunal Constitucional, contudo, não reconheceu diretamente um direito fundamental à proteção de dados pessoais, mas, deduziu, numa leitura conjugada do princípio da dignidade da pessoa humana e do direito ao livre desenvolvimento da personalidade, um direito fundamental implícito à autodeterminação informativa, que, consiste, em suma e de acordo com o Tribunal, na prerrogativa de cada indivíduo decidir, em princípio e substancialmente, sobre a divulgação e a utilização de seus dados pessoais<sup>21</sup>.

Ademais, em decisão paradigmática que reconheceu, no ordenamento jurídico brasileiro, em 7 de maio de 2020, o direito à proteção de dados pessoais como um direito fundamental autônomo, podemos citar o julgamento, no Supremo Tribunal Federal do Brasil, da Ação Direta de Inconstitucionalidade n. 6387, que suspendeu a eficácia da Medida Provisória n. 954. Referimos que, esta Medida Provisória, determinava que “empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas

---

<sup>19</sup>SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: Tratado de proteção de dados pessoais/coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021;

<sup>20</sup>Idem;

<sup>21</sup>Idem;

físicas ou jurídicas.”, para fins de produção estatística oficial, por meio de entrevistas não presenciais.<sup>22</sup>

Diante disso, cinco Ações Diretas de Inconstitucionalidade foram ajuizadas sob o argumento de que o texto apresentava contrariedades com preceitos da CF/88 e grave violação a direitos e garantias fundamentais, como a autodeterminação informativa, a dignidade humana, a inviolabilidade da intimidade e da vida privada<sup>23</sup>. Dessa maneira, dentre outros argumentos utilizados no relatório da ilustre Ministra Rosa Weber, chama a atenção o conceito de “dado pessoal” e de sua tutela constitucional de modo ampliado<sup>24</sup>, nos seguintes termos:

O art. 2.º da MP n. 954/2020 impõe às empresas prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas. Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5.º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5.º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

(...)

Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2.º, I e II, da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.”<sup>9</sup>

(BRASIL, Supremo Tribunal Federal. ADI n. 6387. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24.04.2020, DJe 28.04.2020, p. 8.)<sup>25</sup>

Dessa maneira, conforme entendimento de Mendes, Rodrigues Junior e Fonseca<sup>26</sup>, o STF reconheceu a proteção de dados pessoais, sob a tutela

<sup>22</sup>MENDES Laura Schertel. RODRIGUES JUNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.].* – Rio de Janeiro: Forense, 2021;

<sup>23</sup> Idem;

<sup>24</sup>MENDES Laura Schertel. RODRIGUES JUNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.].* – Rio de Janeiro: Forense, 2021;

<sup>25</sup>BRASIL, Supremo Tribunal Federal. ADI n. 6387. Rel. Min. Rosa Weber, Decisão Monocrática, julgado em 24.04.2020, DJe 28.04.2020, p. 8.;

<sup>26</sup>MENDES Laura Schertel. RODRIGUES JUNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito

constitucional, ao trazer um conceito ampliado de dado pessoal e fazer a sua diferenciação entre os conceitos tradicionais de privacidade e vida privada, da esfera da proteção de dados. Assim, compreende-se que esta decisão representa um passo importante no reconhecimento de um direito autônomo à proteção de dados<sup>27</sup>. Nesse sentido, afirmam que:

A decisão do STF é histórica porque, pela primeira vez, encontrou-se consenso considerável em torno de um conceito amplo de dado pessoal e, por consequência, sobre sua necessária tutela constitucional para além dos ditos dados íntimos. Com isso, a autonomia do direito fundamental à proteção de dados pessoais, também designado por alguns ministros como o direito à autodeterminação informativa, permite que se formule uma diferenciação entre a inviolabilidade da intimidade e da vida privada e a proteção de dados. Tem-se, portanto, um passo fundamental para a proteção da personalidade dos cidadãos na sociedade da informação.<sup>28</sup>

No entanto, embora de extrema relevância para o reconhecimento de um direito fundamental autônomo à proteção de dados, a decisão do STF não é suficiente para o reconhecimento constitucional de um direito fundamental à proteção de dados. Nesse sentido, Sarlet ressalta a importância do reconhecimento na esfera constitucional de um direito fundamental autônomo à proteção de dados.<sup>29</sup>,

À vista disso, devido a uma tendência global de reconhecimento da proteção de dados como um direito fundamental, a preocupação legislativa com o tema demonstrou um viés mais protecionista com a aprovação da Proposta de Emenda à Constituição n. 17/2019, de autoria da Senadora Simone Tebet, em 20 de outubro de 2021. Desse modo, após a promulgação da PEC n. 17/2019, a disciplina acerca da proteção de dados adquire novos contornos, ao alterar a Constituição Federal, para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais

---

fundamental autônomo. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

<sup>27</sup> Idem;

<sup>28</sup> MENDES Laura Schertel. RODRIGUES JUNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

<sup>29</sup> SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: Tratado de proteção de dados pessoais/coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021;;

e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Dessa forma, a referida Emenda Constitucional acresce ao art. 5º, que prevê os Direitos e Garantias Individuais<sup>30</sup>, o seguinte inciso LXXIX: “Art. 5º, inciso LXXIX: é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive, nos meios digitais.”<sup>31</sup> Assim como, insere no art. 21, que prevê as competências da União, o seguinte inciso XXVI: “Art. 21 Compete à União: XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.”<sup>32</sup> Outrossim, insere no art. 22 da CF/88, que diz respeito às competências privativas da União, o seguinte inciso XXX: “Art. 22. Compete privativamente à União legislar sobre: XXX – proteção e tratamento de dados pessoais.”<sup>33</sup>

Além disso, cumpre salientar que, em que o artigo 5º, XII, a CF/88 faz referência ao sigilo de comunicações de dados, bem como, por meio do inciso LXXII<sup>34</sup>, do artigo 5º, traz o procedimento para garantir a autodeterminação informacional e instrumentalizar o chamado direito ao esquecimento, com a previsão do direito a impetrar o *habeas data*.

Dessa maneira, é possível afirmar que a disciplina acerca da regulamentação do direito à proteção de dados no ordenamento jurídico-brasileiro, diante desse fenômeno de ampla digitalização de diversas esferas da vida cotidiana, referido na doutrina, comumente, como computação ubíqua ou onipresença da informática na vida cotidiana (*ubiquitous computing*<sup>35</sup>), adquiriu extrema relevância nas últimas

---

<sup>30</sup>BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 11 out. 2021;

<sup>31</sup> BRASIL. Proposta de Emenda à Constituição n. 17/2019 (PEC 17/2019). Senado Federal. Brasília, DF. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/149723>. Acesso em: 11 out. 2021;

<sup>32</sup>Idem;

<sup>33</sup>Idem.

<sup>34</sup> A Constituição Federal de 1988, em seu art;5º, inciso LXXII estabelece o seguinte: “LXXII - conceder-se-á “*habeas-data*” :a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.” BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 11 out. 2021;

<sup>35</sup> “A ideia básica da computação ubíqua é que a computação move-se para fora das estações de trabalho e computadores pessoais (PCs) e torna-se pervasiva em nossa vida cotidiana. Marc Weiser, considerado o pai da computação ubíqua, vislumbrou há uma década atrás(sic.) que, no futuro, computadores habitariam os mais triviais objetos: etiquetas de roupas, xícaras de café, interruptores de luz, canetas, etc, de forma invisível para o usuário. Neste mundo de Weiser, devemos aprender a

décadas. À vista disso, Doneda ressalta que a proteção de dados pessoais adquire uma importância que vai muito além da mera novidade representada pela terminologia em si, porquanto:

[...]radica numa viragem concepcional, visto que parte do pressuposto de que dados, para efeitos de sua proteção jurídico-constitucional, devem ser compreendidos em sentido amplo, no sentido da inexistência de dados pessoais irrelevantes em face do processamento eletrônico na sociedade de informação, notadamente pelo fato de que, sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais.<sup>36</sup>

Dessa maneira, a facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, aumenta exponencialmente as possibilidades de violação dos direitos e garantias fundamentais individuais, mediante o conhecimento e o controle de informações sobre a vida pessoal, privada e social dos indivíduos por parte dos agentes responsáveis pelo tratamento dos dados pessoais. Sendo assim, compreendemos que as rápidas mudanças impõem novos desafios aos ordenamentos jurídicos, que precisam se adequar e incorporar novas terminologias e conceitos que se alteram a todo instante.

Assim, à medida em que as tecnologias da informação adentram aos mais diversos aspectos da vida cotidiana, o direito à proteção de dados adquire íntima relação com o princípio da dignidade da pessoa humana, com os direitos e garantias fundamentais e as liberdades individuais no Estado Democrático de Direito. Dessa maneira, na doutrina refere-se comumente a um processo acelerado de digitalização da sociedade e das diversas áreas do conhecimento, assim como, do próprio Direito. Nesse sentido, podemos citar o entendimento de Sarlet, ao referenciar um processo de digitalização dos direitos fundamentais, o seguinte:

Assim, não é à toa que já há tempos se fala em um processo de digitalização dos direitos fundamentais (ou de uma dimensão digital dos direitos fundamentais), bem como de uma digitalização do próprio Direito (daí se falar também de um Direito Digital), o que, à

---

conviver com computadores, e não apenas interagir com eles ." ARAÚJO, Regina Borges de. Computação Ubíqua: Princípios, Tecnologias e Desafios. Disponível em: [http://www.professordiovani.com.br/rw/monografia\\_araujo.pdf](http://www.professordiovani.com.br/rw/monografia_araujo.pdf) Acesso em: 15 de nov de 2021.  
36DONEDA, Danilo. Panorama histórico da proteção de dados pessoais in: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021;

evidência, inclui – mas de longe não só isso! – o reconhecimento gradual, na esfera constitucional e no âmbito do direito internacional, de um direito humano e fundamental à proteção de dados, assim como de outros princípios, direitos (e deveres) conexos, mas também de uma releitura de direitos fundamentais “clássicos”. 37

Dessa maneira, é possível afirmar que a proteção dos dados pessoais dos usuários das redes é um dos maiores desafios enfrentados pelo Direito na atualidade, uma vez que a rápida transformação digital e a presença das novas tecnologias impõem problemas inimagináveis anteriormente, no que se refere às possíveis violações aos direitos dos titulares dos dados advindas nesse contexto. Deprendemos, assim, que as informações pessoais devem ser protegidas, por representarem uma extensão da personalidade, tendo em vista a capacidade das tecnologias de processamento de dados, realizados por meio de inteligência artificial, algoritmos complexos e armazenados em sistemas complexos de bancos de dados, exprimem hábitos, predileções e fatores subjetivos precisos dos indivíduos.

Assim, é de suma importância o reconhecimento do direito à proteção de dados como um direito fundamental autônomo, para além de uma mera decorrência da privacidade, como um “direito fundamental autônomo cujo âmbito de proteção está vinculado à tutela da dignidade e da personalidade dos cidadãos no seio da sociedade da informação” 38.

### **2.2.1. O sistema europeu de proteção de dados pessoais**

A partir do século XXI, vivenciamos um aumento exponencial da complexidade das relações estabelecidas com o uso da *internet*, que passou a conectar bilhões de pessoas ao redor do mundo e causar profundos impactos nas relações sociais, políticas, econômicas e culturais, nos mais diversos níveis, com intensidade e velocidade inimagináveis anteriormente. No estágio atual em que a sociedade se encontra, referida, comumente, como “Sociedade da Informação” ou

---

<sup>37</sup>SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: Tratado de proteção de dados pessoais/coordenadores Danilo Doneda...[et al.]. – Rio de Janeiro: Forense, 2021;

<sup>38</sup>Idem;

“Sociedade 4.0”, os dados passam a ser considerados moeda de troca e um valioso ativo econômico.

Nesse sentido, Ribas e Guerra<sup>39</sup> referem que, a partir do século XXI, os dados passam a ser o recurso mais valioso da sociedade, em substituição ao petróleo. Assim, para garantir a segurança organizacional, as empresas devem empregar técnicas que confirmem maior segurança aos dados coletados de seus usuários. Dessa forma, é possível afirmar que o maior desafio diz respeito a como conciliar o surgimento de novas tecnologias, o desenvolvimento econômico e o fluxo de dados em escala global e, ao mesmo tempo, garantir a segurança jurídica dos titulares de dados.

Nesse contexto, diversas legislações protetivas surgiram ao redor do mundo nas últimas décadas, a Convenção 108, do Conselho da Europa para a Proteção de Dados, em 1981, é considerado o primeiro instrumento internacional, juridicamente vinculativo, a considerar a proteção de dados como um direito fundamental.<sup>40</sup>

À vista disso, Pinheiro afirma o seguinte:

[...]a proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia.<sup>41</sup>

Nesse contexto, Doneda<sup>42</sup> ressalta que se deve ter em vista “a Convenção 108 como o ponto de referência inicial do modelo europeu de proteção de dados pessoais, mesmo porque ela é fruto direto do estado da arte das reflexões e debates sobre os rumos da matéria no espaço europeu.” Tendo em vista que, nessa normativa, instituída em 1981, em Estrasburgo, na França, a proteção de dados

---

<sup>39</sup>RIBAS, Brenno Henrique de Oliveira; GUERRA, Caroline Cardoso Guerra. O IMPACTO DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS DA UNIÃO EUROPEIA NO BRASIL. *apud* THE ECONOMIST. The world's most valuable resource is no longer oil, but data. 2017, p. 1. Disponível em: [https://scholar.googleusercontent.com/scholar?q=cache:HpgPYRWKD7MJ:scholar.google.com/+o+m+odelo+europeu+de+prote%C3%A7%C3%A3o+de+dados&hl=pt-BR&as\\_sdt=0,5&as\\_ylo=2020](https://scholar.googleusercontent.com/scholar?q=cache:HpgPYRWKD7MJ:scholar.google.com/+o+m+odelo+europeu+de+prote%C3%A7%C3%A3o+de+dados&hl=pt-BR&as_sdt=0,5&as_ylo=2020). Acesso em 27 set. 2021

<sup>40</sup>Parlamento Europeu. Proteção de Dados Pessoais. Disponível em: [https://www.europarl.europa.eu/ftu/pdf/pt/FTU\\_4.2.8.pdf](https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf). Acesso em: 27 set. 2021;

<sup>41</sup>PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n.º 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

<sup>42</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

personais é relacionada diretamente à proteção das liberdades fundamentais e das garantias individuais, como “pressuposto do estado democrático”<sup>43</sup>.

Dessa maneira, Doneda<sup>44</sup> ressalta que o próprio processo de formação da União Europeia implicou adequações nos sistemas jurídicos por parte dos estados-membros, devido à importância da formação de um direito comunitário. Em razão disso, a disciplina acerca da proteção de dados passou a tender para uma uniformização, com a finalidade de “diminuir atritos entre os vários ordenamentos nacionais, mas, também, a promoção dos valores que orientam a União Europeia.”<sup>45</sup>

Assim, importância do tema evidencia-se na medida em verificamos que o debate, acerca da privacidade no ambiente digital e da captação e processamento de dados de usuários da Internet, já se fazia presente nos ordenamentos jurídicos europeus desde a segunda metade do século XX. No entanto, o tema adquiriu maior relevância em 1995, quando foi aprovada a Diretiva 95/46 CE, por meio da qual, unificou-se normas acerca da proteção de dados pessoais entre os estados-membro da UE. Dessa forma, nos anos seguintes, diversos países integrantes da União Europeia passaram a incorporar a proteção de dados em seus ordenamentos internos.

Dessa forma, ressalta-se que a Diretiva 95/46/CE, de 1995, tinha como finalidade a regulamentação do tratamento de dados pessoais no território da Comunidade Europeia, ao estabelecer princípios, padrões e regras para o tratamento de dados pessoais. Assim, constituía, até a entrada em vigor do Regulamento Geral de Proteção de Dados, em 2016, o texto referência em matéria de proteção de dados e tinha como finalidade “estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da União Europeia (UE).”<sup>46</sup>

Anteriormente, alguns países europeus já haviam legislado a esse respeito, cita o ilustre doutrinador Danilo Doneda, como exemplo, a sintética<sup>47</sup> Lei de Proteção de Dados pessoais do *Lande de Hesse*, na Alemanha Ocidental, em 1970. Assim

---

<sup>43</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

<sup>44</sup>Idem;

<sup>45</sup>Idem;

<sup>46</sup>PARLAMENTO EUROPEU: Regulamento Geral sobre Proteção de Dados Pessoais da União Europeia. Disponível em: <https://gdpr-info.eu/> Acesso em: 27 set. 2021;

<sup>47</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

como, uma Lei Federal sobre o tema, promulgada em 1977, na Alemanha, a *Bundesdatenschutzgesetz*. Nesse sentido, afirma, ainda, o seguinte:

A primeira lei nacional sobre proteção de dados pessoais, porém, foi a lei sueca sobre o controle de bancos de dados, de 1973. Logo a seguir vieram leis em outros países europeus: na França, a Lei 78-17 de 6 de janeiro de 1978, denominada *Informatique et Libertés*, passou a regular a matéria, para cuja tutela foi instituída a CNIL – *Commission Nationale de l’Informatique et des Libertés* – como órgão encarregado de zelar pela sua aplicação. Outros países europeus legislaram à época sobre esse tópico, como Dinamarca, Áustria, Noruega, Luxemburgo e Islândia.<sup>48</sup>

Assim, devido a novas formas de captação de dados, em 1973, “foi publicada uma resolução incentivava os países europeus a adotarem princípios mínimos na matéria, com vistas a uma futura convenção para aprofundar as linhas comuns em seu direito interno.”<sup>49</sup> Dessa forma, o autor ressalta que, o amplo debate, promovido pela edição de leis em diversos países, contribuiu para a percepção da necessidade de se instituir parâmetros mínimos e de se uniformizar o tema em caráter supranacional.<sup>50</sup>

Sendo assim, é possível auferir que essa nova forma de organização social advinda com o uso das redes de computador, pelos avanços tecnológicos e pela globalização dos meios digitais de comunicação e, ainda, pelo surgimento de meios capazes de captar, armazenar, processar e distribuir informações – de forma extremamente rápida e eficaz – trouxe à tona a necessidade de uma regulamentação mais ampla e abrangente, capaz de lidar com esses novos desafios. Assim como, do estabelecimento de diretrizes para a atividade de fiscalização do cumprimento das normas sobre o assunto.

Nesse contexto, foi proposta, em 2012, o Regulamento Geral de Proteção de Dados na União Europeia, que passou por um amplo debate, ao longo de quatro anos, para sua elaboração e aprovação. Assim como, foi aprovada a Diretiva 2016/680, de 27 de abril de 2016, que dispõe acerca da proteção das pessoas singulares e ao tratamento de dados pessoais pelas autoridades competentes, para

---

<sup>48</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

<sup>49</sup>Idem;

<sup>50</sup>Idem;

fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à sua livre circulação.<sup>51)</sup>

O Regulamento Geral de Proteção dos Dados Pessoais, da União Europeia (RGPD), desde que entrou em vigor em 24 de maio de 2016, com aplicação a partir de 25 de maio de 2018<sup>52</sup>, adquiriu extrema notoriedade no cenário internacional sobre proteção de dados. Dessa forma, esse Regulamento tornou-se uma medida essencial, a fim de reforçar os direitos fundamentais das pessoas na era digital, assim como, proporcionar um ambiente comercial seguro, diante da “clarificação das normas aplicáveis às empresas e aos organismos públicos no mercado único digital.”<sup>53</sup> Além disso, a uniformização, por meio de um ato legislativo único, tem por finalidade “acabar com a fragmentação resultante da coexistência de sistemas nacionais diferentes e com encargos administrativos desnecessários.”<sup>54</sup>

Dessa maneira, compreendemos que o RGPD trouxe implicações, à proteção de dados, que ultrapassaram os limites da União Europeia, ao estabelecer novos parâmetros de proteção a serem observados pelos países que pretendam estabelecer relações comerciais com o bloco europeu. Nesse sentido, Döhmman, afirma o seguinte:

A repercussão do RGPD-UE para além das fronteiras da Europa não deveria ser subestimada, pois ele oferece a possibilidade de estabelecer um *level playing field* em um mercado que já parece estar firmemente subdividido, com poucos fornecedores, e contrabalançar fenômenos de falha de mercado já existentes. Mencione-se apenas, a título de exemplo, que três das maiores democracias do mundo assumiram, por sua vez, elementos substanciais do RGPD-UE. 55

---

<sup>51</sup>Parlamento Europeu. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680>. Acesso em: 25 set. 2021;.

<sup>52</sup>Parlamento Europeu. *The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data*. Disponível em: [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_pt#evento](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt#evento). Acesso em: 25 set. 2021;

<sup>53</sup>Idem;

<sup>54</sup>Idem;

<sup>55</sup>DÖHMANN, Indra Spiecker gennant. A proteção de dados pessoais sob o regulamento geral de proteção de dados da união europeia *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

Assim, é possível afirmar o Regulamento Geral sobre Proteção de Dados da União Europeia impulsionou, significativamente, o surgimento de novas legislações sobre proteção de dados ao redor do mundo. Nesse sentido, a autora afirma que o Japão foi o primeiro país a estabelecer uma normativa em estreita sintonia com a UE<sup>56</sup>, o APPI (*Act on the Protection of Personal Information – Lei de Proteção de Informações Pessoais*), promulgado em 12 de junho de 2020<sup>57</sup>, foi considerado pela Comissão Europeia adequado ao nível de protecionismo do RGPD, surgindo, assim, o maior mercado europeu-asiático de dados.<sup>58</sup>

À vista disso, o RGPD, a fim de coibir comportamentos abusivos, surge com o intuito de proporcionar maior proteção à privacidade dos usuários nas redes, por meio da proteção da pessoa natural e, ainda, da necessidade de que seja garantido a livre circulação dos dados pessoais, Doneda, sobre o tema, afirma o seguinte:

Verificamos, portanto, a presença dos dois eixos em torno dos quais a disciplina se estrutura – a proteção da pessoa e a necessidade de proporcionar a livre circulação de “pessoas, mercadorias, serviços e capitais” no espaço comunitário, o que implica a circulação de dados pessoais – bem como a presença de um critério de equilíbrio entre ambos, que é a referência ao homem e aos seus direitos fundamentais, reconhecida como base e fundamento de toda a disciplina.<sup>59</sup>

Assim, com o intuito de proporcionar maior proteção à privacidade na *internet*, o RGPD prevê maior transparência pelas empresas responsáveis pela captação, pelo processamento e pela transmissão dos dados pessoais dos usuários. De acordo com Doneda<sup>60</sup> “O estabelecimento de um nível mínimo de proteção aos dados pessoais, presente em todo o espaço da UE foi o pressuposto necessário para possibilitar um livre fluxo desses dados dentro de suas fronteiras.” Além disso, o autor refere que “o crescente fluxo internacional de dados pessoais gera uma demanda por padrões normativos que o legitimem, e as normas europeias são,

---

<sup>56</sup>DÖHMANN, Indra Spiecker gennant. A proteção de dados pessoais sob o regulamento geral de proteção de dados da união europeia *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

<sup>57</sup>Parlamento Japonês: *Amended Act on the Protection of Personal Information*. Disponível em: [https://www.ppc.go.jp/files/pdf/APPI\\_english.pdf](https://www.ppc.go.jp/files/pdf/APPI_english.pdf). Acesso em: 3 nov. 2021.

<sup>58</sup>DÖHMANN, Indra Spiecker gennant. A proteção de dados pessoais sob o regulamento geral de proteção de dados da união europeia *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

<sup>59</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

<sup>60</sup> Idem;

certamente, o modelo mais desenvolvido nesse sentido.”<sup>61</sup> Outrossim, aponta para “a existência de uma cláusula de vedação da transferência de dados para países fora do espaço comunitário que não apresentem nível “adequado” de tutela.”<sup>62</sup>

Assim, percebemos que a nova realidade digital, advinda com a transformação digital, trouxe inúmeras implicações relativas à proteção dos dados pessoais na sociedade da informação. Diante da exponencial evolução tecnológica, a captura, o processamento, o armazenamento e a transmissão de dados pessoais, assim como, sua transformação em ativos econômicos, trouxeram à tona diversos problemas relativos a violações de direitos e garantias fundamentais.

Nesse contexto, compreendemos que um dos maiores desafios em que a busca pela garantia de proteção de dados esbarra, diz respeito à velocidade das inovações e às rápidas mudanças nas relações estabelecidas, frente à dinâmica complexa das redes de comunicação. Nesse sentido Ribas e Guerra<sup>63</sup> ressaltam que as normas que tratam da proteção de dados poderiam tornar-se ultrapassadas em pouco tempo, diante das rápidas mudanças experimentadas no ambiente virtual. Dessa forma, afirmam que o RGPD utilizou o conceito expansionista em sua concepção,<sup>64</sup> a fim de que essa amplitude permita uma maior dinamização da legislação, diante da “necessidade de expansão e de “atualização” das formas jurídicas de tutela da personalidade dos cidadãos perante as mudanças tecnológicas ocorridas.”<sup>65</sup>

Além dos mais, as organizações que disponham de dados de cidadãos europeus, devem seguir a lei europeia, ainda que não estejam situadas em território europeu. Nesse contexto, o Regulamento Europeu somente permite a transferência dos dados pessoais de cidadãos europeus para países com lei de proteção de dados equivalente ao RGPD. Assim, devido à importância que o RGPD adquiriu em cenário internacional e o fato de que esta legislação estabeleceu um nível de

---

<sup>61</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

<sup>62</sup>Idem;

<sup>63</sup>RIBAS, Brenno Henrique de Oliveira; GUERRA, Carolinne Cardoso Guerra. O impacto do regulamento geral de proteção de dados pessoais da união europeia no Brasil. Disponível em: [https://scholar.googleusercontent.com/scholar?q=cache:HpgPYRWKD7MJ:scholar.google.com/+o+m+odelo+europeu+de+prote%C3%A7%C3%A3o+de+dados&hl=pt-BR&as\\_sdt=0,5&as\\_ylo=2020](https://scholar.googleusercontent.com/scholar?q=cache:HpgPYRWKD7MJ:scholar.google.com/+o+m+odelo+europeu+de+prote%C3%A7%C3%A3o+de+dados&hl=pt-BR&as_sdt=0,5&as_ylo=2020). Acesso em 27 set. 2021;

<sup>64</sup>POLIDO, FBP; ANJOS, LC; BRANDÃO, LCC; MACHADO, DC; OLIVEIRA, DTN GDPR e suas repercussões no direito brasileiro. Primeiras impressões de análise comparativa. 2018, p. 7.;

<sup>65</sup>MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização; *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

adequação aos demais países que pretendam estabelecer uma relação comercial com os países do bloco, compreende-se que tal normativa influenciou, diretamente, no surgimento de legislações que disciplinam a proteção de dados ao redor no mundo. Nessa toada, da mesma maneira, influenciou no debate que deu origem ao anteprojeto de lei e ao projeto que resultou na Lei Geral de Proteção de Dados Pessoais, Lei n. 13.709, de 2018 – (LGPD) em território brasileiro.

Ademais, cita-se a proposta de nova regulamentação, em território europeu, acerca da privacidade eletrônica, o *ePrivacy Regulation*<sup>66</sup>, cuja justificativa<sup>67</sup> reside na necessidade de que a legislação europeia acompanhe o acelerado ritmo de desenvolvimento e evolução das tecnologias da informação. Compreende-se, assim, que o sistema europeu está constantemente buscando maneiras de se adequar aos novos desafios impostos por essa nova realidade digital, por meio da organização e da promoção de um amplo debate com as partes interessada. Em consulta ao sítio eletrônico da proposta, verifica-se que foi realizada uma pesquisa para reunir a opinião dos cidadãos, realizada uma avaliação de impacto, apoiada por um estudo e estabelecido o atual projeto.<sup>68</sup>

Dessa maneira, é possível afirmar que para a compreensão do fenômeno da proteção de dados e do surgimento de diversas legislações que tratam do tema, dentre as quais, inclui-se, o modelo brasileiro de proteção de dados, recentemente atualizado e compilado pela LGPD, é preciso compreender, antes de tudo, a existência de uma tendência global acerca da necessidade se proteger os dados pessoais dos usuários das redes e da adequação das organizacional das instituições responsáveis pelas operações de tratamento.

Nesse sentido, conforme leciona o professor Danilo Doneda, há uma tendência para à convergência entre as legislações a respeito da proteção de dados pessoais, diante da necessidade de que sejam adotados modelos não “meramente nacionais”, devido à influência digital na vida cotidiana e do caráter global que as

---

<sup>66</sup> COMISSÃO DO PARLAMENTO EUROPEU. *Proposal for an ePrivacy Regulation*. Projeto disponível em: <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>. Acesso em: 25 set. 2021;

<sup>67</sup> “European legislation needs to keep up with the fast pace at which IT- based services are developing and evolving. The Commission has started a major modernisation process of the data protection framework over the past few years, which culminated in the adoption of the General Data Protection Regulation (GDPR). The ePrivacy legislation needs to be adapted to align with these new rules.”. Idem;

<sup>68</sup> Idem;

violações ao direito à privacidade, por meio de vazamentos de dados adquirem nesse contexto de mundo globalizado.

Dessa maneira, percebe-se que o surgimento de novas tecnologias da informação e a digitalização das mais diversas áreas do conhecimento trouxe-se à luz a urgência de uma necessária regulamentação por parte do direito e do poder estatal. Outrossim, de fiscalização por entidades governamentais competentes e pelos mais diversos setores interessados. Nesse contexto, Doneda ressalta que o modelo europeu, estrutura-se “em torno de uma Diretiva”<sup>69</sup>, ao oferecer uma sistemática mais ampla e detalhista, que deve ser incorporada na legislação interna de cada estado-membro, disciplinada recentemente, conforme já referenciado, pelo Regulamento Geral de Proteção de Dados (RGPD), que entrou em vigor em maio de 2018.

Ademais, nos Estados Unidos da América, no estado da Califórnia, tem-se o *Consumer Privacy Act*, de 2018, que possibilita aos consumidores terem maior controle sobre suas informações pessoais coletadas pelas empresas, trazendo orientações sobre como implementar esse marco regulatório. Dessa forma, traz novas garantias do direito à privacidade dos consumidores como: I) o direito de saber sobre as suas informações pessoais coletadas pelas empresas e como elas são usadas e compartilhadas; II) o direito de requisitar a exclusão das suas informações pessoais coletadas (com algumas exceções); III) o direito de decidir sobre a venda de suas informações pessoais; e IV) o direito à não discriminação para o exercício de seus direitos.<sup>70</sup>

Em contrapartida, o modelo norte-americano não possui uma sistemática consolidada, sendo representado por legislações esparsas, sobretudo pelo *Consumer Privacy Act*, do estado da Califórnia e por jurisprudências das Cortes Superiores. Nesse sentido, Doneda afirma que as diferenças existentes entre “os sistemas de *common law* e *civil law* certamente exerceu influência no desenvolvimento de diferentes regimes de proteção de dados pessoais”<sup>71</sup>, ao afirmar que alguns países que adotam o modelo de *common law* oferecem certa resistência

---

<sup>69</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

<sup>70</sup>GOVERNO DO ESTADO DA CALIFÓRNIA. *California Consumer Privacy Act (CCPA)*, Tradução nossa. Disponível em: <https://oag.ca.gov/privacy/ccpa>. Acesso em: 3 nov. de 2021.

<sup>71</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021

em vincular, a sistemática da proteção de dados aos direitos fundamentais e a tutela da dignidade da pessoa humana.<sup>72</sup>

Conforme preceitua o ilustre doutrinador, o modelo norte-americano:

[..]apresenta-se fracionado, com disposições legislativas e jurisprudenciais concorrentes em uma complexa estrutura federativa, o que torna sua leitura em chave sistemática – e até mesmo a compreensão geral de seu conjunto – um desafio para os próprios juristas norte-americanos.<sup>73</sup>

Assim, objetiva-se demonstrar que, diante dos notórios casos de uso indevido de dados pessoais, torna-se urgente a necessidade de aperfeiçoamento de instrumentos jurídicos com a finalidade de proteção de dados e da privacidade na *internet*. Assim como, da implementação de boas práticas empresariais relativas à governança de dados e de implementação e adequação das práticas de *compliance empresarial* à luz da LGPD e demais normas setoriais e técnicas de segurança da informação, que versam sobre o tratamento dos dados pessoais.

### **2.3. Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709/2018 e seus fundamentos**

Na LGPD a temática relacionada a proteção de dados tem como fundamentos o cumprimento aos valores éticos e normativos, assim como, o respeito a outros valores fundamentais resguardados por todo o ordenamento jurídico, como a Constituição Federal, o Marco Civil da Internet, a Lei do Cadastro Positivo, a Lei de Acesso à Informação e outros regulamentos esparsos.

Assim, encontram previsão no art. 2º, da Lei, o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; o direito ao desenvolvimento econômico e tecnológico e à inovação; à livre iniciativa, à livre concorrência e à defesa do consumidor; aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e o exercício da cidadania pelas

---

<sup>72</sup>DONEDA, Danilo. Panorama histórico da proteção de dados pessoais *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

<sup>73</sup> Idem;

pessoas naturais. Nesse sentido, o art. 2º, disciplina a proteção de dados pessoais, tendo em vista dos seguintes fundamentos.

### **2.3.1. O respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem, o direito à autodeterminação informativa, à liberdade de expressão, de informação, de comunicação e de opinião**

Em consonância com disposição constitucional que, conforme referido anteriormente, trata de um direito fundamental, com previsão expressa no art. 5º, inciso X, da CF/88, assim como, trata-se de um direito de personalidade, previsto no art. 21, do Código Civil Brasileiro de 2002, necessário para o livre desenvolvimento da personalidade da pessoa natural.

Possui fundamento constitucional, no art. 5º, inciso X, da CF/88, bem como, preceitos previstos em outras legislações, como o Marco Civil da Internet que, em seu art. 10, que trata “Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas”, o seguinte:”

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.<sup>74</sup>

Dessa forma, a LGPD buscou conferir maior segurança jurídica aos titulares dos dados, ao reafirmar esse direito fundamental. Além do mais, o art. 7º, inciso I, do MCI, prevê, além da proteção da intimidade, o direito à indenização pelo dano material ou moral em face de sua violação.

Compreendida como uma das mais importantes manifestações do direito à privacidade, por meio da qual, reafirma-se o direito ao controle por parte dos cidadãos sobre seus dados pessoais e, assim, à proteção das informações de caráter pessoal e íntima. Dessa, maneira, verifica-se que a intenção do legislador, ao fundamentar a LGPD na autodeterminação informativa, é conferir papel ativo aos cidadãos quanto ao uso de seus dados pessoais.

---

74BRASIL. Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Estabelece Princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 16 nov. 2021;

Nesse sentido, Sarlet ressalta o seguinte:

[..]o direito à autodeterminação informativa – que, no concernente à sua estrutura normativa, assume a condição de princípio – também não se sobrepõe ao direito à privacidade e mesmo outros direitos especiais de personalidade, o que se verá logo adiante. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão de seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (right to be alone).<sup>75</sup>

Além disso, cumpre salientar que o reconhecimento do direito à autodeterminação informativa como um direito fundamental remonta à decisão do Tribunal Constitucional Alemão de 1983, na decisão sobre a Lei do Censo, que reconheceu o direito ao titular de dados de dispor sobre suas informações pessoais. Nesse sentido, a decisão referiu que com as tecnologias de processamento de dados e a estruturação de bancos de dados, por meio de algoritmos e programas de computador as informações poderiam ser cruzadas e agregadas, impossibilitando ao indivíduo ter controle de forma precisa sobre o seu uso e possíveis violações aos direitos de personalidade dos titulares.<sup>76</sup>

Ademais, em uma sociedade em que a informação é o ativo mais valioso, as garantias individuais, constitucionalmente garantidas no art. 5º, inciso IX, da CF/88, são extremamente importantes para o livre desenvolvimento da personalidade e “condição para o pleno exercício do direito de acesso à internet.”<sup>77</sup>

Além disso, cumpre salientar que nenhum direito é absoluto, da mesma maneira, a liberdade individual não pode ser exercida irrestritamente, ou seja, de maneira ultrapasse os direitos alheios, devendo ser levado em consideração, por

---

<sup>75</sup> SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. SARLET, Ingo Wolfgang. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021.

<sup>76</sup>ROCHA, Elisa Corrêa da. O direito à autodeterminação informativa e a proteção de dados pessoais. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/134888/000986821.pdf?sequence=1&isAllowed=y>. Acesso em: 16 nov. 2021;

<sup>77</sup>Em consonância com o art. 8º, da Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

meio do princípio da proporcionalidade, outros interesses socialmente relevantes. Nesse sentido, o Ministro Gilmar Mendes ressalta que:

As liberdades de expressão e informação e, especificamente, a liberdade de imprensa, somente podem ser restringidas pela lei em hipóteses excepcionais sempre em razão da proteção de outros valores e interesses constitucionais igualmente relevantes, como os direitos à honra, à imagem, à privacidade e à personalidade em geral. STF: ADPF nº 130, Rel. Min. Carlos Brito. (STF, em julgamento do Recurso Extraordinário n. 511.961, de 17 de junho 2009)<sup>78</sup>

### **2.3.2. O direito ao desenvolvimento econômico e tecnológico e à inovação, à livre iniciativa, à livre concorrência e a defesa do consumidor**

Por meio de um cenário de segurança jurídica no ambiente virtual, que possibilite ao país estar adequado às exigências do mercado. A *internet* constitui um ambiente fértil para as empresas oferecerem seus produtos e serviços, por meio da captação das informações pessoais dos usuários, podem gerar conteúdos mais específicos, de acordo com as preferências dos clientes. No entanto, as facilidades advindas com o desenvolvimento tecnológico trazem inúmeras possibilidades de práticas abusivas e de condutas ilícitas. Assim, por meio desse fundamento, compreende-se que a LGPD buscou conferir maior segurança jurídica para ambas as partes, ou seja, maior proteção aos titulares dos dados, ao estabelecer parâmetros de conduta para as empresas, que impliquem maior segurança e prevenção dos riscos envolvidos no tratamento dos dados pessoais.

Por meio do estabelecimento de regras claras e objetivas, a serem observadas pelo setor privado. Dessa maneira, evidencia-se a intenção da LGPD em promover o desenvolvimento econômico e tecnológico, tendo em vista a promoção não apenas da proteção da privacidade e a segurança dos dados pessoais, mas também, o direito à livre iniciativa, a concorrência e a defesa dos direitos dos consumidores-titulares.

---

<sup>78</sup>Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605643>> Acesso em: 16 nov. 2021;

### **2.3.3. Os direitos humanos, como o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, a liberdade de expressão, de informação, de comunicação e de opinião**

Em uma sociedade em que a informação é o ativo mais valioso, essas garantias fundamentais individuais, constitucionalmente garantidas no art. 5º, inciso IX, da CF/88, são extremamente importantes para o livre desenvolvimento da personalidade e “condição para o pleno exercício do direito de acesso à internet;”<sup>79</sup>

Além disso, cumpre salientar que nenhum direito é absoluto, da mesma maneira, a liberdade individual não pode ser exercida irrestritamente, ou seja, de maneira ultrapasse os direitos alheios, devendo ser levado em consideração, por meio do princípio da proporcionalidade, outros interesses socialmente relevantes. Nesse sentido, o Ministro Gilmar Mendes ressalta que:

As liberdades de expressão e informação e, especificamente, a liberdade de imprensa, somente podem ser restringidas pela lei em hipóteses excepcionais sempre em razão da proteção de outros valores e interesses constitucionais igualmente relevantes, como os direitos à honra, à imagem, à privacidade e à personalidade em geral. STF: ADPF nº 130, Rel. Min. Carlos Brito. (STF, em julgamento do Recurso Extraordinário n. 511.961, de 17 de junho 2009)<sup>80</sup>

Estabelece preceito em relação direta com disposições Constitucionais sobre os direitos fundamentais. Quanto ao livre desenvolvimento da personalidade, à dignidade e ao livre exercício da cidadania pelas pessoas naturais, possuem fundamento, com base no art. 1º, III, CF/88 na dignidade humana.

Nesse sentido, Mota e Tena afirmam o seguinte a respeito dos fundamentos da LGPD:

[...]indicam os caminhos que ela segue e que pretende que a sociedade também observe, o que vale para as três esferas dos Poderes constituídos; os valores que protege ou que deseja ver realizados. Há uma evidente quebra de paradigmas que obriga uma adequação (ou mudança) de rotas, principalmente no que tange aos direitos da personalidade. É um caminho sem volta e que precisa ser

---

<sup>79</sup>Em consonância com o art. 8º, da Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet);

<sup>80</sup>Disponível em: < <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605643>> Acesso em:16 nov. 2021;

regulamentado para além do conteúdo presente na LGPD, sob pena de se tornar irreversível. 81

Assim, compreende-se que a LGPD vem resguardar os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade das pessoas naturais. Outrossim, a Lei demonstra preocupação acerca do equilíbrio entre a observância ao princípio da dignidade da pessoa humana, o desenvolvimento de sua personalidade, a preocupação com a privacidade, bem como, com o desenvolvimento econômico e tecnológico.

### **3. GOVERNANÇA E TRATAMENTO DE DADOS PESSOAIS**

Conforme salientado anteriormente, busca-se demonstrar a necessidade de inserção e adequação da temática sobre a Proteção de Dados, como objeto das já existentes políticas de governança em privacidade implementadas nas empresas de tecnologia. Assim, a fim de compreender os desafios impostos pelas novas tecnologias e as inovações trazidas pela LGPD, foram analisados seus objetivos, alguns conceitos introduzidos, seus princípios e bases legais. Tendo em vista, a necessidade da promoção de uma cultura organizacional de boas práticas de governança de dados, que perpassa tanto pela regulamentação sobre o tema, quanto pela implementação de normas e padrões éticos de conduta, aos preceitos relacionados à segurança informacional, os quais, compreende-se que devem ser adequados às inovações implementadas pela Lei n. 13.709/2018. Além do mais, mister que tenham uma política interna bem definida, de proteção das informações sensíveis, por meio da adoção de medidas preventivas e de mitigação dos riscos. Assim como, promovam uma cultura organizacional de conscientização quanto à necessidade de resguardo dessas informações.

Além do mais, a estrita observância às políticas de privacidade e proteção de dados e o estabelecimento de regras claras e precisas aos agentes de tratamento, têm o intuito de conferir maior segurança aos usuários das redes e às relações estabelecidas no meio digital. Compreendemos, assim, que esta abordagem é tema urgente e necessário às organizações e às instituições responsáveis pelas

---

<sup>81</sup>MOTA, Ivan Dias da; TENA, Lucimara Plaza. Fundamentos da LGPD: círculos concêntricos e sociedade da informação no contexto de direitos da personalidade. *Revista Jurídica Unicuritiba. Curitiba*.V.02, n.59, p.538-5, Abril-Junho. 2020 [Received/Recebido: Março 15, 2018; Accepted/Aceito: Fevereiro 22, 2019]

operações de tratamento de dados pessoais. Tendo em vista as imposições e as sanções já estarem em vigor e representarem, para além de meros impactos económicos, diante das sanções administrativas prevista na LGPD, riscos à imagem e à confiabilidade das organizações, que não se adequem às exigências impostas pelo sistema protetivo de dados pessoais.

Dessa maneira, os agentes responsáveis pelas operações de tratamento devem fazer uso de medidas técnicas e administrativas, adequadas à proteção dos dados pessoais dos titulares. Em vista de garantir os direitos dos titulares, previstos na LGPD, diante de possíveis acessos não autorizados de terceiros e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão das informações armazenadas, coletadas e processadas. Assim, as organizações responsáveis pelo tratamento, devem dispor de métodos e procedimentos seguros e eficientes, capazes de monitorar à *internet*, em busca de possíveis violações, a fim de mitigar os riscos e conter possíveis vazamentos de dados. Além do mais, devem promover o fortalecimento da cultura organizacional de proteção e de boas práticas de governança de dados.

### **3.1. Objetivos e aplicabilidade da LGPD**

A Lei n. 13.709, de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, de pessoas naturais ou jurídicas, inclusive no meio digital, a fim de proteger os seus direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da sua personalidade<sup>82</sup>. Por meio da qual, buscou-se a unificação dos diversos regulamentos esparsos sobre o tratamento de dados pessoais no Brasil, a fim de garantir maior efetividade e proteção aos direitos dos titulares de dados, estabelecendo princípios éticos de conduta e procedimentos adequados para conferir maior segurança às operações de tratamento de dados.

Nesse sentido, Pinheiro afirma o seguinte:

O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento

---

<sup>82</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis. 83

Conforme salientado anteriormente, apesar do RGPD se tratar de um regulamento europeu, estão abrangidos e obrigados a seguir as regras imposta, todos os países que mantenham presença e operações em países da União Europeia, com filiais ou armazenamento e processamento de dados de cidadãos europeus, inclusive o Brasil. À vista disso, após longo debate, que envolveu diversos setores da sociedade, a LGPD foi promulgada, alterando o art. 7º e 16 do Marco Civil da Internet, com a finalidade de regulamentar o tratamento de dados pessoais e promover um cenário de maior segurança jurídica aos titulares de dados.

Ademais, as proteções e garantias trazidas pela LGPD aplicam-se, tão somente, às pessoas naturais. Assim, o titular de dados pessoais diz respeito aos sujeitos que detêm a titularidade dos dados que são objeto de tratamento, serão sempre pessoas naturais. Porém, vale ressaltar que as pessoas jurídicas também são alvo da regulação, já que podem atuar como agentes de tratamento de dados pessoais (controladores ou operadores). Contudo, elas não são protegidas pelas garantias trazidas pela norma, pelo contrário, garantem os direitos das pessoas naturais.<sup>84</sup>

Ademais, considerando a relevância que o tema adquiriu nos últimos anos no cenário internacional, em seu art. 3º<sup>85</sup>, dispõe sobre sua aplicabilidade em qualquer operação de tratamento de dados realizada em território nacional, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados<sup>86</sup>. Assim, nos termos da Lei, se os dados forem coletados no território nacional ou, a atividade de tratamento, objetive o fornecimento de bens ou serviços no país ou, ainda, nos

---

<sup>83</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021

<sup>84</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>85</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>86</sup>Idem;

casos em que o tratamento de dados se refira aos titulares localizados no território nacional<sup>87</sup>.

Além do mais, em seu art. 3º, preceitua que é aplicável a todos que realizem qualquer operação de tratamento de dados pessoais, independentemente do meio, do país em que esteja localizada a sua sede ou do país em que os dados estejam localizados, de acordo com os seguintes pressupostos, desde que:

I) a operação ocorra em território nacional; II) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III) os dados pessoais tenham sido coletados em território nacional.<sup>88</sup>

Outrossim, são considerados coletados, em território nacional, os dados pessoais, cujo titular nele se encontre no momento da coleta<sup>89</sup>. Sendo assim, destaca-se o fato de que ela possui alcance extraterritorial, nesse sentido, Pinheiro ressalta o seguinte:

A LGPD tem alcance extraterritorial, ou seja, efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil. Desse modo, o dado pessoal tratado por uma empresa de serviço de cloud computing que armazene o dado fora do país terá que cumprir as exigências da LGPD.<sup>90</sup>

Conforme já mencionado, devido aos novos modelos de negócio, que fazem uso das informações coletadas como moedas de troca e às novas relações estabelecidas no ambiente virtual, houve uma demanda pela criação de sistemas normativos capazes de trazer maior proteção aos dados dos titulares de dados. Dessa maneira, é possível afirmar que a Lei Brasileira, em similaridade com o RGPD, tem alcance extraterritorial. Na medida em que aos dados tratados fora do

---

<sup>87</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 10 nov. 2021.

<sup>88</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 10 nov. 2021.

<sup>89</sup> Idem;

<sup>90</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

Brasil, desde que coletados em território nacional, também são resguardados pela LGPD.

Em seu artigo 4º, ficam estabelecidas as exceções à aplicação da LGPD, ao determinar os usos pela pessoa natural, para os seguintes fins:

- I) exclusivamente particulares e não econômicos;
- II) jornalístico, artísticos, acadêmicos e;
- II) de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais. Além disso, cumpre salientar que o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais será regido, nos termos do art. 4º, §1º, da LGPD, por legislação específica.

No que diz respeito, ainda, ao tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, a lei aponta que é proibida sua realização por pessoa jurídica de direito privado, exceto em procedimentos realizados sob a tutela de pessoa jurídica de direito público. Nesses casos, as operações deverão ser informadas à Autoridade Nacional.

### **3.1.1. Conceitos**

#### **3.1.1.1. Dados pessoais e dados pessoais sensíveis**

A LGPD define como toda informação relacionada a pessoa natural identificada ou identificável<sup>91</sup>. Além disso, para os fins da Lei, também são considerados dados pessoais aqueles utilizados para formação do perfil comportamental (perfilamento) de determinada pessoa natural, se identificada.<sup>92</sup>

Nesse sentido, Pinheiro, define dados pessoais da seguinte maneira:

Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de

---

<sup>91</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>92</sup> BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.<sup>93</sup>

Além disso, consideram-se os dados pessoais sensíveis, aqueles referentes à 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, desde que vinculados a uma pessoa natural.<sup>94</sup>

Assim, PINHEIRO, 2018, define como dados sensíveis aqueles:

São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.<sup>95</sup>

Dessa forma, compreende-se os dados pessoais sensíveis aqueles com maior potencial de serem utilizados para fins discriminatórios, ilícitos ou abusivos. Dessa maneira, as empresas devem promover a revisão dos seus processos de coleta, armazenamento e processamento de dados, mapeando-os e avaliando a necessidade dessas operações para os fins da atividade. Além do mais, é fundamental que tenham uma política interna bem definida de proteção aos dados sensíveis, por meio da adoção de medidas preventivas e de mitigação dos riscos. Assim como, promovam uma cultura organizacional de conscientização quanto à necessidade de resguardo dessas informações, conforme será estudo mais afrente em capítulo específico sobre o tema.

---

<sup>93</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 10 nov. 2021.

<sup>94</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 10 nov. 2021.

<sup>95</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

### 3.1.1.2 Tratamento de dados pessoais e de dados pessoais sensíveis

A LGPD traz um conceito bastante amplo e abrangente no que se refere ao tratamento de dados<sup>96</sup>, inclui-se qualquer tipo de operação realizada com informações coletadas de pessoas naturais, inclusive nos meios digitais. Dessa maneira, por meio dessas operações, informações que possam ser consideradas irrelevantes, após a captação, a organização e o cruzamento por meio de algoritmos e sistemas de computador, podem resultar em valiosíssimos ativos econômicos, capazes de apresentar informações comportamentais e traçar um perfil preciso dos hábitos dos titulares.

Nesse sentido, Teffé e Viola ressaltam o seguinte:

Na Lei Geral de Proteção de Dados (Lei n. 13.709/18 - LGPD), parte-se da ideia de que todo dado pessoal tem importância e valor. Por essa razão se adotou conceito amplo de dado pessoal, assim como estabelecido no Regulamento europeu (*GDPR - General Data Protection Regulation*), sendo ele definido como informação relacionada a pessoa natural identificada ou identificável. Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela, conforme já observou o *Bundesverfassungsgericht* (Tribunal Constitucional Federal Alemão) no emblemático julgamento sobre a lei do censo de 1983.<sup>97</sup>

Dessa maneira, a LGPD possui aplicabilidade em qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica, de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde os dados estejam localizados, desde que:<sup>98</sup>.

---

96Nos termos do art. 5º, inciso X, da LGPD, refere-se “X - a 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.” BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

97TEFFÉ, Chiara Spadaccini de. VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510/384>. Acesso em: 16 nov. 2021;

98 Conforme disposto no art.3º , caput e incisos I a III, da LGPD. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

- I) a operação de tratamento seja realizada no território nacional;
- II). a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- III). os dados pessoais objetos do tratamento tenham sido coletados no território nacional.<sup>99</sup>

Além disso, a LGPD não é aplicada ao tratamento de dados pessoais provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados<sup>100</sup> com agentes de tratamento brasileiros ou objeto de transferência internacional de dados<sup>101</sup> com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Ademais, o tratamento dos dados pessoais sensíveis, conforme disposto no art. 11, inciso I, da LGPD, somente poderá ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas. Dessa maneira, quando não houver consentimento, essa operação somente poderá ocorrer nas hipóteses em que o tratamento for indispensável para:

- I – O cumprimento de obrigação legal ou regulatória pelo controlador;
- II – O tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas<sup>102</sup> previstas em leis ou regulamentos;
- III – A realização de estudos por órgão de pesquisa<sup>103</sup>, garantida, sempre que possível, a anonimização;

<sup>99</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>100</sup>Compartilhamento de dados, nos termos do art. 5º, XVI, da LGPD, refere-se à “XVI - 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. BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>101</sup>Nos termos do art. 5º, XV, da LGPD, refere-se à “XV - transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;” BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>102</sup>Dizem respeito às operações realizadas pela administração pública, para o tratamento e uso compartilhado de dados, necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, conforme disposto no art. 7º, III, da LGPD, observadas as disposições do Capítulo IV da LGPD; BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>103</sup>.Nos termos do art. 13, caput, da LGPD :”Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente

IV – O exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral<sup>104</sup> (a última hipótese, em observância ao disposto na Lei n. 9.307/96);

V – A proteção da vida ou da incolumidade física do titular ou de terceiros<sup>105</sup>;

VI – A tutela da saúde<sup>106</sup>, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

VII – A garantia da prevenção à fraude<sup>107</sup> e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos do titular e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.<sup>108</sup>

Dessa forma, a tutela da proteção ao tratamento dos dados pessoais sensíveis pode ser considerado um dos pontos mais importantes da Lei, na medida em que estes representam os dados com maior potencial de discriminação e segregação dos titulares dos dados. Nesse sentido, Mulholland ressalta o seguinte:

Dos princípios previstos, dois são de especial relevância quando do tratamento de dados sensíveis, quais sejam, o princípio da finalidade

---

dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. “BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>104</sup> O art. 7º, VI, refere-se à possibilidade de tratamento de dados pessoais para fins de andamento de processos judiciais, administrativos e arbitrais, ou seja, para fins de produção de provas; BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>105</sup> Nos termos do art. 7º, VII, da LGPD, refere-se à possibilidade de tratamento de dados pessoais para “VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;” BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>106</sup> Nos termos do art. 7, VIII, conforme redação dada pela Lei n. 13.853/2019, refere-se à possibilidade de tratamento de dados pessoais quando necessário “VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;” BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

<sup>107</sup> No que se refere à proteção de crédito, ressalta-se o seguinte: “é a hipótese de tratamento de dados pessoais voltada a viabilizar e proteger as operações do mercado financeiro de crédito, permitindo, por exemplo, a inscrição de consumidores nos cadastros positivos de crédito e análises de risco com base no histórico de inadimplemento (Art. 7o, X). É mais um caso em que a LGPD deve dialogar com outras leis setoriais (e.g. Código de Defesa do Consumidor e Lei do Cadastro Positivo).” Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getúlio Vargas - São Paulo: CEPI-FGV Direito SP, 2021.

<sup>108</sup> BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

e o princípio da não discriminação. Pelo princípio da finalidade, os dados devem ser tratados para determinados propósitos, que devem ser informados ao titular de dados previamente, de maneira explícita e sem que seja possível a sua utilização posterior para outra aplicação.

[...]

Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas.<sup>109</sup>

### 3.1.1.3 Tratamento de dados pessoais de crianças e adolescentes

Por meio do seu art. 14, a LGPD visa a proteção integral, nas operações de tratamento de dados, dos direitos das crianças e adolescentes, por meio da observância a princípios já previstos na CF/88 e no Estatuto da Criança e do Adolescente, tendo em vista a posição destes como vulneráveis e que necessitam de proteção diferenciada.

Assim, o referido artigo leva em consideração as operações de tratamento de dados, que devem ser realizadas em observância ao melhor interesse da criança e do adolescente, conforme preceitua o art.14, da LGPD. Outrossim, o art. 14, § 1º, da Lei preceitua que “O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal”<sup>110</sup>.

Nesse sentido, Botelho ressalta o seguinte:

É evidente que o dispositivo supramencionado adota o princípio da proteção integral da criança e do adolescente, se amoldando ao plexo de normas protetivas existentes tanto no plano interno como no externo. Logo, há evidente obrigatoriedade de observância no tratamento de dados, do melhor interesse da criança o que significa que a hermenêutica utilizada na interpretação das normas da LGPD

---

<sup>109</sup>MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Disponível em: <<https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>> Acesso em: 16 nov2021;

<sup>110</sup>BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Leis/2002/L10406.htm](http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm). Acesso em: 15 nov. 2021;

devem sempre promover a otimização dos direitos fundamentais de crianças e adolescentes 111

Ademais, o art. 14, § 6º da LGPD, prevê que as informações, referentes ao tratamento de dados dos titulares, devem ser apresentadas de maneira simplificada, clara e acessível. Nesse sentido, devem ter em vista as capacidades físico-motoras, perceptivas, sensoriais, intelectuais e mentais dos indivíduos.<sup>112</sup> Além do mais, poderão utilizar recursos audiovisuais adequados, com a finalidade de propiciar, adequadamente, as informações necessárias, aos pais ou responsáveis legais e apropriadas ao discernimento de todos os sujeitos.<sup>113</sup>

### 3.1.1.4 Tratamento de dados pelo poder público

Refere-se ao tratamento efetuado pelas pessoas jurídicas de direito público, ou seja, órgãos integrantes da administração pública direta ou indireta, que deverá ser realizada para o atendimento de sua finalidade pública, em vista do interesse público, com o objetivo de executar competências legais ou cumprir atribuições legais do serviço público.

Nesse sentido, Aguilera e Di Biase ressaltam que:

[...] a diferença na base legal para o tratamento de dados pelo Poder Público é igualmente marcante, prevalecendo, na relação assimétrica existente entre Estado e particulares, os propósitos indicados no art. 23, caput, da LGPD. Nos termos do referido dispositivo, a manipulação de dados pessoais somente será lícita se realizada em observância aos seguintes propósitos: (i)atendimento da finalidade pública do agente; (ii)persecução do interesse público; e (iii) execução de competência ou atribuições legais do servidor público.<sup>114</sup>

---

111BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. Disponível em: [http://www.mpsp.mp.br/portal/page/portal/documentacao\\_e\\_divulgacao/doc\\_biblioteca/bibli\\_servicos\\_produtos/bibli\\_informativo/bibli\\_inf\\_2006/Rev-Dir-Soc-Pol-Publicas\\_v.8\\_n.2.08.pdf](http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf). Acesso em: 16 de nov. de 2021.

<sup>112</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 10 nov. 2021.

<sup>113</sup>Idem;

<sup>114</sup>AGUILERA, Daniel Fortes; BIASE, Nicholas Furlan Di. Dificuldades interpretativas no regime de tratamento de dados pelo poder público: lacunas, contradições e atecnias na LGPD. Disponível em: <http://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238/182>. Acesso em: 16 nov. 2021;

Além do mais, conforme disposto no art. 23, parágrafo único, da LGPD, quando as empresas públicas e as sociedades de economia mista estiverem operacionalizando políticas públicas, no âmbito da sua execução, deverão observar as mesmas regras impostas aos órgãos e entidades do Poder Público, dispostas no capítulo IV, da Lei.

### **3.2. Princípios aplicáveis às operações de tratamento de dados**

Este é um dos princípios gerais fundamentais de todo o direito, público e privado. Previsto, como um princípio geral, no caput, do art. 6º da Lei, estabelece normas de conduta proba e correta, a serem observadas em todas as etapas procedimentais do tratamento de dados. Assim, tendo em vista, a disparidade estabelecida na relação entre os operadores e os titulares, a boa-fé é de suma importância, na busca pelo equilíbrio dos interesses das partes envolvidas no tratamento dos dados pessoais.

Esse princípio, nesse sentido, refere-se à prática rigorosa de um comportamento leal, correto e probo, nas operações das atividades de tratamento de dados pessoais. Nesse sentido, como um princípio geral do direito, opera como norteador de todos os procedimentos e da aplicação dos demais princípios, ao atuar como um balizador para a interpretação e aplicação de conceitos mais amplos.

Dessa maneira, pode-se afirmar que possui íntima relação com outros princípios previstos nessa legislação, que estabelecem comportamento íntegros e coerentes a serem observados pelos responsáveis pelas operações. A LGPD estabelece, como critérios de segurança, a prevenção, a responsabilização e a prestação de contas<sup>115</sup>, por meio da gestão dos riscos empreendidos na atividade.

Sendo assim, os agentes de tratamento devem ter em vista normas de conduta e de trabalho compatíveis com a finalidade informada, com a proteção das informações e o resguardo pelas informações pessoais, a fim de mitigar os riscos e

---

<sup>115</sup>Relaciona-se com o Inciso X, do art. 6º, da LGPD e diz respeito à necessidade do agente demonstrar que adotou medidas eficazes e capazes de comprovar a observância e o cumprimento das normas e padrões exigidos para a efetiva proteção dos dados pessoais e, também, a eficácia das medidas de segurança utilizadas nas atividades de tratamento de dados pessoais. BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 12 nov. 2021.

os efeitos causados pelos possíveis danos ao direito à privacidade, à vida privada e aos direitos de personalidade dos titulares dos dados pessoais.

### **3.2.1. Princípio da Finalidade, da Adequação, da Necessidade e da Prevenção**

A LGPD, no art. 6º, inciso I, estabelece que o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados previamente aos titulares. Além disso, não é possível tratamento posterior de forma incompatível ou desvirtuada com a finalidade previamente informada.

Nesse sentido, Pestana afirma o seguinte:

Por propósitos legítimos, quer se referir a uma finalidade movida pelo bom senso, razão, legalidade, bons costumes e boa-fé, distanciando-se, portanto, da iniciativa subalterna, emulativa, emocional, ilícita e de má fé.

Refere-se a propósitos específicos, por enfatizar a preocupação de que o tratamento se volte, certamente, para um objetivo determinado relevante para o ser, como se dá ao procurar minorar as repercussões do infarto ou de prolongar a vida no espaço sideral.

Já por propósitos explícitos procura enfatizar o aspecto unívoco do tratamento, ou seja, não admitindo a equivocidade ou ambiguidade. Em outras palavras, tendo o objetivo clara e previamente delineado, não permitindo que dúvidas possam surgir após ser especificado seu conteúdo. 116

Assim, a coleta de dados deve ocorrer de forma específica, conforme a finalidade informada ao titular, bem como, que o tratamento dos dados pessoais se restrinja à finalidade pretendida e informada. Nesse sentido, verifica-se a relação entre os princípios e conceitos gerais previstos nessa Lei, assim, o fornecimento do consentimento. Nesse sentido, havendo mudanças na finalidade para o tratamento em incompatibilidade com o consentimento anteriormente firmado, o art. 9º, parágrafo 2º, estabelece que: “o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.<sup>117</sup>”

---

<sup>116</sup>PESTANA, Márcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 09 nov. 2021.

<sup>117</sup> BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 12 nov. 2021.

Além do mais, relaciona-se com o princípio da retenção mínima, que estabelece coleta e tratamento de dados para finalidades específicas. Assim, quando alcançada a finalidade específica almejada ou, ainda, quando os dados deixam de ser necessários ou pertinentes, nos termos do art. 15, inciso I, da LGPD, é necessária à sua exclusão.

O princípio da adequação, nesse contexto, significa conformidade na relação estabelecida entre o tratamento e a finalidade informada previamente ao titular dos dados. Dessa maneira, o art. 6º, inciso II, da LGPD prevê que os dados sejam tratados em compatibilidade com as finalidades informadas aos titulares, levando em conta o contexto do tratamento.

Nesse sentido, no âmbito da LGPD, Pestana afirma o seguinte:

[...]refere-se ao nexo de pertinência lógica de conformidade que se estabelece entre o tratamento e a finalidade objetivada, tal como previamente informada ao titular.

Estabelece, portanto, relação lógica entre:

- a) o tratamento e a finalidade objetivada;
- b) o tratamento e a comunicação transmitida ao titular;
- c) a finalidade almejada e a comunicação transmitida ao titular; e,
- d) entre os três elementos, integradamente considerados, ou seja, entre o tratamento, a finalidade objetivada e a comunicação transmitida ao titular.<sup>118</sup>

Assim, o resguardo à privacidade e o zelo adequado com o tratamento de dados, em conformidade com a destinação à qual foi previamente informada e consentida pelos titulares, são pressupostos para o tratamento adequado das informações coletadas. Dessa maneira, não é permitida a sua utilização para fins diversos e em contradição com a o propósito previamente acordado.

Além dos mais, o tratamento dos dados, nos termos do art. 6º, III, da LGPD, deve observar as finalidades da atividade e estabelecer um limite ou uma redução da quantidade de dados coletados e tratados. Tendo em vista o mínimo necessário para a realização das finalidades da atividade-fim, com a utilização apenas dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

---

<sup>118</sup>PESTANA, Márcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em 12 de nov de 2021.

A LGPD estabelece, ainda, que os dados sensíveis devem ser processados por órgãos de pesquisa de forma estritamente necessária com os fins de atividade acadêmica e recomenda-se, ainda, o anonimato das informações. Outrossim, o processamento de dados pessoais, para fins de pesquisa em saúde pública, deve ser realizado estritamente de acordo com a necessidade do estudo e os levantamentos devem ser mantidos em ambiente seguro e controlado, de acordo com as boas práticas e empreendimento de técnicas de segurança, incluindo anonimização<sup>119</sup> e pseudoanonimização<sup>120</sup>.

Nesse sentido, PESTANA<sup>121</sup> afirma que “A regra geral, portanto, trazida pela LGPD, é não se realizar o tratamento; a exceção, ao reverso, é a de realizá-la, se e quando o atingimento de determinada finalidade se mostrar relevante para que o tratamento seja realizado.” Assim, somente as informações pertinentes e imprescindíveis para o atingimento da finalidade serão processadas na operação. À vista disso, o autor aponta o seguinte:

A necessidade, ao seu turno, poderá ser compreendida como a adoção de um meio que, a par de preencher o requisito de adequação à finalidade almejada, seja o menos gravoso para o indivíduo e para o interesse público.

---

119ANONIMIZAÇÃO: utilização de meios técnicos razoáveis e disponíveis, no momento do tratamento. Por meio dos quais, um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo (Art. 5º , XI, LGPD). Dessa maneira, por meio da anonimização, as informações são modificadas ou removidas para que o titular não possa ser identificado, inclusive pelo controlador. O dado anonimizado, de acordo com a lei, deixa de ser considerado dado pessoal (Art. 12, caput, LGPD). Assim, a operação voltada a desvincular, na maior medida possível, o dado pessoal de seu(sua) titular. Envolve o emprego de técnicas consideradas razoáveis, observados os protocolos de segurança da informação, para afastar a possibilidade de ataques de inferência, diretos ou indiretos, acerca da titularidade do dado. É importante ressaltar que, pelos ditames da LGPD, para ser considerado dado anonimizado, o processo de anonimização não pode ser revertido por meios próprios ou com esforços razoáveis (Art. 12, caput, LGPD). Caso isso ocorra, considera-se que o dado nunca foi anonimizado. Para determinar o que é razoável, a LGPD leva em conta: i. fatores objetivos: tempo, custo e estado da arte para reversão do processo de anonimização; ii. fatores subjetivos: a própria capacidade do agente de tratamento de dados que, a partir de utilização exclusiva de meios próprios, poderia reidentificar uma base de dados.”. Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo: CEPI-FGV Direito SP, 2021.

120PSEUDONIMIZAÇÃO: tratamento de dados, por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, a não ser que haja o uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (Art. 13, § 4º, LGPD). Consiste em substituir um atributo (tipicamente um atributo único), em um registro, por outro, reduzindo a vinculação de um conjunto de dados com a identidade original de um dado. Não é um método de anonimização. Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo: CEPI-FGV Direito SP, 2021;

121PESTANA, Márcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em 12 nov. 2021.

A Administração Pública em inúmeras circunstâncias interfere no exercício da liberdade e da propriedade dos indivíduos, ora promovendo desapropriações, ora apreendendo alimentos deteriorados, estabelecendo condições para o exercício do comércio etc.

Agora, sua intervenção, de acordo com o princípio da proporcionalidade, deverá dar-se por meio da adoção do ato administrativo mais suave à situação, constituindo-se, portanto, num elemento de intensidade e extensão, de graduação, em outras palavras.<sup>122</sup>

Dessa maneira, compreende-se que esse princípio estabelece a proporcionalidade na manipulação dos dados da pessoa natural. Visando, assim, estabelecer um limite mínimo necessário para a realização da operação de tratamento atingir a finalidade a que se propõe. Com a finalidade de maior resguardo aos direitos de proteção, tendo em vista aquilo que foi previamente informado e acordado pelos titulares dos dados.

O princípio da prevenção está diretamente relacionado com a adoção de práticas preventivas, de adequação a normas, regulamentos, a condutas éticas e probas, por meio de uma política organizacional. Nesse sentido, refere o art. 6º, VIII, da LGPD, que se deve adotar medidas para prevenir a ocorrência de danos em decorrência das operações de tratamento. Assim como, prevenir práticas ilícitas, abusivas ou fraudulentas.

Nesse sentido, Pinheiro ressalta o seguinte:

Da mesma forma que as organizações são responsáveis no caso de incidentes – como vazamentos – no tratamento dos dados, devem aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação das informações. Ainda assim, no caso de qualquer incidente é obrigação da organização notificar as autoridades imediatamente.<sup>123</sup>

Dessa maneira, as práticas de adequação (*compliance* – do verbo *to comply*, que significa adequar) são expressas em um conjunto de procedimento e normas de proteção e governança dos dados que, se observadas pelas empresas, permitem a sua conformidade com as novas exigências impostas pela digitalização da sociedade e os desafios impostos pelas novas legislações protetivas.

---

<sup>122</sup>PESTANA, Márcio. Direito Administrativo Brasileiro, São Paulo: Ed. Atlas, 4ª ed., 2014.

<sup>123</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

Nesse sentido, Gutierrez e Reoloni ressaltam o seguinte:

Empresas que estavam atentas aos padrões globais relacionados à tecnologia da informação (tais como os de segurança da informação e de governança de dados) terão seus controles muito mais próximos do que espera a LGPD, do que aquelas empresas que nunca se preocuparam com esse tipo de controle.<sup>124</sup>

Dessa maneira, os autores referem a boas práticas adotadas por empresas de Tecnologia da Informação (TI), setor que está em constante transformação e há décadas precisa se adequar às exigências de segurança e padrões éticos de conduta. Assim, ferramentas digitais podem ser utilizadas com a finalidade de promover maior segurança e prevenir, detectar e mitigar os riscos envolvidos nas operações de tratamento, de acordo com o seu porte, a complexidade das operações e a estrutura organizacional.

Sendo assim, os autores referem que o setor de TI possui normativas com a finalidade de traçar parâmetros relativos à segurança da informação. Nesse sentido, citam as normas técnicas da Família ISO 27000, relativas ao Sistema de Gestão de Segurança da Informação, especificamente da ISO 27701, que estabelece um padrão internacional, para assegurar a conformidade da organização com as legislações mais modernas sobre proteção de dados, inclusive a LGPD e o RGPD<sup>125</sup>.

### **3.2.2. Princípio do livre acesso, da transparência, da segurança e da qualidade dos dados**

Relacionado com a observância ao dever de informação entre as partes, o art. 6º, inciso IV, da LGPD, estabelece que os titulares tenham a garantia de consulta facilitada e gratuita. Nesse sentido Pinheiro<sup>126</sup> afirma que “têm direito a informações claras e acessíveis do início ao fim do tratamento do dado, podendo revogar o consentimento a qualquer momento.” Dessa maneira, a forma, a duração do

---

<sup>124</sup>GUTIERREZ, Andriei; REOLONI, Carlos. Lições e boas práticas do setor de tecnologia para todas as organizações: segurança e governança de dados. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 11 nov. 2021.

<sup>125</sup>Idem;

<sup>126</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

tratamento e a integralidade de seus dados pessoais fácil acesso, fácil compreensão e, ainda, gratuitamente, mediante requisição do titular.

Além do mais, após a confirmação de existência, o acesso aos dados pessoais, nos termos do art. 19, da LGPD, a entrega pode ser sob forma impressa ou por meio eletrônico. Dessa maneira, o formato da entrega poderá ser de forma simplificada, imediatamente ou, ainda, por meio de declaração clara e completa, indicando a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, com observância aos segredos comercial e industrial, no prazo de até 15 (quinze) dias, a contar da data do requerimento do titular. Assim, é possível afirmar que a previsão do direito ao livre acesso possui relação com a preocupação da Lei em “garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade.”<sup>127</sup>

Ademais, quando a lei estabelece a qualidade dos dados, refere-se à garantia, nos termos do art. 6º, V, da LGPD, aos titulares dos dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Nesse sentido, diz respeito à maneira como os dados disponíveis são manipulados e está relacionado ao conceito de governança de dados, que se refere ao conjunto de boas práticas empresariais. Nesse sentido, a organização deve adotar políticas e padrões de procedimento que impliquem em um ambiente organizado e seguro, a fim de garantir maior eficiência no atingimento dos resultados esperados diante da operação de tratamento e a privacidade e integridade dos dados.

Nesse sentido, Pestana ressalta o seguinte:

A exatidão nos remete à ideia de precisão, do liame estrito estabelecido entre dados, tratamento e finalidade; clareza, por sua vez, associa-se à noção de que tal relação seja assentada em palavras e procedimentos que, indubitavelmente, esclareçam os destinatários da mensagem, sobretudo a pessoa natural titular dos dados a serem tratados, assim como para que se voltem, certamente, para o resultado almejado; relevância, à sua vez, indica que o tratamento em questão somente será realizado, caso tal proceder permita atingir-se a finalidade previamente objetivada e, também, que, antecipadamente, tenha sido aprovada pelo titular do dados; finalmente, atualização é o elemento que, de pronto, enfatiza o aspecto temporal e dinâmico dos dados, nos remetendo à ideia de

---

127PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

que, não obstante tenham sido recolhidos e fixados num determinado átimo, é compreensível que a dinâmica da realidade da vida promova modificações em tais dados, o que exige a sua constante atualização.<sup>128</sup>

Outrossim, a Lei estabelece o princípio da transparência, o qual relaciona-se, com os princípios anteriores, na medida em que representa, nos termos do art. 6º, VI, da LGPD, a garantia dos titulares dos dados, de obter informações claras, precisas e facilmente acessíveis, referentes à realização do tratamento, ao compartilhamento das informações com terceiros, aos agentes de tratamento, com observância aos segredos comerciais e industriais. Dessa maneira, a Lei buscou conferir maior transparência, não apenas em relação ao tratamento dos dados, mas também em relação aos agentes que participaram da operação.

Nesse sentido, Pinheiro afirma o seguinte:

Do consentimento ao fornecimento de dados ao término do tratamento dos dados, as informações acerca do processo devem ser claras, acessíveis e adequadas à linguagem e compreensão do usuário, de forma que o seu consentimento possa ser revogado a qualquer momento. O consentimento do usuário deve ser realizado por escrito ou de qualquer outro modo que demonstre a sua livre manifestação da vontade.<sup>129</sup>

Dessa maneira, compreende-se que a efetiva observância às políticas de privacidade e proteção de dados e o estabelecimento de regras claras e precisas aos agentes, venha conferir maior segurança aos usuários das redes e às relações estabelecidas no meio digital, em relação à coleta, ao armazenamento, ao compartilhamento e ao tratamento dos seus dados pessoais. Tendo em vista que as empresas, tanto do setor público quanto do setor privado, devem garantir informações claras, precisas e de fácil acesso e, ainda, informar de que maneira serão realizadas as operações e a finalidade almejada.

Da mesma maneira, previsto no art. 6º, inciso VII, da LGPD, do princípio da segurança, compreende-se que os agentes responsáveis pelas operações de tratamento devem fazer uso de medidas técnicas e administrativas adequadas à

---

<sup>128</sup>PESTANA, Márcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em 12 de nov de 2021.

<sup>129</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

proteção das informações pessoais contra acessos não autorizados de terceiros e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Nesse sentido, Gutierrez e Reoloni ressaltam o seguinte:

Cuidar e proteger a informação é uma prioridade para o setor de Tecnologia da Informação (TI), que vem amadurecendo há décadas. Com a transformação digital de todas as outras organizações do País, é interessante observar como as boas práticas e os conceitos de segurança e governança de dados do setor de TI passam a ser “importados” para esses outros setores.<sup>130</sup>

Sendo assim, compreende-se que as organizações responsáveis pelo tratamento devem dispor de métodos e procedimentos seguros e eficientes, para monitorar a internet em busca de possíveis violações e reduzir os riscos da atividade. Assim como, promover o fortalecimento da cultura interna de proteção e de boas práticas empresariais.

### **3.2.3. Da não-discriminação e da prestação de contas (*accountability*)**

A LGPD reconhece de forma explícita o princípio da não discriminação como um princípio fundamental de proteção de dados. Assim, pode ser compreendido como fundamento de todo o processo para um tratamento justo de dados pessoais, diante da vedação à realização do processamento para fins discriminatórios, ilícitos ou abusivos<sup>131</sup>.

Dessa maneira, ao estabelecer proibição à realização do tratamento para esses fins, conforme disposto no art. 6º, IX, em todas as circunstâncias, o uso de dados, sejam sensíveis ou, ainda, aqueles que possam ocasionar a indução a resultados segregativos, observem procedimentos e padrões éticos e equitativos.

Nesse sentido, a exemplo do RGPD, a LGPD trata das revisões das decisões tomadas nos tratamentos de dados pessoais sensíveis ao determinar que:

---

130GUTIERREZ, Andriei; REOLONI, Carlos. Lições e boas práticas do setor de tecnologia para todas as organizações: segurança e governança de dados. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 11 nov. 2021.

<sup>131</sup>Princípios da LGPD”. In: Governo Federal. Acesso à Informação. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd>; Acesso em: 11 nov. 2021;

Art.20 – O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. 132

Nesse sentido, o perfilamento (*profiling*), implica o tratamento de dados pessoais com objetivo de delinear o perfil comportamental, profissional, de consumo e de crédito dos titulares de dados, por meio de operações como cruzamento de dados, agregação de dados, parametrização, enriquecimento de dados<sup>133</sup> etc. Dessa, forma, a tomada de decisões pelos algoritmos e sistemas de processamento podem favorecer a discriminação dos titulares, restringindo-lhes as suas liberdades democráticas, como o acesso aos direitos sociais, à saúde, ao trabalho e às políticas públicas, de moradia e de consumo, de crédito.

Cumprir salientar que este trabalho não visa pôr à proteção de dados pessoais contra à utilização das tecnologias da informação e os avanços tecnológicos. Mas sim, ressaltar a importância de que sejam adotadas boas práticas, tanto para a implementação de uma cultura organizacional, pautada em princípios éticos e probos, quanto para o desenvolvimento de *softwares* e algoritmos com um maior nível de transparência e equidade, por meio de métodos de tratamento que atentem a fins éticos e não discriminatórios.

Além disso, por meio do art. 6º, X, a LGPD, exprime a necessidade de os agentes demonstrarem a 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. No RGPD, tal princípio encontra previsão no art. 5.2, referido como *accountability*<sup>134</sup> e é compreendido como a responsabilidade do controlador de demonstrar que está em conformidade com as normas e princípios sobre proteção de dados.

Nesse sentido, Leal refere o seguinte:

---

<sup>132</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 10 nov. 2021.

<sup>133</sup>Refere-se ao processo de combinação dos dados pessoais entre as informações constantes em duas ou mais bases de dados. Dessa forma, envolve o acréscimo de informações sobre o titular pela combinação de dados de uma fonte externa.

<sup>134</sup>5.2. “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)” in PARLAMENTO EUROPEU. *General Data Protection Regulation (GDPR)*. Disponível em: <https://gdpr-info.eu/art-5-gdpr/> Acesso em: 17 nov 2021;

[...]a partir dos princípios que norteiam a LGPD, a figura do *accountability* (artigo 6º, X, da LGPD) torna-se instrumento capaz de garantir as finalidades pelas quais os dados pessoais foram originalmente coletados, dando-lhes destinação de acordo com a finalidade, a adequação, a segurança e a prevenção, as quais são princípios de observância obrigatória na execução da LGPD, que toma o *compliance* (artigo 46, § 1º c/c artigo 49, ambos da LGPD) como seu mecanismo de governança, aptos a resguardar o direito à privacidade enquanto não promulgada a legislação específica (artigo 4º, § 1º, da LGPD) e de observância obrigatória quando da sua regulamentação.<sup>135</sup>

Assim, para a implementação de boas práticas de governança de dados, a implementação de um sistema de *compliance* eficaz é de suma importância. Dessa maneira, a organização deve estabelecer e fornecer os meios para o desenvolvimento e implementação de sistemas efetivos, capazes de avaliar os riscos e, ainda, implementar melhorias contínuas nos sistemas de gestão, de acordo com sua capacidade e necessidade.

Sendo assim, é possível afirmar que as boas práticas perpassam por uma estrutura organizacional capaz de avaliar os riscos e a eficácia das medidas adotadas. Assim como, as organizações ofereçam treinamento aos responsáveis e promovam uma cultura de proteção aos dados coletados, processados e tratados. Nesse sentido, é possível afirmar que uma empresa que já adotasse, antes da LGPD, práticas coerentes, probas e éticas, assim como, promovam uma cultura organizacional em conformidade, terão menos dificuldades em se adequar às novas imposições.

### **3.2.4 Consentimento e o legítimo interesse**

O estudo das bases legais é necessário para a compreensão dos fundamentos que autorizam as operações de tratamento de dados pessoais e de tratamento de dados pessoais sensíveis pelos agentes. Assim, o consentimento dos titulares dos dados é imprescindível para a compreensão da matéria, uma vez que, por meio desse, legitima-se as operações de tratamento. Além disso, somente não será exigido o consentimento nas hipóteses em que não se aplica a LGPD, como

---

<sup>135</sup>LEAL, Dionis Janner. Governança no compartilhamento de dados pessoais entre órgãos da administração pública: *accountability* e *compliance* como instrumentos de controle e gestão. Disponível em: [https://www.imed.edu.br/Uploads/DISSERTA%C3%87%C3%83O\\_GOVERNAN%C3%87A\\_parcial\\_IMED.pdf](https://www.imed.edu.br/Uploads/DISSERTA%C3%87%C3%83O_GOVERNAN%C3%87A_parcial_IMED.pdf). Acesso em: 16 nov. 2021;

aquelas elencadas no art.4º da Lei, nas hipóteses de tratamento de dados anonimizados ou de tratamento fundamentado no interesse público.

Assim, nos termos do art. 5º, inciso XII, da LGPD, o consentimento é conceituado como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Além disso, no art. 7º, I, da LGPD, consta como um dos requisitos para o tratamento de dados.

Nesse sentido, possui estrita relação com a autodeterminação informativa, na medida em que:

A autodeterminação informacional consiste, em suma, na perspectiva de que o indivíduo deve controlar (autodeterminar) os seus dados pessoais (informações pessoais: autodeterminação informacional), exigindo-se, por isso, o consentimento do titular das informações pessoais para que elas sejam coletadas, processadas e compartilhadas. A terminologia surgiu no julgamento paradigmático do Tribunal Constitucional Alemão, em 1983, que considerou, parcialmente, inconstitucional a lei de recenseamento que não delimitava a finalidade para a qual os dados pessoais dos cidadãos seriam utilizados, permitindo-se, ainda, o seu cruzamento com dados de registros públicos e a sua transferência para outras unidades da administração pública, esvaziando, assim, qualquer perspectiva de controle por parte dos cidadãos sob seus dados pessoais.<sup>136</sup>

Dessa maneira, o consentimento do usuário é tido como um dos fundamentos para o tratamento dos dados. Além disso, deve ser livre, informado e inequívoco e anterior à coleta e uso dos dados pessoais, podendo ainda ser revogado a qualquer tempo, conforme disposto no art. 7º, parágrafo 1º, da LGPD. Ademais, a política de proteção de dados deve ser disposta em linguagem compreensível e a coleta deve se limitar apenas aos dados que forem essenciais ao funcionamento do serviço.

Nesse sentido, o professor Ingo SARLET<sup>137</sup> afirma que "O consentimento livre e informado é, nesse sentido e contexto, exigência constitucional estrita para o exercício da autodeterminação informacional, integrando, de tal sorte, o próprio conteúdo essencial do direito fundamental."

---

<sup>136</sup>MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevideu: Fundação Konrad Adenauer, 2005. p. 233-245;

<sup>137</sup>SARLET, Ingo Wolfgang. Fundamentos de um direito fundamental à proteção de dados. In: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

Além disso, possibilita que os usuários possam solicitar relatórios sobre os dados coletados, a correção de informações e que as informações sejam apagadas, por meio do reconhecido “direito ao esquecimento.” Nesse sentido, Cueva afirma o seguinte:

O direito ao esquecimento, ou o direito a ser esquecido, origina-se na proteção da intimidade e da vida privada e tem sido invocado, sobretudo no mundo digital, como direito ao apagamento de dados pessoais no contexto da internet, mas também no contexto da mídia em geral, como direito à não veiculação de informação desprovida de atualidade e relevância para o público, mas ofensiva ao interessado.<sup>138</sup>

Dessa forma, o consentimento refere-se à manifestação, nos termos do art. 5º, inciso XII, LGPD, por meio da qual o titular concorda que seus dados pessoais sejam tratados para determinada finalidade, que deverá ser informada de forma clara e inequivocadamente. Dessa maneira, o consentimento deverá ser fornecido por escrito ou por outro meio, nos termos do art. 8º, da LGPD, que demonstre a manifestação de vontade do titular. Assim, a finalidade do tratamento deverá ser apontada expressamente, no que se refere à coleta, ao uso, ao armazenamento e qualquer outra operação de tratamento dos pessoais, de forma destacada das demais cláusulas contratuais, conforme preceituado no art. 7º, inciso IX, da Lei n. 12.965/2014 — Marco Civil da Internet.

Além disso, quando se refere que deverá ser livre, compreende-se que, por meio da leitura do parágrafo 1º, do art. 8º, será considerado nulo, nos casos em que as informações fornecidas aos titulares tenham apresentado conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Nesse sentido, refere-se às situações em que não existe qualquer vício de consentimento, quanto à concordância do titular para o tratamento dos seus dados pessoais.

Além do mais, as informações devem ser apresentadas de maneira objetiva, clara e precisa, com linguagem de fácil compreensão e de maneira específica quanto às finalidades do tratamento, assim, informações imprecisas ou genéricas podem anular o consentimento. Dessa forma, a declaração de vontade deve ser

---

<sup>138</sup>SARLET, Ingo Wolfgang. Fundamentos de um direito fundamental à proteção de dados. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

apresentada de maneira inequívoca pelo titular, de maneira expressa e espontânea, podendo, ainda, discordar e requerer a revisão do seu consentimento e a exclusão dos dados coletados e utilizados para finalidade diversa daquela previamente acordada. À vista disso, afirma-se que não é admitido o consentimento presumido para as operações de tratamento.

Ademais, cumpre salientar que a LGPD prevê situações em que o consentimento é dispensado. Nesse sentido, o art. 7º, da LGPD, dispõe o seguinte

II – Para o cumprimento de obrigação legal ou regulatória pelo controlador;<sup>139</sup>

III – Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;<sup>140</sup>

IV – Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;<sup>141</sup>

V – Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;<sup>142</sup>

---

139Sobre o tema, VIOLA e TEFFÉ ressaltam o seguinte: “[...]o tratamento de dados pessoais poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador, como obrigações trabalhistas, deveres oriundos da lei anticorrupção e a guarda de registros por determinados provedores na forma do Marco Civil da Internet.” VIOLA, Mario. TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

140Referente a isso, VIOLA e TEFFÉ afirmam o seguinte “[...]o tratamento de dados pessoais pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres [...]As políticas em questão podem envolver, por exemplo, a implementação de saneamento básico, de auxílios a cidadãos em situação de vulnerabilidade ou de projetos voltados à educação de crianças e adolescentes.[...]deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: a) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e b) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.”. IDEM

141Nesse sentido, VIOLA e TEFFÉ asseveram o seguinte “Pode-se também tratar dados para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Dispõe a lei, em seu Art. 5.º, XVIII, que órgão de pesquisa representa “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.” IDEM;

142 Nesse contexto VIOLA e TEFFÉ ressaltam o seguinte “Outra hipótese autorizativa do tratamento de dados estará presente quando for necessário legitimar a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. A disposição em questão é mais ampla do que aquela prevista no art. 11, II, “d”, da LGPD, podendo o agente tratar, sem consentimento, os dados que são necessários para a contratação,

VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;<sup>143</sup>

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;<sup>144</sup>

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;(Redação dada pela Lei nº 13.853, de 2019)

IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.<sup>145</sup>

Não obstante, compreende-se que devido às complexas relações estabelecidas na *internet* e o seu uso e dependência em diversas esferas da vida cotidiana, uma questão suscitada frequentemente pela doutrina acerca da proteção de dados, diz respeito à insuficiência do consentimento para a integral e efetiva proteção dos direitos dos titulares. À vista disso, Mendes e Fonseca<sup>146</sup> afirmam que as limitações cognitivas dos usuários em compreender e avaliar os riscos aos seus direitos de personalidade, devido à complexidade e utilização de linguagem técnica nos termos de privacidade. Assim como, na maioria dos casos, a utilização dos

---

bastando que o titular seja parte ou esteja em tratativas para um contrato. É possível trabalhar, aqui, dois exemplos: a) nas situações em que o titular adquira produtos ou serviços para entregá-los será preciso conhecer o nome completo, o endereço e outras informações de contato do consumidor e b) levantamentos realizados por instituições financeiras em relação a determinada pessoa, anteriormente à concessão de crédito a ela.” IDEM;

143 À vista disso, VIOLA e TEFFÉ ressaltam o seguinte “O tratamento também pode ter como base o exercício regular de direitos em processo judicial, administrativo ou arbitral (nos termos da Lei 9.307/1996). Há, aqui, base legal ampla que autoriza o uso de dados pessoais em processos para garantir o direito de produção de provas de uma parte contra a outra. O exercício regular de direitos compreende ações do cidadão comum autorizadas pela existência de direito definido em lei e condicionadas à regularidade do exercício desse direito. Dentro dessa hipótese, não pode haver conduta abusiva ou o desempenho disfuncional de certa posição jurídica pela parte.” IDEM;

144 Sobre o tema, VIOLA e TEFFÉ ressaltam o seguinte “[...]tutela-se ainda a proteção da vida ou da incolumidade física do titular ou de terceiro. A aplicação da hipótese parece ser razoável em situações excepcionais e pontualmente, não sendo cabível para justificar ações genéricas. Recordase o seguinte exemplo: obtenção de dados de geolocalização de celulares visando a encontrar pessoas desaparecidas em desastres e escombros ou que possam ter sido sequestradas ou estar perdidas. Outra aplicação dessa base poderia ser para o tratamento de dados importantes para se conter o avanço de epidemias, como o recente caso do Covid-19”; Idem;

145 Nesse contexto, VIOLA e TEFFÉ afirmam o que segue: “Por fim, a última base legal para o tratamento de dados [não sensíveis] refere-se à proteção do crédito. Espera-se que, por meio dela, os tratamentos realizados busquem ampliar e facilitar a concessão de crédito, melhorar as análises de risco e impulsionar o mercado de consumo. Nesse caso, a base deverá estar em constante diálogo com normas como o Código de Defesa do Consumidor (Lei 8.078/1990), a Lei do Cadastro Positivo (Lei 12.414/2011) e portarias do Ministério da Justiça.” Idem;

146 MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

serviços está condicionada ao consentimento dos titulares, sem o qual não podem acessar ou fazer uso das funcionalidades e das conexões que, por exemplo, as redes sociais permitem. Além dos mais, referem que a utilização de técnicas complexas de processamento de dados e de bancos de dados impossibilitam aos usuários mensurar as possibilidades de uso das suas informações pessoais.

Dessa forma, ressalta-se o seguinte:

Novos riscos e maneiras de explorar os dados pessoais demonstram que a proteção de dados deve englobar parâmetros de legitimidade mais amplos do que a existência de um consentimento individual prévio, levando em consideração a compatibilidade entre o contexto da relação e as características do tratamento. Não sendo mero “cheque em branco”, o consentimento inicialmente expressado é analisado posteriormente de acordo com as “legítimas expectativas” para o contexto daquele tratamento.

Essas “legítimas expectativas” passam a ser avaliadas a partir de elementos como: (i) o contexto em que a suposta violação ocorreu (qual era o ambiente social que estruturava o fluxo de informações analisado?); (ii) os atores envolvidos (quem eram os emissores, receptores e sujeitos do fluxo de informação?); (iii) os atributos da informação analisada (com que tipo de informação se estava lidando? Informações médicas, bancárias, preferências pessoais?); (iv) os princípios de transmissão aplicáveis (quais eram os constrangimentos aplicáveis ao fluxo de informações analisado, ele estava condicionado à confidencialidade, reciprocidade, necessidade?).<sup>147</sup>

Entretanto, este trabalho não tem o intuito de adentrar-se nas questões referentes aos limites e problemas envolvidos no consentimento. Dessa forma, reitera-se que para que o tratamento seja considerado adequado, a Lei Geral de Proteção de Dados prevê que a manifestação da vontade do titular deve ser livre, informada e inequívoca, bem como, ter em vista uma finalidade determinada para a coleta e operações de tratamento de dados pessoais, que deve ser especificada de maneira explícita e específica.

Além do mais, o interesse legítimo do controlador ou de terceiros, refere-se às hipóteses em que o tratamento é necessário para atender aos interesses da atividade-fim, conforme hipóteses previstas no art. 7º, IX, LGPD. Ressalta-se, ainda, que essa base legal não legitima a utilização em detrimento aos direitos e liberdades fundamentais dos titulares dos dados pessoais. Nesse sentido, compreende-se que

---

<sup>147</sup>MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

o legítimo interesse somente deve ser utilizado para fundamentar o tratamento em vista de legítimas finalidades e somente autoriza o uso dos dados estritamente necessários para o atingimento da finalidade. Considerado em vista das situações concretas, que incluem, mas não se limitam, ao apoio e promoção de atividades do controlador e a proteção do exercício regular dos direitos dos titulares e a prestação de serviços que lhe tragam benefícios, conforme disposto no art. 10, da LGPD.

Além disso, prevê que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados e a ANPD poderá solicitar, ao controlador, relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, com observância aos segredos comercial e industrial. Assim, compreende-se que deve ser realizado um teste de proporcionalidade, previamente à operação de tratamento, para a avaliação do legítimo interesse, com base nos seguintes critérios:

- I – Se o tratamento de dados pessoais possui uma finalidade legítima;
- II – Se não existem outras estratégias que utilizem uma menor quantidade ou que independam de dados pessoais;
- III – um balanço de riscos avaliando a natureza da relação;
- IV – As expectativas razoáveis do titular; e
- V – Os efetivos resultados diante de suas garantias fundamentais e liberdades civis.<sup>148</sup>

### **3.3. Agentes de tratamento de dados pessoais**

A compreensão da LGPD perpassa pela conceituação dos sujeitos envolvidos no tratamento de dados. Nesse contexto, conforme o art. 5º, V, o titular de dados refere-se à pessoa natural cujos dados pessoais são objeto de tratamento.

Ademais, o setor acadêmico refere-se às organizações de cunho educacional, científico e tecnológico que utilizam dados pessoais para fins de pesquisa acadêmica e científica. Assim como, o setor público refere-se ao Poder Público, às empresas públicas e os órgãos da administração direta e indireta, que utilizam informações pessoais para fins próprios da atividade. Além disso, o setor público não-estatal refere-se ao conjunto de entidades da sociedade civil, que presta

---

<sup>148</sup>Proteção de dados pessoais [recurso eletrônico] : glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo: CEPI-FGV Direito SP, 2021;

atividades de relevância pública, sem fins lucrativos, também chamado de terceiro setor.

Nesse contexto, ressalta-se o seguinte:

O setor público e o privado, assim como o terceiro setor, estão em alta demanda por projetos de adequação à LGPD e esse cenário tem gerado oportunidades de negócios para escritórios jurídicos e consultorias especializadas no tema. Dessa forma, o desenvolvimento e concepção de uma metodologia madura, assertiva e contendo boas práticas para implantação de projetos que exijam conhecimento sobre essa lei é um fator altamente requerido para propiciar uma agilidade no diagnóstico e a obtenção de êxito nesse novo mercado, fazendo que os clientes que demandem essa atuação, mitiguem os riscos.<sup>149</sup>

Ademais, no art. 5º, IX, da Lei, define-se os agentes de tratamento, que são o controlador e o operador de dados pessoais, podendo ser pessoas naturais ou jurídicas, de direito público ou privado. A Autoridade Nacional de Proteção de Dados (ANPD) ressalta que os agentes de tratamento devem ser definidos a partir de seu caráter institucional. Dessa maneira, afirmam que não podem ser considerados controladores ou operadores os indivíduos que sejam subordinados ao poder diretivo do agente de tratamento, tais como funcionários, servidores públicos ou as equipes de trabalho de uma organização.<sup>150</sup>

### 3.3.1. Controlador e operador

O controlador possui a competência referente às decisões acerca das operações de tratamento de dados pessoais e por definir a finalidade destas operações. Dessa forma, conforme art. 5º, VI, da Lei, refere-se à pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, ou seja, é quem determina como os dados são

---

<sup>149</sup>CELIDONIO, T.; NEVES, P.S.; DONÁ, C.M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil nº 13.709/18) e sua adequação perante a lei em uma instituição financeira. Um estudo de caso. Revista *Brazilian Journals of Business*, Curitiba, v.2, n. 4, p.3626-3648 out./dez. 2020. Disponível em: <<https://www.brazilianjournals.com/index.php/BJB/article/view/18382>>. Acesso em: 18 de nov de 2021.

<sup>150</sup>BRASIL. Autoridade Nacional de Proteção de Dados. (ANPD). Acesso à Informação. Governo Federal. Presidência da República. Guia Orientativo para Definições dos Agentes de Tratamentos de Dados Pessoais e do Encarregado. p. 5. Disponível em: [https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento\\_final.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf) . Acesso em 17 de nov de 2021;

processados e passa as instruções ao operador. Além disso, compete ao controlador elaborar relatório de impacto à proteção de dados pessoais, nos termos do art. 38, da LGPD; comprovar que o consentimento foi obtido em conformidade com às exigências legais, nos termos do art. 8º §2º, da LGPD; comunicar à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidentes de segurança, conforme disposto no art. 48, da LGPD;

Além disso, esse controle pode ser exercido de forma compartilhada, no caso em que dois ou mais agentes são responsáveis pelas decisões. Dessa maneira, quando decorram danos aos titulares das operações de tratamento, ambos respondem solidariamente, conforme disposto no art. 42, §1], II, exceto nas hipóteses do art. 43. Dessa forma, os agentes somente deixaram de ser responsabilizados nas hipóteses elencadas no art. 43, LGPD, quais sejam: I) quando provarem não terem participado do tratamento que lhes é atribuído; II) quando provarem que não violaram as legislações que disciplinam a proteção de dados; III) que o dano decorre de culpa exclusiva do titular dos dados ou de terceiros. No que se refere à indenização, aquele que reparar o dano, nos termos do §4º, do art. 42, tem direito de regresso contra os demais responsáveis, de acordo com a sua participação no evento danoso.

Além dos mais, o art. 5º, VII, da LGPD, dispõe sobre a figura do operador, que é a pessoa natural ou jurídica, de direito público ou privado, responsável pelo tratamento de dados pessoais em nome do controlador, ou seja, quem executa, a mando do controlador, as determinações acerca da forma como os dados devem ser tratados, conforme a finalidade por ele delimitada. Assim, é possível afirmar que a diferença na figura do operador e na do controlador, reside no poder de decisão, ou seja, o operador somente pode agir de acordo com as finalidades determinadas pelo controlador.

Dessa maneira, cabe destacar, entre as obrigações do operador as seguintes:

- I – Seguir as instruções do controlador;
- II – Firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;
- III – Dar ciência ao controlador em caso de contrato com suboperador.<sup>151</sup>

---

151BRASIL. Autoridade Nacional de Proteção de Dados. (ANPD). Acesso à Informação. Governo Federal. Presidência da República. Guia Orientativo para Definições dos Agentes de Tratamentos de

Embora o controlador seja o principal responsável pelo tratamento e o operador apenas atue sob suas ordens, o art. 37 da LGPD, prevê obrigações e responsabilidades compartilhadas, como de manter o registro das operações. Além do mais, o art. 42, prevê a responsabilidade solidária, em razão da atividade de tratamento de dados pessoais que resulte em prejuízo patrimoniais, morais, individuais ou coletivos. Nesse sentido, o tratamento irregular é considerado aquele que realiza em inobservância aos preceitos das legislações sobre proteção de dados pessoais ou quando observar parâmetros de segurança esperados, dentre os quais, aponta-se o modo que foi realizado, os resultados e os riscos esperados e as técnicas de tratamento disponíveis à época em que foi realizado.<sup>152</sup>

### 3.3.2. Encarregado (DPO)

Ademais, o encarregado (no RGPD referido como *Data Protection Officer*) é a pessoa indicada pelo controlador que atua como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados. Nesse sentido, o DPO, conforme disposto no art. 5º, VIII e art. 41, *caput*, LGPD, deverá ser indicado pelos controladores e pelos operadores e a sua identidade e suas informações de contato deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador, conforme disposto expressamente no art. 41, § 1º, da LGPD. Nesse contexto, o encarregado é responsável pelas seguintes atividades:

- Art. 41, § 2º - As atividades do encarregado consistem em:
- I - Aceitar reclamações e comunicações dos(as) titulares, prestar esclarecimentos e adotar providências;
  - II - Receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
  - III - orientar os(as) funcionários(as) e os(as) contratados(as) da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.<sup>153</sup>

Dessa maneira, é possível afirmar que o encarregado é responsável por garantir a conformidade de uma organização aos preceitos da LGPD. Nesse sentido, é importante que o encarregado tenha recursos adequados e liberdade para a realização de suas atividades, bem como, disponha de conhecimentos acerca de proteção de dados e segurança da informação em nível adequado às exigências e à complexidade das operações realizadas pela organização.

Nesse sentido, Pinheiro ressalta o seguinte:

O encarregado, também chamado de Data Protection Officer (DPO), pode ser tanto uma pessoa física como uma pessoa jurídica, interno ou externo, individual ou atuando de forma colegiada como em um comitê.

Portanto, é possível nomear um colaborador interno para ocupar essa posição, assim como é possível contratar uma empresa que preste este tipo de serviço, conhecido por “DPO as a service”.<sup>154</sup>

Ademais, o art. 41, § 3º, estabelece que a Autoridade Nacional estabelecerá normas complementares, detalhando as atribuições do encarregado, inclusive, das hipóteses de dispensa exigibilidade de sua indicação, tendo em vista a natureza e o porte da organização ou o volume e complexidade das operações de tratamento de dados.<sup>155</sup>

#### **4. ADEQUAÇÃO, RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS**

A organização deve promover práticas pautadas em princípios éticos e probos, em estrita observância às boas práticas em governança de dados e segurança da informação, as quais devem ser atualizadas constantemente, diante de novos regulamentos, internos e externos, normas e padrões técnicos disponíveis e adequados à complexidade da atividade. Além do mais, cabe às

---

<sup>153</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 18 nov. 2021;

<sup>154</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018. São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021;

<sup>155</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 20 nov de 2021;

organizações oferecer treinamento e aperfeiçoamento qualificados ao seu quadro funcional, conforme as normas e os procedimentos mais adequados à complexidade e ao risco das operações.

Assim, ressaltamos que as organizações que já possuem, em suas operações técnicas, a promoção de boas práticas de governança em privacidade e uma cultura organizacional protetiva das informações dos clientes, terão menos dificuldades em se adequarem às novas legislações a respeito do tema. Nesse sentido, anteriormente, verificamos a adoção de procedimentos técnicos já existentes e de normas técnicas setoriais, como aquelas da família ISO 27000, que representam normas técnicas procedimentais, que adotam padrões internacionais em segurança da informação. Especificamente a norma ISO 27701, alinhada como as inovações trazidas pela LGPD e o Regulamento Europeu.

Nesse sentido, é possível afirmar que, ao adotar ferramentas eficazes e promover uma cultura de proteção de dados, as organizações estarão um passo à frente em atender às necessidades de adequação impostas pela LGPD, resultando em maior confiabilidade e competitividade no mercado. Dessa maneira, a adequação digital é capaz de reduzir as dificuldades impostas e a sobrecarga de trabalho por parte dos agentes de tratamento. Ao promover um ambiente mais simplificado e eficaz.

Além do mais, ressalta-se que as consequências da não adequação podem ocasionar danos, não apenas de cunho pecuniário, mas também, à imagem da organização, por meio da perda de confiabilidade, de clientes e de oportunidades de negócio. Assim, verifica-se que, a médio e longo prazo, a adequação empresarial e organizacional, tende a trazer inúmeros benefícios às organizações, ao conferir maior confiabilidade e segurança jurídica aos titulares de dados, assim como, da simplificação dos procedimentos de conformidade, resultando, assim, em maior competitividade e confiança à organização.

#### **4.1. Adequação das operações de tratamento à LGPD**

A globalização e os processos de transformação da sociedade e da digitalização dos diversos aspectos da vida cotiada trouxeram à tona novos modelos

de negócios. Nesse contexto, a economia passou por profundas transformações e os dados tornaram-se os mais valiosos ativos econômicos da sociedade da informação. Dessa maneira, a influência digital na vida cotidiana deflagrou violações ao direito à privacidade e a inferências na vida privada dos indivíduos, diante dos episódios frequentes de vazamentos de dados dos usuários das redes. Compreende-se, assim, que as novas tecnologias de captação, processamento e transmissão de dados trouxeram à luz a urgência de uma necessária regulamentação e fiscalização por parte dos ordenamentos jurídicos e de maior conformidade por parte das organizações responsáveis por essas operações.

Nesse sentido, Lósio e Santos ressaltam o seguinte:

O cenário provocado pela transformação digital e pela necessidade de uma cultura de proteção de dados é um desafio que pessoas físicas ou jurídicas, tanto do direito público quanto privado, precisam inserir em suas políticas, controles e processos presentes no tratamento de dados, em face da necessidade de alcançar as boas práticas de governança.<sup>156</sup>

Assim, a disciplina acerca da proteção de dados começou a ganhar força, diante de uma tendência global sobre a necessidade de assegurar a titularidade e a proteção dos dados pessoais dos indivíduos, considerados uma extensão de sua personalidade, ao serem capazes de traçar os seus padrões de comportamento, seu perfil profissional, de consumo, de saúde, dentre outros. Dessa maneira, evidenciou-se a necessidade de aperfeiçoamento de instrumentos capazes de fiscalizar as práticas de ilícitos e das instituições implementarem meios capazes de coibir as práticas e punir os responsáveis.

Nesse sentido, Pinheiro ressalta o seguinte:

Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de *compliance* digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos

---

<sup>156</sup>LÓSSIO, Claudio Joel Brito. SANTOS, Coriolano Aurélio Almeida Camargo. A confidencialidade e a lei geral de proteção de dados. in DE, LIMA, Ana Paula Moraes. C. LGPD Aplicada. São Paulo: Grupo GEN, 2021. 9788597026931. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 11 nov. 2021.

de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura.<sup>157</sup>

Além disso, as organizações devem adotar práticas preventivas, de adequação às normas e aos regulamentos, por meio da adoção de condutas éticas e probas e de uma política interna de boas práticas de governança dos dados pessoais dos titulares e de minimização dos riscos das atividades de tratamento. Dessa maneira, as práticas de adequação (*compliance* – do verbo *to comply*, que significa adequar) são expressas em um conjunto de procedimento e normas de proteção e governança dos dados que permitem a sua conformidade com as exigências impostas pela digitalização da sociedade e os preceitos e exigências das novas legislações protetivas de dados.

Nesse contexto, Lósio e Santos ressaltam o seguinte:

[...]a transmissão de valores relacionados às boas práticas de proteção de dados é fundamental para que organizações minimizem os riscos relacionados a incidentes de segurança da informação, até pelo fato de que não existe a plenitude de segurança, mas o máximo que deve ser feito para que as boas práticas de governança em proteção de dados sejam atingidas.<sup>158</sup>

Diante disso, esse trabalho buscou analisar as novas exigências impostas pelo mercado digital de dados, que impulsionou o surgimento do Regulamento Geral sobre Proteção de Dados da União Europeia e às suas influências no surgimento de legislações semelhantes ao redor do mundo, especificamente, em vista da Lei Geral de Proteção. Nesse sentido, A LGPD reconhece a responsabilidade e a prestação de contas (*accountability*) como princípios fundamentais de proteção de dados. Em art. 6º, X, estabelece a responsabilidade dos agentes pela demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das regras de proteção de dados pessoais, incluindo a eficácia de tais medidas.

Dessa maneira, a LGPD impõe aos controladores e processadores a adoção de processos e políticas internas que garantam a ampla conformidade com as

---

<sup>157</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021

<sup>158</sup>LÓSSIO, Claudio Joel Brito. SANTOS, Coriolano Aurélio Almeida Camargo. A confidencialidade e a lei geral de proteção de dados *in* DE, LIMA. Ana Paula Moraes. C. LGPD Aplicada. São Paulo: Grupo GEN, 2021. 9788597026931. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 11 nov. 2021.

regras de boas práticas, diante da necessidade de maior transparência e prestação de contas, que incluem um programa de governança de privacidade e demonstrem, ainda, a eficácia das medidas adotadas. Assim, o programa de governança deve manter o registro das suas atividades de tratamento e podem:

- I – Demonstrar o compromisso do controlador em adotar processos e políticas internas que garantam o amplo cumprimento das regras e boas práticas relativas à proteção de dados pessoais;
- II – Aplicar-se a todo o conjunto de dados pessoais sob seu controle, independentemente do meio utilizado para coletá-los;
- III – Ser adaptável à estrutura, escala e volume de suas operações, bem como à sensibilidade dos dados processados;
- IV – Estabelecer políticas e salvaguardas adequadas com base em um processo de avaliação sistemática dos impactos e riscos à privacidade dos titulares dos dados armazenados;
- V – Estabelecer uma relação de confiança com o titular dos dados, por meio de maior transparência das operações que envolvam seus dados pessoais e garantir mecanismos para a participação do titular dos dados no processo;
- VI – Integrar na sua estrutura geral de governança, princípios éticos e probos, bem como estabelecer e aplicar mecanismos internos e externos de supervisão das operações;
- VII - Implementar planos de resposta a incidentes em segurança da informação e de solução dos problemas enfrentados; e
- VIII – Atualizar constantemente a base de informações, por meio de monitoramento contínuo e avaliações periódicas dos riscos e de planos de mitigação dos danos.<sup>159</sup>

Dessa maneira, a governança de dados pode ser compreendida com a adoção de processos, procedimentos, estruturas organizacionais, adoção de regras de conduta, de normas técnicas, da adoção de políticas internas e externas que incentivem a implementação de uma cultura organizacional de proteção dos dados dos titulares.

Nesse sentido, Lisboa e Vilhena afirmam o seguinte:

Exemplos de medidas a serem tomadas pelas empresas para que estas se adequem à LGPD são a implementação de programas de *compliance* digital e de governança corporativa. As empresas de modo geral devem estabelecer condições, regimes e procedimentos internos para o tratamento de dados pessoais junto a profissionais de Tecnologia da Informação, realizando periodicamente auditorias internas para avaliar o grau de conformidade com a LGPD e determinar quais os riscos no tratamento de dados. As empresas

---

<sup>159</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 nov de 2021;

devem gerenciar com frequência os dados pessoais, descrevendo quais são esses dados, onde estão e para que estão sendo utilizados.<sup>160</sup>

Nesse sentido, refere-se que as regra de boas práticas e de governança, definem as condições organizacionais, o regime de funcionamento, os procedimentos internos, inclusive os canais de reclamação e peticionamento dos titulares. Assim como, as obrigações e as responsabilidades de prestar contas de todos os sujeitos envolvidos nas operações de tratamento de dados, de maneira a garantir que os dados sejam utilizados e o uso seja feito de maneira adequada e apropriada para o atingimento da finalidade a que se propõe, respeitando os direitos dos titulares, em observância com o consentimento prévio, específico e informado previamente.

Dessa maneira, compreende-se que a organização deve promover práticas pautadas em princípios éticos e probos, em observância às boas práticas em segurança da informação, atualizando-as e oferecendo treinamento e aperfeiçoamento constantes, conforme as normas e os procedimentos mais adequados à complexidade e o risco das operações. Nesse contexto, as organizações que já possuam em suas operações técnicas e boas práticas e uma cultura organizacional protetiva das informações dos clientes, terão menos dificuldades em se adequarem à realidade digital e às novas legislações a respeito do tema, assim como, de obterem melhores resultado e tornar mais eficientes os seus programas de conformidade e não apenas se prevenir das sanções e das penalidades impostas pela legislação.

Nesse contexto, Bioni ressalta o seguinte:

O processo de conformidade não deve ser internalizado como um custo, muito menos enquanto uma papelada para formalmente fazer um “checklist” das obrigações legais. Pelo contrário, deve ser compreendido como um investimento capaz de otimizar e tornar mais eficiente as atividades dos atores regulados. A partir dessa mentalidade, abre-se espaço para que a nova regulação seja um gatilho para: a) a criação de novos produtos e serviços e, até mesmo, a revisão de um modelo de negócio ou de uma política pública, ao invés de servir apenas para a manutenção ou a revisão de produtos e serviços existentes; b) geração de valor através de diagnósticos e

---

<sup>160</sup> LISBOA, Anna Luiza de Carvalho. VILHENA, Marília Marques Rêgo. Proteção de dados: nova dimensão da função social da empresa. Disponível em: [https://www.academia.edu/42733880/Governan%C3%A7a\\_e\\_direitos\\_fundamentais\\_revisitando\\_o\\_debate\\_entre\\_o\\_p%C3%BAblico\\_e\\_o\\_privado](https://www.academia.edu/42733880/Governan%C3%A7a_e_direitos_fundamentais_revisitando_o_debate_entre_o_p%C3%BAblico_e_o_privado); Acesso em: 21 nov. 2021;

prognósticos recorrentes e dinâmicos, ao invés de avaliações estanques focadas apenas no risco regulatório. Enfim, o processo de conformidade passa a fazer parte de um plano maior de gestão baseado em inovação, ao invés de se guiar apenas pelo receio da aplicação de sanções em caso de não conformidade à nova regulação.<sup>161</sup>

## **4.2. Direitos dos titulares de dados**

A LGPD prevê, nos arts. 9º e 17 a 22, os direitos dos titulares de dados, concentrando em um diploma legal as garantias dos titulares nas operações de tratamento, sem excluir os direitos previstos em outros diplomas legais, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo, o Marco Civil da Internet e outros. Nesse sentido, o artigo 17 preceitua que toda pessoa natural tem assegurada a titularidade de seus dados e garantidos os seus direitos fundamentais de liberdade, à privacidade, à intimidade. Assim como, o art. 18, preceitua o direito do titular de dados de obter, mediante requisição, do controlador, a confirmação de existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com as situações previstas na Lei; a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses do art. 16, da Lei. Além disso, foi incluído, pela Lei n. 13.853/2019, o direito à portabilidade dos dados.

### **4.2.1. Direito à titularidade dos dados pessoais, à confirmação de existência de tratamento, de acesso aos dados e de requerer a correção de dados incompletos, inexatos ou desatualizados**

A qualidade de titular dos dados é pressuposto da pessoa natural de garantir a titularidade de seus dados pessoais e garantir seus direitos fundamentais de liberdade, intimidade e de privacidade, nos termos do art. 17, da LGPD. O titular possui, ainda, o direito de obter, do controlador, mediante requisição e a qualquer momento, nos termos do art. 18, inciso I, da LGPD, informações relativas ao uso de

---

<sup>161</sup> BIONI, Bruno Ricardo. Regulação de dados é uma janela de oportunidade. p. 71. Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes / [organização Bruno Ricardo Bioni]. -- São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

seus dados pessoais nas operações. Além disso, cumpre salientar que as informações devem ser fornecidas de forma clara, adequada e específica, quanto às finalidades das operações de tratamento. Além disso, prevê que as informações podem ser fornecidas imediatamente, de forma simplificada, ou por meio de declaração clara e completa, no prazo de 15 (quinze) dias, nos termos do art. 19, I e II.

Nesse contexto, ressalta o seguinte:

Esse é um direito de suma importância para que o titular de dados possa, inclusive, exercer os demais direitos elencados na LGPD. Portanto, é direito subjetivo do titular dos dados pessoais obter, sem custo, do agente de tratamento de dados a confirmação de tal prática. O formato da requisição deve ser simplificado e disponibilizado nos sites dos agentes de tratamento de dados, que deverão responder no prazo de 15 (quinze) dias (art. 19, inc. II da LGPD), podendo a ANPD dispor especificamente sobre prazos diferenciados (§ 4º). Na resposta, o controlador do tratamento de dados deverá indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento de dados pessoais.<sup>162</sup>

Nesse sentido, relaciona-se ao princípio da transparência e o direito ao acesso facilitado, uma vez que a Lei prevê que os titulares devem ter acesso a informações relativas à finalidade específica do tratamento, a duração do processamento, com observância aos segredos industriais e comerciais, a identidade do controlador e informações sobre o uso compartilhado dos dados e a finalidade.

Assim, compreende-se que ao deter a posse sobre os seus dados e o direito às informações relativas às operações de tratamento, o titular possui o direito de requisitar cópia e acesso gratuito e facilitado aos dados processados e armazenados pelo controlador, conforme art. 18, II, da LGPD. Dessa maneira, a Lei prevê, ainda, que o relatório deve indicar, de forma completa, a origem dos dados, os registros de todas as operações de tratamento, pelo controlador e de compartilhamento com terceiros, indicando a finalidade do tratamento, resguardando os segredos industriais e comerciais.

Nesse sentido, ressalta-se o seguinte:

---

<sup>162</sup>LIMA, Cíntia Rosa Pereira. D. Comentários à Lei Geral de Proteção de Dados. Coimbra: Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 20 nov. 2021;

Além de receber a confirmação do tratamento de seus dados pessoais, o titular tem direito de acesso aos dados, que deve ser providenciado nos mesmos termos e prazo do direito de confirmação supramencionado. Para tanto, o titular deverá fazer um requerimento expresso, devendo ser facilitado pelo agente, por exemplo, disponibilizando no seu site. Os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso (§ 1º do art. 19 da LGPD), o que pode ser disciplinado pela ANPD ao sugerir alguns formatos. No requerimento de acesso aos dados pessoais, o titular deverá indicar se quer receber tais informações em meio eletrônico ou sob forma impressa (§2º do art. 19 da LGPD).<sup>163</sup>

Nesse sentido, a Lei afirma que os dados pessoais devem ser armazenados de maneira que facilite o acesso e o exercício desse direito e, ainda, que a Autoridade Nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares.

Além do mais, no art. 18, VII, a LGPD prevê o direito dos titulares a obter informações, das entidades públicas e privadas, informações sobre o uso compartilhado de dados realizada pelo controlador. Nesse sentido, possui direito de tomar conhecimento sobre o compartilhamento dos seus dados, a fim de consentir ou não com essa prática e solicitar a exclusão dos dados compartilhados ou processados sem o seu prévio consentimento.

Em estrita relação com os direitos citados anteriormente, a LGPD prevê o direito dos titulares de requerer que seus dados sejam retificados, diante da constatação de que estejam incorretos, inexatos, insuficientes ou desatualizados, nos termos do art. 18, III. Além disso, no § 6º, afirma que o responsável pelo tratamento deverá informar, imediatamente, aos agentes de tratamento, com os quais tenha realizado uso compartilhado de dados, a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento corretivo, com exceção naqueles casos em a comunicação seja comprovadamente impossível ou implique esforço desproporcional.

Nesse sentido, ressalta-se o seguinte:

Ao constatar alguma inexatidão ou necessária complementação ou atualização dos dados pessoais, o titular pode pleitear a correção destes dados, em homenagem ao princípio da qualidade dos dados

---

<sup>163</sup>LIMA, Cíntia Rosa Pereira. D. *Comentários à Lei Geral de Proteção de Dados*. Coimbra: Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 20 nov. 2021;

personais (art. 6º, inc. V da LGPD). Assim, por exemplo, se em determinado banco de dados consta que uma pessoa foi condenada por um crime, quando na verdade foi absolvida, o titular pode exigir que o agente do tratamento de dados faça a devida correção.<sup>164</sup>

#### 4.2.2. Direito à anonimização, bloqueio ou eliminação dos dados

Nos termos do art. 18, IV, LGPD, refere-se ao direito do titular de requerer que seus dados sejam anonimizados, bloqueados ou que haja a eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com as disposições legais. Nesse contexto, a anonimização refere-se ao emprego de técnicas azoáveis e disponíveis no momento do tratamento, por meio da qual, os dados perdem a possibilidade de serem associados diretamente ou indiretamente ao indivíduo, nos termos do art. 5º, inciso XI, da LGPD.

Dessa forma, as informações são alteradas para que o titular não possa ser identificado, nem mesmo pelo controlador. Dessa maneira, nos termos do art. 12, *caput*, da Lei, o dado anonimizado deixa de ser considerado dado pessoal, diante da desvinculação das informações ao titular.

Quanto ao bloqueio ou eliminação dos dados, ressalta-se o seguinte:

O direito ao bloqueio ou eliminação dos dados é aplicável em duas hipóteses: i) tratamento lícito quando os dados pessoais forem desnecessários ou excessivos; e ii) quando se tratar de tratamento ilícito. Na primeira hipótese, o titular pode pleitear esse direito em homenagem aos princípios da finalidade, adequação e necessidade (art. 6º, incisos I, II e III, respectivamente da LGPD). No entanto, entendemos que se os dados forem desnecessários ou excessivos, justamente em virtude dos princípios ora destacados, o tratamento de dados não estará em conformidade com a lei. Já na segunda hipótese, trata-se de uma regra mais elástica, isto é, se por qualquer outra razão, constatar-se alguma ilicitude no tratamento de dados.<sup>165</sup>

Assim, a LGPD prevê, aos titulares dos dados, o direito de requerer a exclusão dos seus dados pessoais. Dessa maneira, o direito de solicitar exclusão aplica-se a dados desnecessários ou excessivos, ou dados processados com o

---

<sup>164</sup> LIMA, Cíntia Rosa Pereira. D. *Comentários à Lei Geral de Proteção de Dados*. Coimbra: Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 20 nov. 2021;

<sup>165</sup> LIMA, Cíntia Rosa Pereira. D. *Comentários à Lei Geral de Proteção de Dados*. Coimbra: Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 20 nov. 2021;

consentimento do titular dos dados, exceto nas situações em que exista base legal que autorize a sua manutenção, como nas hipóteses previstas no Artigo 16.

Nesse sentido, ressalta-se o seguinte:

Além desse direito e/ou sanção administrativa, o titular dos dados pessoais pode pleitear a eliminação dos dados pessoais, nos termos do art. 18, inc. VI da LGPD. Em regra, os dados pessoais devem ser automaticamente eliminados ao término do tratamento de dados (art. 16, caput da LGPD). Contudo, se não o forem, cabe ao titular o direito de obter a eliminação de suas informações da base de dados do agente, que somente está autorizado a conservá-las quando: i) por obrigação legal ou regulatória; ii) para estudo por órgão de pesquisa, garantida, sempre que possível a anonimização; iii) tenha transferido para terceiros conforme os requisitos estabelecidos na LGPD; iv) para uso exclusivo do controlador, desde que os dados sejam anonimizados, vedado seu acesso por terceiro.<sup>166</sup>

#### **4.2.3. Direito de petição, de oposição e à revisão das decisões tomadas unicamente com base em tratamento automatizado de dados**

Nesse sentido, nos termos do art. 18, § 1º, diz respeito ao direito do titular de dados, de peticionar perante a ANPD, quaisquer requerimentos relativos aos seus dados em face do controlador. Assim, ressalta-se a importância que a Autoridade Nacional possui na resolução dos conflitos e na fiscalização das atividades de tratamento de dados pessoais. Em vista do art. 18, § 2º, da LGPD, o titular dos dados possui o direito de se opor ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento aos preceitos da legislação.

Além disso, o direito à oposição refere-se à possibilidade de o titular de dados requerer a revisão das decisões tomadas com base unicamente em tratamento automatizado de dados, em vista prejuízos aos seus interesses, naquelas decisões destinadas a definir seu perfil pessoal, profissional de consumo e de crédito e afetem aspectos relativos à sua personalidade, conforme disposto no art. 20, *caput*, da LGPD.

---

<sup>166</sup> LIMA, Cíntia Rosa Pereira. *D. Comentários à Lei Geral de Proteção de Dados*. Coimbra: Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 20 nov. 2021;

#### **4.2.4. Direito à portabilidade dos dados, a revogar o consentimento, a ser informado sobre a possibilidade de não consentir**

A LGPD define o direito à portabilidade de dados como a possibilidade de o titular requerer, mediante requisição expressa, observados os segredos comercial e industrial, a portabilidade dos dados a outro provedor de serviços ou produtos.

Nesse sentido, Pinheiro ressalta o seguinte:

No que diz respeito à regulação da portabilidade dos dados pessoais, o art. 18 apresenta alterações no inciso V e no § 6º e prevê que a Autoridade Nacional ficará responsável por regulamentar a portabilidade dos dados em tratamento, observando os segredos comercial e industrial.

O art. 18, § 6º, acrescenta ainda a possibilidade de o controlador não comunicar os demais agentes de tratamento que tenham realizado uso compartilhado de dados se esta comunicação for comprovadamente impossível ou implique esforço desproporcional. Todavia, o parágrafo peca ao não especificar ou quantificar o grau de esforço que pode ser considerado desproporcional.<sup>167</sup>

Além do mais, considerando que, em regra, as operações de tratamento possuem fundamento na manifestação expressa do titular, do seu consentimento para as finalidades a que se propõe a atividade, ele possui o direito de revogar, a qualquer tempo, mediante manifestação expressa, por procedimento gratuito e facilitado, o seu consentimento, nos termos do § 5º do art. 8º da Lei. Nesse sentido, os controladores e os operadores devem encerrar o processamento dos dados imediatamente após a comunicação por parte do titular.

Ademais, a Lei prevê a o direito dos titulares de obterem informações a respeito da possibilidade de não consentirem com o processamento dos seus dados e, nestes casos, as consequências da recusa. Nesse sentido, ressalta-se que as informações devem ser fornecidas de forma clara, adequada e ostensiva. Nos casos em que a atividade depende do consentimento, quando as informações forem passadas de maneira abusiva, enganosa ou apresentada de forma não transparente, o consentimento é considerado nulo. Assim, como quando houver mudança nas finalidades do processamento, em relação ao consentimento original, o titular tem o direito de ser informado e de recusar dos novos termos.

---

<sup>167</sup>PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021

### 4.3. Autoridade Nacional, responsabilidade e sanções na LGPD

#### 4.3.1. Autoridade Nacional de Proteção de Dados (ANPD) e estrutura regulatória

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão vinculado à Presidência da República, dotado de autonomia técnica e decisória, tem a competência de zelar pela proteção dos dados pessoais, a fim de resguardar os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto nos arts. 55-A a 55-L, inseridos na LGPD por meio da Lei n. 13.853/2019.

Além disso, tem a finalidade orientativa, ou seja, de orientar os agentes de tratamento sobre boas práticas e da implementação de medidas de segurança da informação e de estimular a adequação à LGPD. Dessa maneira, sua atuação é de suma importância para o reconhecimento e divulgação de boas práticas de governança de dados, de gestão de riscos<sup>168</sup>, da implementação de programas de governança em privacidade e a promoção de uma cultura de proteção de dados.

Nesse sentido, Sarlet, Fernandes e Ruaro ressaltam o seguinte:

Entre outras, as principais atribuições da ANPD são: criação de uma política nacional de proteção de dados pessoais; garantir a privacidade desses dados; fiscalizar e aplicar sanções; promover campanhas de informação com a população sobre as normas e as políticas públicas de proteção de dados pessoais; promover ações de cooperação com autoridades estrangeiras sobre esse tema; propor diretrizes estratégicas; e elaborar relatórios anuais de avaliação da execução da política nacional de proteção de dados.<sup>169</sup>

Além disso, conforme ressalta a diretora do Conselho Diretor da ANPD, Nairane Rabelo Farias Leitão, “induzir e direcionar a proteção de dados pessoais é

---

<sup>168</sup> “REGULAÇÃO DE RISCO: envolve ações que promovam a melhoria da gestão de risco (i.e., a cognição, avaliação e gerenciamento, que possui como viés a implementação da política de gestão de riscos). Exige o implemento de medidas apropriadas para assegurar e demonstrar conformidade, levando em consideração, entre outros, os riscos de probabilidade e gravidade em certas circunstâncias, apresentando-se em um contexto de obrigação geral de gerir adequadamente os riscos.” Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo: CEPI-FGV Direito SP, 2021.

<sup>169</sup> SARLET, Gabrielle Bezerra Sales. FERNANDES, Márcia Santana. RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

uma importante missão da ANPD e avançar no fornecimento de ferramentas e modelos de documentos pode ajudar as organizações a entrarem em conformidade com a LGPD.”<sup>170</sup>

Dessa maneira, a LGPD visa a criação de um sistema nacional de proteção de dados, uma missão complexa e importante que perpassa pela implementação de uma Autoridade Nacional que atue conjuntamente com diversos setores da sociedade e demais órgãos relacionados a proteção de dados, assim como, pelos poderes Legislativo e Judiciário.

Nesse sentido, o Conselho Nacional de Proteção de Dados pessoais e da Privacidade (CNPd) é o órgão consultivo criado no âmbito da ANPD, com uma composição multissetorial, formada por membros da sociedade e do poder público. Compete ao Conselho as seguintes atribuições, nos termos do art. 58-B, da LGPD: propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da Autoridade Nacional de Proteção de Dados; elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; sugerir ações a serem realizadas pela ANPD; realizar estudos, debates e audiências públicas sobre o tema; e disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral.<sup>171</sup>

Além disso, o Ministério Público do Distrito Federal e Territórios instituiu, por meio da Portaria Normativa PGJ n. 539, de 12 de abril de 2019, a Comissão de Proteção de Dados Pessoais, que atua ativamente em questões referentes às normas de proteção de dados pessoais no país, a fim de combater os crimes cibernéticos por meio da efetiva proteção dos dados pessoais.

Dessa maneira, nos termos dessa portaria compete ao MPDFT:

promover e incentivar, nos termos das legislações sobre o tema, a proteção dos dados pessoais; sugerir diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade; promover o conhecimento das normas e das políticas sobre proteção de dados pessoais e as medidas de segurança entre a população, as

---

170BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Governo Federal. Presidência da República. Brasília, DF. Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte> Acesso em: 19 nov de 2021;

171BRASIL. Conselho Nacional de Proteção de Dados (CNPd). Governo Federal. Presidência da República. Disponível em: <https://www.gov.br/anpd/pt-br/composicao-1/conselho-nacional-de-protecao-de-dados-pessoais-e-privacidade-cnpd> Acesso em 19 de nov de 2021;

empresas e órgãos público; promover estudo sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; estimular a adoção de padrões que facilitem o exercício de controle dos titulares sobre seus dados pessoais; promover ações de cooperação com autoridade de proteção de dado pessoais de outros países, de natureza internacional ou transacional; sugerir a adoção de cláusulas contratuais padrão (*standard contractual clauses, model clauses*) para fins de transferência internacional de dados; sugerir a adoção de normas corporativas globais (*binding corporate rules - BCRs*) para fins de transferência internacional de dados; receber comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares dos dados (*data breach notification*); recomendar, diante da gravidade do incidente de segurança, ao responsável pelo tratamento dos dados a adoção de outras providências, tais como: pronta comunicação aos titulares; ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente; reconhecer e divulgar as regras de boas práticas formulada pelas organizações; recomendar padrões técnicos e organizacionais objetivando proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito; incentivar o estabelecimento de procedimentos de certificação de proteção de dados, bem como de selos e marcas de proteção de dados e privacidade; acompanhar e, se for o caso, apresentar propostas de modificação regulamentar e legislativa; promover a defesa dos interesses e direitos difusos, coletivos e individuais homogêneos dos titulares dos dados pessoais.<sup>172</sup>

Além disso, cita-se, ainda, mas não menos importante, o PROCON, órgão que atua na proteção de dados pessoais nas relações de consumo em nível estadual e municipal, fazendo parte do Sistema Nacional de Defesa do Consumidor. Nesse sentido, compreende-se que o incentivo à proteção de dados no Brasil tem aumentado de maneira progressiva desde a promulgação da LGPD, em 2018. Assim, é possível afirmar que a tutela aos direitos de proteção de dados pessoais e privacidade perpassa por diversos setores e instituições, que devem atuar conjuntamente, tendo em vista a ANPD como norteador das políticas acerca do tema, a fim de garantir maior efetividade, esses atores devem atuar conjuntamente, na busca por um sistema de proteção efetivo e integrado dos órgãos competentes.

A Lei Geral de Proteção de Dados prevê, a partir do art. 52, sanções administrativas e pecuniária, que estão em vigor desde o dia 1º de agosto de

---

<sup>172</sup>BRASIL. MPDFT. Procuradoria Geral de Justiça. Portaria Normativa. PGJ n. 539, de 12 de abril de 2018. Disponível em: [https://www.mpdft.mp.br/portal/pdf/comissao\\_protecao\\_dados\\_pessoais/Portaria\\_PGJ\\_n2018\\_0539.pdf](https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Portaria_PGJ_n2018_0539.pdf). Acesso em: 19 nov. 2021;

2021.<sup>173</sup> Dessa maneira, as sanções previstas na Lei somente são aplicáveis a fatos ocorridos após a entrada em vigor destas sanções ou, ainda, para delitos de natureza continuada iniciados antes desta data.

Dessa maneira, a ANPD, após a aprovação do Regulamento de Fiscalização e de Aplicação de Sanções Administrativas, a Autoridade Nacional começará a atuar na fiscalização e aplicação das sanções administrativas, conforme verifica-se em consulta ao *site* da ANPD<sup>174</sup>. Além do mais, a Autoridade já dispõe de um canal para comunicação das infrações relativas ao descumprimento dos preceitos da LGPD pelo titular dos dados em face do controlado.

Conforme salientado anteriormente, no capítulo que trata dos agentes de tratamento, a responsabilidade, à luz da LGPD é, em regra, solidária. Nesse contexto, o operador e o controlador respondem solidariamente pelos danos causados em virtude das operações de tratamento de dados, nas hipóteses em que deixarem de cumprir com as obrigações de cuidado impostas por toda a legislação que disciplina a proteção de dados pessoais.

Nesse sentido, Pinheiro afirma o seguinte:

As punições variam entre advertências, aplicação de multas, suspensão e até mesmo proibição das atividades relacionadas ao tratamento de dados. Essas punições variam de forma gradativa de acordo com cada caso, conforme a gravidade do dano, a condição econômica do infrator, a reincidência, a boa-fé do infrator etc., e devem ser investigadas por meio de um processo administrativo que assegura o contraditório, a ampla defesa e o direito de recurso. As multas podem ser simples ou diárias, com valor relativo a 2% do faturamento da organização privada, limitadas a um total de R\$ 50 milhões por infração.<sup>175</sup>

Nesse sentido, o art. 42, da LGPD, prevê que os agentes que, em virtude das operações de tratamento, causarem dano patrimonial, moral, individual ou coletivo, diante da violação às leis sobre proteção de dados, são obrigados a reparar o dano.

---

<sup>173</sup> BRASIL. Autoridade Nacional de Proteção de Dados. (ANPD) Governo Federal. Presidência da República. Sanções Administrativas: o que muda após 1º de agosto de 2021? ANPD traz esclarecimentos sobre a entrada em vigor das sanções administrativas. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 20 nov. 2021;

<sup>174</sup> Idem;

<sup>175</sup> PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021

Dessa forma, a fim de assegurar a efetiva indenização do titular dos dados, prevê, no § 1, a responsabilidade solidária do controlador e do operador. Considera-se, ainda, irregular, o tratamento realizado em inobservâncias às legislações ou que deixarem de adotar medidas de segurança adequadas e esperadas, de acordo com as circunstâncias e a complexidade das operações.

Nesse sentido, compreende-se que os agentes de tratamento são obrigados a adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados de terceiros e de situações acidentais ou ilícitas que impliquem na destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Dessa maneira, é imperioso o emprego de regras claras, de boas práticas de governança e adoção de padrões técnicos aos procedimentos e de normas de segurança, que deverão ser atualizadas periodicamente, a fim de promover o cumprimento das exigências das legislações sobre o tema e das normas técnicas e organizacionais que poderão ser recomendadas e estimuladas pela Autoridade Nacional.

Diante da inobservância aos preceitos legais e técnicos, o art. 52, prevê a aplicação de penalidade aos agentes em face das infrações cometidas e da não observância aos preceitos estabelecidos. Além disso, a lei prevê critérios para a aplicação das sanções, que serão aplicadas após procedimento administrativo, que possibilite o exercício do direito à ampla defesa, de forma gradativa, isolada ou cumulativa, tendo em vista as peculiaridades do caso em análise, de acordo com os seguintes critérios:

- 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.<sup>176</sup>

Em vista desses critérios e das peculiaridades do caso concreto, a ANPD poderá aplicar as seguintes sanções administrativas:

- I – Advertência: diz respeito à repreensão, ao agente de tratamento, nos termos do art. 52, I, da LGPD, com prazo para a adoção de medidas corretiva;
- II – Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por cada infração;
- III – Multa diária: em observância aos limites imposto anteriormente, de no máximo R\$ 50.000.000,00 (cinquenta milhões de reais);
- IV – Publicização: refere-se, nos termos do art. 52, IV, ao ato de publicização da infração após ter sua ocorrência devidamente apurada e confirmada;
- V – Bloqueio dos dados pessoais, nos termos do art. 52, V, a que se refere a infração até sua regularização, representa a suspensão temporária das operações de tratamento envolvendo os dados pessoais afetados, até sua devida regularização;
- VI – Eliminação dos dados pessoais, refere-se a uma das mais graves sanções, tendo em vista que a atividade depende dos dados, valiosos ativos econômicos na sociedade da informação. Nesse sentido, a sua exclusão pode ser considerada de grande prejuízo econômico para toda a atividade econômica desempenhada pela organização. (com adaptação e comentários nossos)<sup>177</sup>

Dessa maneira, em observância ao disposto no art. 52, as sanções administrativas devem ser aplicadas somente pela ANPD. Nesse sentido, a Lei estabelece as competências da Autoridade Nacional, que prevalecerão sobre as competências das outras entidades ou órgãos da administração pública, que tratam da proteção dos dados pessoais. Além do mais, ressalta-se que as sanções administrativas a serem aplicadas pela ANPD não implicam a sua substituição em face da responsabilidade civil, penal ou outras sanções administrativas, assim como, aquelas previstas no Código de Defesa do Consumidor ou outras normas específicas sobre o tema. Assim, cabe a ANPD, a fim de conferir maior efetividade à sua atuação, devido à sua importância na defesa dos direitos dos titulares de dados,

---

<sup>176</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 nov de 2021;

<sup>177</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 nov de 2021;

ampliar as relações com outros órgãos e entidades, estabelecendo normas e diretrizes, na construção de um efetivo sistema nacional de proteção dos dados pessoais.

Nesse sentido, as sanções deverão ser aplicadas por meio de uma criteriosa apreciação e ponderação de critérios, acerca da natureza e da gravidade das infrações e dos direitos atingidos. Além disso, deve-se ter em vista uma abordagem responsiva, tendo em vista, pela organização, a adoção de boas práticas de governança e de medidas de segurança disponíveis e adequadas, capazes de mitigar os danos e preveni-los; em vista da sua capacidade econômica, da complexidade das operações e das exigências impostas pelo sistema de proteção de dados e pela adoção de normas técnicas de segurança da informação.

Nesse sentido, quanto à atuação da Autoridade Nacional, ressalta-se o seguinte:

Tendo em vista tais parâmetros, e em conformidade com sua Agenda Regulatória, a ANPD encontra-se em fase de conclusão da elaboração do Regulamento de Fiscalização e Aplicação de Sanções Administrativas, que passou por Consulta Pública entre 28 de maio e 28 de junho de 2021.

[...]

Segundo a proposta de regulamento submetida à Consulta Pública, ainda sujeita a alterações em razão das contribuições recebidas, prevê-se que a atuação da ANPD se dê conforme uma abordagem responsiva, ou seja, de maneira gradual, baseada no comportamento do regulado e alicerçada em um plano de monitoramento do setor que permita a priorização de temas segundo seu risco, gravidade, atualidade e relevância.

[...]

Assim, a proposta de regulamento prevê etapas de monitoramento, orientação, prevenção e repressão de infrações, levando em consideração as informações recebidas a partir de reclamações, denúncias, representações e notificações de incidentes para estabelecer prioridades a serem incluídas na agenda de fiscalização.

[...]

A LGPD prevê que a ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação da Lei e do estabelecimento de normas e diretrizes para a sua implementação.

[...]

Assim, a ANPD já possui acordos de cooperação técnica firmados com a Secretaria Nacional do Consumidor - SENACON e com o Conselho Administrativo de Defesa Econômica - CADE que permitem o desenvolvimento de atividades conjuntas em temas que gerem repercussões nas áreas de atuação dos órgãos envolvidos. Já há,

inclusive, casos concretos sob análise da Autoridade que envolvem a atuação cooperativa com esses órgãos e com o Ministério Público.<sup>178</sup>

#### **4.3.2. Incidentes em segurança e prestação de contas (*accountability*)**

A LGPD impõe aos agentes a obrigação de adotarem medidas de segurança para proteger os dados pessoais que processados nas operações de tratamento. Além do mais, especifica que a ANPD poderá divulgar orientações sobre quais medidas de segurança específicas devem ser adotadas e fiscalizar a sua implementação e cumprimento. Dessa maneira, refere, em seu art. 48, que o controlador tem a obrigação de notificar a Autoridade Nacional e ao titular acerca de incidentes de segurança que tenham posto em risco os direitos dos titulares dos dados.

Nesse sentido, em similaridade com disposto na RGPD, que prevê a violação dos dados (*data breach*), referido como um incidente de segurança caracterizado pela violação da segurança dos sistemas e redes, que leva a incidentes acidentais ou ilícitos de destruição, perda, alteração ou divulgação não autorizada de dados pessoais tratados pelos agentes. por outro lado, traz a definição de *data breach* (violação de dados pessoais).

Dessa maneira, em semelhança à legislação europeia, a LGPD reconhece o princípio da segurança da informação como um direito fundamental relacionado à proteção de dados pessoais. Além do mais, conforme salientado anteriormente, por meio do art. 6º, X, a LGPD, exprime a necessidade de os agentes demonstrarem a 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. No RGPD, tal princípio encontra previsão no art. 5.2, referido como *accountability*, que diz respeito à responsabilidade do controlador de demonstrar que está em conformidade com as normas e princípios sobre proteção de dados e prestar contas nos casos de ocorrência de incidentes em segurança.

Assim, ressalta-se que a segurança significa o uso de medidas técnicas e procedimentais capazes de proteger os dados pessoais de acessos não autorizados

---

<sup>178</sup>BRASIL. Autoridade Nacional de Proteção de Dados. (ANPD) Governo Federal. Presidência da República. Sanções Administrativas: o que muda após 1º de agosto de 2021? ANPD traz esclarecimentos sobre a entrada em vigor das sanções administrativas. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 20 nov. 2021;

de terceiros e de situações acidentais ou ilegais que ocasionem a destruição, a perda, a alteração das informações, a comunicação ou a disseminação dos dados no ambiente virtual, ocasionado graves violações aos direitos dos titulares dos dados pessoais. Nestes casos, a LGPD prevê que, os controladores e processadores devem informar à ANPD e ao titular dos dados a ocorrência de um incidente de segurança e do risco ou dano relevantes aos titulares. Nesse contexto, essa comunicação deve ser feita em prazo razoável (conforme determinado pela ANPD) e nos termos do art. 48, § 1º, incisos I a VI, mencionar:

I – A descrição da natureza dos dados pessoais afetados (que tipo de dados estão envolvidos, se há dados sensíveis, de crianças e adolescente);

II – As informações relativas aos titulares envolvidos;

III – A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, com observância aos segredos comercial e industrial;

IV – Os riscos relacionados ao incidente;

V – Os motivos da demora, caso a comunicação não tenha sido imediata; e

VI – As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.<sup>179</sup>

Além do mais, diante das novas exigências impostas pela LGPD, é importante que as empresas atualizem às suas políticas de privacidade, por meio do documento que informa aos titulares a maneira e as finalidades com que os agentes irão realizar as atividades de tratamento dos dados e explicita os direitos dos titulares, em face de tais operações. Assim como, estruturar uma política adequada em segurança da informação, que disponha sobre as diretrizes de proteção às informações, dos padrões técnicos procedimentais e de conduta a serem aplicadas e observadas por todos os integrantes da organização, a fim de garantir maior segurança em todos os níveis da organização, desde a alta chefia até os níveis hierárquicos inferiores.

Nesse sentido, ressalta-se que a chefia deve demonstrar comprometimento com o programa de governança e os preceitos de adequação, a fim de garantir que o programa, incluindo a política, os procedimentos e os objetivos, sejam implementado, mantidos e analisados criticamente e de maneira a assegurar sua eficácia. Assim como, abordar de forma adequada os riscos que a sua não

---

<sup>179</sup>BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 nov de 2021;

observância podem ocasionar à organização e aos direitos dos titulares dos dados. Além disso devem disponibilizar todos os recursos adequados e necessários para a efetiva implementação/adequação dos sistemas de gestão de *compliance*.

Além do mais, devem comunicar a importância de uma gestão eficaz e em conformidade com a os requisitos impostos pela legislação que disciplina a proteção de dados e os procedimentos técnicos adequados para alcançar os objetivos a que a atividade se propõe. Assim, devem promover uma cultura de conformidade adequada à atividade exercida pela organização e promover a melhoria e atualização contínuas dos programas de adequação às normas técnicas de segurança da informação.

Isto posto, compreende-se que a efetividade dos programas de governança e *compliance* perpassam pela implementação de uma cultura organizacional, em todos os níveis organizacionais, que promova formas eficazes de resguardo às informações pessoais dos titulares de dados e, da mesma maneira, às informações da própria organização. Assim, importa assegurar a implementação de canais de comunicação facilitados, entre os colaboradores e o órgão diretivo. A fim de, encorajar as denúncias de práticas de má-fé ou em inobservância às boas-práticas em governança de dados, que possam ocasionar danos à atividade e aos direitos dos titulares.

Nesse sentido, em relação ao programa de governança em privacidade, a LGPD determina, em seu art. 50, § 2º, inciso I, que o operador, em observância à estrutura, a escala e ao volume de suas operações, bem como a sensibilidade dos dados e a probabilidade e a gravidade dos danos que poderão ser ocasionados aos titulares, poderá implementar um programa de governança em privacidade que, no mínimo contenha:

- I – A demonstração do comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- II – A aplicação a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- III – A adaptação à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- IV – O estabelecimento de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

- V – Afirme o objetivo de estabelecer relação de confiança com os titulares, por meio de atuação transparente e que assegure mecanismos para sua participação;
- VI – Demonstre a integração à sua estrutura geral de governança e estabelecimento e aplicação de mecanismos de supervisão internos e externos;
- VII – Conte com planos de resposta a incidentes e remediação; e
- VIII – Seja, constantemente, atualizado com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.<sup>180</sup>

Além disso, o controlador deverá demonstrar a efetividade das medidas adotadas em seus programas de governança em privacidade, quando apropriado e, em especial, a pedido da ANPD ou de outra entidade responsável por promover o cumprimento de boas práticas e padrões de conduta em conformidade com as legislações que tratam da proteção dos dados pessoais dos titulares. Ademais, o art. 50, § 3º, estabelece que as regras de boas práticas e de governança deverão ser publicadas e atualizadas, periodicamente, e poderão ser reconhecidas e divulgadas pela ANPD. Ademais, o art. 51, prevê que a Autoridade Nacional poderá estimular a adoção de padrões técnicos que facilitem o controle pelos titulares das suas informações pessoais.

Dessa maneira, a organização deve determinar os objetivos a que se propõe o sistema de gestão de *compliance* em funções e níveis relevantes e necessários para o desempenho da atividade. Nesse sentido, os objetivos de *compliance* devem ser consistentes com a política interna de adequação; levar em consideração os fatores aplicáveis a organização, que deve determinar as questões internas e externas que são pertinentes para o seu propósito e que afetam sua capacidade de alcançar os objetivos da atividade.

Nesse sentido, Jesus ressalta o seguinte:

Um programa de compliance deve sempre atender às necessidades específicas da empresa, levando em consideração que a depender da atividade explorada estarão sujeitas a riscos diferentes. Assim, antes de criar um programa de compliance, deve ser feita uma

---

<sup>180</sup> BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 20 nov de 2021;

análise de risco, com o objetivo de verificar quais são as reais necessidades da empresa.<sup>181</sup>

Assim, compreende-se que a política de *compliance* deve ter em vista o tamanho e a estrutura da organização, assim como, a natureza, a escala e a complexidade das operações da atividade relativa ao processamento e armazenamento dos dados, como as finalidades a que se propõe, em vista do modelo de negócio praticado pela organização e o consentimento previamente informado. Assim como, da constante atualização dos procedimentos técnicos empregados em face de novos regulamentos e normas técnicas, destinadas a assegurar os direitos dos titulares, o emprego de procedimentos adequados, o monitoramento de possíveis vazamentos relacionados aos riscos da atividade.

Com a finalidade de resguardar os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade das pessoas naturais. Outrossim, verificamos o comprometimento da Lei, em assegurar o equilíbrio entre a observância ao princípio da dignidade da pessoa humana, o desenvolvimento de sua personalidade, a preocupação com a privacidade e o desenvolvimento econômico e tecnológico. Nesse sentido, percebemos que a LGPD buscou conferir maior segurança jurídica nas relações estabelecidas no ambiente virtual, ou seja, maior proteção aos titulares dos dados e, da mesma maneira, estabelecer parâmetros de conduta para as empresas, que impliquem em maior segurança, prevenção dos riscos e prestação de contas, relacionadas às operações de tratamento dos dados pessoais.

Além disso, está previsto a obrigação das empresas manterem maior transparência sobre suas operações e disponibilizar canais de contato com os usuários, que lhes possibilite, gratuitamente e de forma facilitada, visualizar, corrigir e excluir os seus dados mantidos pela organização. Outrossim, prevê que as empresas e organizações devem manter seus procedimentos técnicos de segurança da informação e seus códigos de conduta atualizados e em conformidade com as

---

181JESUS, Johnnatan Douglas Andrade de. A nova realidade do tratamento e da proteção de dados dos trabalhadores frente a LGPD e o Compliance jurídico. São Cristóvão, 2021. Monografia (graduação em Direito) – Departamento em Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão, SE, 2021. Disponível em: [https://scholar.googleusercontent.com/scholar?q=cache:2B2XYe\\_YizQJ:scholar.google.com/+LGPD+%2B+compliance+&hl=pt-BR&as\\_sdt=0,5&as\\_ylo=2021](https://scholar.googleusercontent.com/scholar?q=cache:2B2XYe_YizQJ:scholar.google.com/+LGPD+%2B+compliance+&hl=pt-BR&as_sdt=0,5&as_ylo=2021)). Acesso em: 15 nov. 2021;

exigências impostas pela LGPD e demais normas técnicas, que tratem da disciplina sobre a proteção de dados, como aquelas reconhecidas e divulgadas pela ANPD.

Nesse sentido, os profissionais de segurança da informação e toda a organização, devem garantir o cumprimento dos regulamentos e das normas técnicas disponíveis e adequadas, capazes de proporcionar maior resguardo às informações coletadas, processadas e tratadas. Outrossim, devem prezar pela implementação de políticas organizacionais internas e externas de conformidade, a fim de preservar a integridade institucional e operacional, por meio da estrita observância aos princípios éticos de conduta e às normas de segurança e governança em privacidade dos dados.

Além do mais, tendo em vista que os dados pessoais sensíveis representam aqueles com maior potencial de serem utilizados para fins discriminatórios, ilícitos ou abusivos, as empresas devem promover a revisão dos seus processos e políticas internas e externas sobre captação, armazenamento e transmissão dessas informações. As quais, podem ser realizadas por meio do mapeamento dos dados e utilização de técnicas adequadas e disponíveis, para a avaliação da necessidade de sua manutenção ou exclusão para as operações, que visem a persecução dos fins da atividade. Além do mais, mister que tenham uma política interna bem definida, de proteção das informações sensíveis, por meio da adoção de medidas preventivas e de mitigação dos riscos. Assim como, promovam uma cultura organizacional de conscientização quanto à necessidade de resguardo dessas informações.

Assim sendo, os agentes responsáveis pelas operações de tratamento devem fazer uso de medidas técnicas e administrativas, adequadas à proteção dos dados pessoais dos titulares, em face de possíveis acessos não autorizados de terceiros e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão das informações armazenadas, coletadas e processadas. Assim, as organizações responsáveis pelo tratamento, devem dispor de métodos e procedimentos seguros e eficientes, capazes de monitorar à *internet*, em busca de possíveis violações, a fim de mitigar os riscos e conter possíveis vazamentos de dados. Além dos mais, devem promover o fortalecimento da cultura organizacional de proteção e de boas práticas de governança de dados.

## 5 CONSIDERAÇÕES FINAIS

A presente pesquisa se propôs a analisar o reconhecimento do direito à proteção de dados pessoais como um direito fundamental, frente aos avanços tecnológicos e à transformação digital, que têm impactado em sua proteção e regulamentação. Em vista de que, as tecnologias de processamento e de armazenamento de dados, de inteligência artificial, do aprendizado de máquina e dos complexos algoritmos computacionais, serem capazes de exprimir hábitos, predileções e fatores subjetivos, estritamente relacionados às características da personalidade dos titulares. Nesse contexto, percebe-se que o reconhecimento de um direito fundamental à proteção de dados está intrinsecamente relacionado ao princípio da dignidade humana, na medida em que as informações representam uma extensão da personalidade dos indivíduos.

Nesse sentido, observou-se que os ordenamentos jurídicos tradicionais enfrentam grandes dificuldades em avaliar os efeitos da utilização das novas tecnologias, frente a todo um universo amplo, complexo e dinâmico e da sua imprevisibilidade e rápida transformação. Assim, entendemos que, a dinamicidade e complexidade das relações, estabelecidas no meio digital, representam verdadeiros desafios aos operadores do direito, aos órgãos de regulamentação e de fiscalização, às organizações de direito público e privado e a toda a sociedade, que precisam se atualizar e se reinventar na mesma medida e velocidade experimentadas no ciberespaço.

Dessa maneira, depreendemos a existência de uma tendência global, acerca da necessidade de se proteger os dados pessoais dos usuários das redes e de uma necessária adequação das organizações e das instituições responsáveis pelas operações de tratamento de dados. Sendo assim, auferimos que o sistema europeu, referência internacional no tocante à proteção de dados, está constantemente buscando maneiras de se adequar aos novos desafios impostos por essa nova realidade digital, por meio da organização e atualização de seus conceitos. Assim como, pela promoção de um amplo debate com as partes interessada e a sociedade em geral.

Portanto, compreendemos que, o Regulamento Geral Europeu sobre Proteção de Dados, implicou em efeitos, relativos à proteção de dados, que ultrapassaram os limites da União Europeia. Por meio do estabelecimento de

parâmetros de proteção, a serem observados por todos os países que cogitem estabelecer relações comerciais com o bloco europeu. Dessa maneira, é possível afirmar que tal normativa influenciou, diretamente, no surgimento de legislações que disciplinam a proteção de dados ao redor no mundo.

Além disso, verificamos que, os dados pessoais sensíveis representam aqueles com maior potencial de serem utilizados para fins discriminatórios, ilícitos ou abusivos. Dessa maneira, pressupõe-se, nos sistemas de proteção de dados, que as empresas promovam a revisão dos seus processos de coleta, armazenamento e processamento de dados. Por meio do mapeamento dos dados existente e avaliação da necessidade de sua manutenção ou exclusão para as operações, que visem a persecução dos fins da atividade. Além do mais, mister que tenham uma política interna bem definida, de proteção das informações sensíveis, por meio da adoção de medidas preventivas e de mitigação dos riscos. Assim como, promovam uma cultura organizacional de conscientização quanto à necessidade de resguardo dessas informações.

Assim, depreendemos que a Lei Geral de Proteção de Dados surgiu, nesse contexto, com a finalidade de resguardar os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade das pessoas naturais. Outrossim, verificamos o comprometimento da Lei, em assegurar o equilíbrio entre a observância ao princípio da dignidade da pessoa humana, o desenvolvimento de sua personalidade, a preocupação com a privacidade e o desenvolvimento econômico e tecnológico. Nesse sentido, percebemos que a LGPD buscou conferir maior segurança jurídica nas relações estabelecidas no ambiente virtual, ou seja, maior proteção aos titulares dos dados e, da mesma maneira, estabelecer parâmetros de conduta para as empresas, que impliquem em maior segurança e prevenção dos riscos envolvidos no tratamento dos dados pessoais.

Sendo assim, o reconhecimento do direito fundamental à proteção de dados é de extrema relevância para a sua plena concretização, não como uma mera decorrência do direito à privacidade e do resguardo à intimidade e à vida privada. Nesse sentido, verificamos que o STF reconheceu a proteção de dados pessoais, em recente julgamento, implementando um novo paradigma à tutela constitucional deste direito fundamental, ao trazer um conceito ampliado de dado pessoal e fazer a sua diferenciação, entre os conceitos tradicionais de privacidade e vida privada da esfera da proteção de dados.

Além do mais, a estrita observância às políticas de privacidade e proteção de dados e o estabelecimento de regras claras e precisas aos agentes de tratamento, têm o intuito de conferir maior segurança aos usuários das redes e às relações estabelecidas no meio digital. Compreendemos, assim, que esta abordagem é tema urgente e necessário às organizações e às instituições responsáveis pelas operações de tratamento de dados pessoais. Tendo em vista as imposições e as sanções já estarem em vigor e representarem, para além de meros impactos econômicos, diante das sanções administrativas prevista na LGPD, riscos incomensuráveis à imagem e à confiabilidade das organizações que não se adequarem às exigências impostas pelo sistema protetivo de dados pessoais.

Dessa maneira, verificamos que os agentes responsáveis pelas operações de tratamento devem fazer uso de medidas técnicas e administrativas, adequadas à proteção dos dados pessoais dos titulares. Em face de possíveis acessos não autorizados de terceiros e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão das informações armazenadas, coletadas e processadas. Assim, as organizações responsáveis pelo tratamento, devem dispor de métodos e procedimentos seguros e eficientes, capazes de monitorar à *internet*, em busca de possíveis violações, a fim de mitigar os riscos e conter possíveis vazamentos de dados. Além dos mais, devem promover o fortalecimento da cultura organizacional de proteção e de boas práticas de governança de dados.

Isto posto, percebemos que, devido às complexas relações estabelecidas na *internet* e o seu uso e dependência em diversas esferas da vida cotidiana, enfrentamos problemas relativos à insuficiência do consentimento para a integral e efetiva proteção dos direitos dos titulares. Em vista das limitações cognitivas dos usuários, em compreender e avaliar os riscos aos seus direitos de personalidade, devido à utilização de linguagem técnica e complexa nos termos de privacidade. Bem como, pelo fato de que, na maioria dos casos, a utilização dos serviços está condicionada ao fornecimento do seu consentimento, sem o qual ficam impossibilitados de fazer uso das funcionalidades e serviços ofertados nas redes. Outrossim, a utilização de técnicas complexas de processamento e armazenamento, que impossibilitam aos usuários comensurar todas as implicações de uso dos seus dados.

Sendo assim, compreendemos que a organização deve promover práticas pautadas em princípios éticos e probos, em estrita observância às boas práticas em

governança de dados e segurança da informação, as quais devem ser atualizadas constantemente, diante de novos regulamentos, normas e padrões técnicos disponíveis e adequados. Além do mais, as organizações devem oferecer treinamento e aperfeiçoamento qualificados ao seu quadro funcional, conforme as normas e os procedimentos mais adequados à complexidade e ao risco das operações. Assim, ressaltamos que as organizações que já possuem, em suas operações técnicas, a promoção de boas práticas de governança em privacidade e uma cultura organizacional protetiva das informações dos clientes, terão menos dificuldades em se adequarem às novas legislações a respeito do tema. Da mesma maneira, serão capazes de obter melhores resultados e tornar mais eficientes os seus programas de conformidade e, não apenas, se prevenir das sanções e das penalidades impostas pela legislação.

Nesse sentido, verificamos que a LGPD prevê a obrigação das empresas manterem maior transparência sobre suas operações e disponibilizar canais de contato com os usuários, que lhes possibilite, gratuitamente e de forma facilitada, visualizar, corrigir e excluir os seus dados mantidos pela organização. Outrossim, prevê que as empresas e organizações devem manter seus procedimentos técnicos de segurança da informação e seus códigos de conduta atualizados e em conformidade com as exigências impostas pela LGPD e demais normas técnicas, que tratem da disciplina sobre a proteção de dados, como aquelas reconhecidas e divulgadas pela ANPD.

Sendo assim, cabe aos profissionais de segurança da informação e a toda a organização, garantir o cumprimento dos regulamentos e das normas técnicas de resguardo às informações coletadas, processadas e tratadas. Assim como, de prezar pela implementação de políticas organizacionais internas e externas de conformidade, a fim de preservar a integridade institucional e operacional, por meio da estrita observância aos princípios éticos de conduta e às normas de segurança e governança em privacidade dos dados.

Nesse sentido, verificamos a adoção de procedimentos existentes, como a criptografia dos dados, o mapeamento e programas de gestão de riscos. Assim como, das técnicas de anonimização e armazenamento dos dados estritamente necessários à atividade-fim. Portanto, as políticas de gestão em privacidade devem determinar a necessidade de armazenamento das informações e da possibilidade de

retenção ou exclusão dos dados desnecessários ou inúteis para as operações relativas à finalidade da atividade.

Dessa maneira, permite-se verificar a necessidade de emprego de diferentes níveis de segurança, diante da necessidade de maior proteção de determinadas informações, em vista de maior sensibilidade dos dados e dos riscos envolvidos no armazenamento e/ou compartilhamento destas informações. Assim como, protegê-los de invasões de terceiros, de exclusões acidentais ou intencionais e remover informações desnecessárias, desatualizadas, redundantes ou irrelevantes para a atividade. Assim, ao adotar ferramentas eficazes e programas de gestão de dados, as organizações estarão um passo à frente em atender às necessidades de adequação, resultando em maior competitividade. Compreendemos que a adequação é capaz de reduzir as dificuldades impostas e a sobrecarga de trabalho por parte dos controladores, ao promover um ambiente mais simplificado e eficaz de proteção e de prestação de informações aos titulares.

Portanto, ressaltamos que as consequências da não adequação podem ocasionar danos, não apenas de cunho pecuniário, mas também, à imagem da organização, por meio do bloqueio das operações, da retenção e exclusão dos dados e, em consequência da publicização das sanções, perda de confiabilidade, de clientes e de oportunidades de negócio. Dessa maneira, é possível afirmar que, a médio e longo prazo, a adequação empresarial e organizacional, em estrita observância às normas éticas e aos padrões de conduta e à adoção de medidas técnicas de segurança da informação, por meio de programas de *compliance* em privacidade e governança de dados, tendem a trazer inúmeros benefícios à organização. Tanto à confiabilidade e à segurança jurídica dos titulares de dados nas práticas empresariais e institucionais, quanto na simplificação dos procedimentos de conformidade e na competitividade da organização.

## REFERÊNCIAS

AGUILERA, Daniel Fortes; BIASE, Nicholas Furlan Di. Dificuldades interpretativas no regime de tratamento de dados pelo poder público: lacunas, contradições e atecnias na LGPD. Disponível em: <http://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238/182>. Acesso em: 16 nov. 2021;

ANDRADE, André Gustavo Corrêa de. O princípio fundamental da dignidade humana e sua concretização judicial. *In*: Tribunal de Justiça do Rio de Janeiro, Rio de Janeiro, 2004. Disponível em: [http://www.tjrj.jus.br/c/document\\_library/get\\_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe](http://www.tjrj.jus.br/c/document_library/get_file?uuid=5005d7e7-eb21-4fbb-bc4d-12affde2dbbe). Acesso em: 29 out de 2021;

ARAÚJO, Regina Borges de. Computação Ubíqua: Princípios, Tecnologias e Desafios. Disponível em: [http://www.professordiovani.com.br/rw/monografia\\_araujo.pdf](http://www.professordiovani.com.br/rw/monografia_araujo.pdf) Acesso em: 15 de nov. de 2021.

BIONI, Bruno Ricardo. Regulação de dados é uma janela de oportunidades. p. 71. Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes / [organização Bruno Ricardo Bioni]. -- São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. Disponível em: [http://www.mpsp.mp.br/portal/page/portal/documentacao\\_e\\_divulgacao/doc\\_biblioteca/bibli\\_servicos\\_produtos/bibli\\_informativo/bibli\\_inf\\_2006/Rev-Dir-Soc-Pol-Publicas\\_v.8\\_n.2.08.pdf](http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf). Acesso em: 16 de nov. de 2021.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 11 out. 2021;

BRASIL. Autoridade Nacional de Proteção de Dados. (ANPD) Governo Federal. Presidência da República. Sanções Administrativas: o que muda após 1º de agosto de 2021? ANPD traz esclarecimentos sobre a entrada em vigor das sanções administrativas. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 20 nov. 2021;

BRASIL. Autoridade Nacional de Proteção de Dados. (ANPD). Acesso à Informação. Governo Federal. Presidência da República. Guia Orientativo para Definições dos Agentes de Tratamentos de Dados Pessoais e do Encarregado. p. 5. Disponível em: [https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento\\_final.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf). Acesso em 17 de nov de 2021;

BRASIL. Conselho Nacional de Proteção de Dados (CNPD). Governo Federal. Presidência da República. Disponível em: [https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento\\_final.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf)

br/composicao-1/conselho-nacional-de-protecao-de-dados-pessoais-e-privacidade-cnpd Acesso em 19 de nov de 2021;

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 10 nov. 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Leis/2002/L10406.htm](http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm). Acesso em: 15 nov. 2021;

BRASIL. MPDFT. Procuradoria Geral de Justiça. Portaria Normativa. PGJ n. 539, de 12 de abril de 2018. Disponível em: [https://www.mpdft.mp.br/portal/pdf/comissao\\_protecao\\_dados\\_pessoais/Portaria\\_PGJ\\_n2018\\_0539.pdf](https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Portaria_PGJ_n2018_0539.pdf). Acesso em: 19 nov. 2021;

BRASIL. Proposta de Emenda à Constituição n. 17/2019 (PEC 17/2019). Senado Federal. Brasília, DF. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/149723>. Acesso em: 11 out. 2021;

CELIDONIO, T.; NEVES, P.S.; DONÁ, C.M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil nº 13.709/18) e sua adequação perante a lei em uma instituição financeira. Um estudo de caso. Revista *Brazilian Journals of Business*, Curitiba, v.2, n. 4, p.3626-3648 out./dez. 2020. Disponível em: <https://www.brazilianjournals.com/index.php/BJB/article/view/18382>. Acesso em: 18 de nov de 2021.

COMISSÃO DO PARLAMENTO EUROPEU. *Proposal for an ePrivacy Regulation*. Projeto disponível em: <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>. Acesso em: 25 set. 2021;

COMPARATO, Fábio Konder. A afirmação histórica dos direitos humanos. 11. ed. São Paulo: Editora Saraiva, 2017. p. 111.

DÖHMANN, Indra Spiecker gennant. A proteção de dados pessoais sob o regulamento geral de proteção de dados da união europeia. *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

GRANVILLE, Kevin. *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*. In NY Times. Nova Iorque, 2018. Disponível em: <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>. Acesso em: 03 nov. 2021.

GUTIERREZ, Andriei; REOLONI, Carlos. Lições e boas práticas do setor de tecnologia para todas as organizações: segurança e governança de dados.

Disponível em: < <https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 11 nov. 2021.

JESUS, Johnnatan Douglas Andrade de. A nova realidade do tratamento e da proteção de dados dos trabalhadores frente a LGPD e o Compliance jurídico. São Cristóvão, 2021. Monografia (graduação em Direito) – Departamento em Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão, SE, 2021. Disponível em: [https://scholar.googleusercontent.com/scholar?q=cache:2B2XYe\\_YizQJ:scholar.google.com/+LGPD+%2B+compliance+&hl=pt-BR&as\\_sdt=0,5&as\\_ylo=2021](https://scholar.googleusercontent.com/scholar?q=cache:2B2XYe_YizQJ:scholar.google.com/+LGPD+%2B+compliance+&hl=pt-BR&as_sdt=0,5&as_ylo=2021)). Acesso em: 15 nov. 2021;

LEAL, Dionis Janner. Governança no compartilhamento de dados pessoais entre órgãos da administração pública: *accountability* e *compliance* como instrumentos de controle e gestão. Disponível em: < [https://www.imes.edu.br/Uploads/DISSERTA%C3%87%C3%83O\\_GOVERNAN%C3%87A\\_parcial\\_IMED.pdf](https://www.imes.edu.br/Uploads/DISSERTA%C3%87%C3%83O_GOVERNAN%C3%87A_parcial_IMED.pdf). Acesso em: 16 nov. 2021;

LIMA, Cíntia.Rosa.Pereira. D. *Comentários à Lei Geral de Proteção de Dados*. Coimbra: Grupo Almedina (Portugal), 2020. 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 20 nov. 2021;

LISBOA, Anna Luiza de Carvalho. VILHENA, Marília Marques Rêgo. Proteção de dados: nova dimensão da função social da empresa. Disponível em: [https://www.academia.edu/42733880/Governan%C3%A7a\\_e\\_direitos\\_fundamentais\\_revisitando\\_o\\_debate\\_entre\\_o\\_p%C3%BAblico\\_e\\_o\\_privado](https://www.academia.edu/42733880/Governan%C3%A7a_e_direitos_fundamentais_revisitando_o_debate_entre_o_p%C3%BAblico_e_o_privado); Acesso em: 21 nov. 2021;

LÓSSIO, Claudio Joel Brito. SANTOS, Coriolano Aurélio Almeida Camargo. A confidencialidade e a lei geral de proteção de dados. *in* DE, LIMA. Ana Paula Moraes. C. LGPD Aplicada. São Paulo: Grupo GEN, 2021. 9788597026931. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 11 nov. 2021.

MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Trad. Beatriz Henning et al. Prefácio: Jan Woischnik. Montevideu: Fundação Konrad Adenauer, 2005. p. 233-245;

MENDES Laura Schertel. RODRIGUES JUNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares. O supremo tribunal federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

MENDES, Gilmar Ferreira; BRANCO, Paulo Gonet. Série IDP - Linha Doutrina - Curso de direito constitucional. São Paulo: Editora Saraiva, 2020. E-book. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553618088/>. Acesso em: 09 jun. 2021.

MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização; *in*: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;

MOTA, Ivan Dias da; TENA, Lucimara Plaza. Fundamentos da LGPD: círculos concêntricos e sociedade de informação no contexto de direitos da personalidade. *Revista Jurídica Unicuritiba*. Curitiba.V.02, n.59, p.538-5, Abril-Junho. 2020 [Received/Recebido: Março 15, 2018; Accepted/Aceito: Fevereiro 22, 2019]

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf> Acesso em: 16 nov 2021;

PARLAMENTO EUROPEU. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680>. Acesso em: 25 set. 2021;

PARLAMENTO EUROPEU. Proteção de Dados Pessoais. Disponível em: [https://www.europarl.europa.eu/ftu/pdf/pt/FTU\\_4.2.8.pdf](https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf). Acesso em: 27 set. 2021;

PARLAMENTO EUROPEU. *The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data*. Disponível em: [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_pt#evento](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt#evento). Acesso em: 25 set. 2021;

PARLAMENTO JAPONÊS: *Amended Act on the Protection of Personal Information*. Disponível em: [https://www.ppc.go.jp/files/pdf/APPI\\_english.pdf](https://www.ppc.go.jp/files/pdf/APPI_english.pdf). Acesso em: 3 nov.. de 2021.

PEIXOTO, Erick Lucena Campos; ERHARDT JÚNIOR, Marcos. Os Desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. *Revista Jurídica Luso-Brasileira*. Ano 6, 2020. n. 2. Disponível em: [https://www.cidp.pt/revistas/rjlb/2020/2/2020\\_02\\_0389\\_0418.pdf](https://www.cidp.pt/revistas/rjlb/2020/2/2020_02_0389_0418.pdf). Acesso em: 13 jun 2021.

PESTANA, Márcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 09 nov. 2021.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021. 9786555595123. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 21 nov. 2021

Princípios da LGPD. *In: Governo Federal. Acesso à Informação. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/principios-da-lgpd>; Acesso em: 11 nov. 2021;*

Proteção de dados pessoais [recurso eletrônico] :glossário temático / Centro de Ensino e Pesquisa em Inovação da Escola de Direito de São Paulo da Fundação Getulio Vargas - São Paulo : CEPI-FGV Direito SP, 2021.

*Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. In: The Guardian, Londres, 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em 03 nov. 2021.*

THE ECONOMIST. *The world's most valuable resource is no longer oil, but data.* 2017, p. 1. Disponível em: [https://scholar.googleusercontent.com/scholar?q=cache:HpgPYRWKD7MJ:scholar.google.com/+o+modelo+europeu+de+prote%C3%A7%C3%A3o+de+dados&hl=pt-BR&as\\_sdt=0,5&as\\_ylo=2020](https://scholar.googleusercontent.com/scholar?q=cache:HpgPYRWKD7MJ:scholar.google.com/+o+modelo+europeu+de+prote%C3%A7%C3%A3o+de+dados&hl=pt-BR&as_sdt=0,5&as_ylo=2020). Acesso em 27 set. 2021

ROCHA, Elisa Corrêa da. O direito à autodeterminação informativa e a proteção de dados pessoais. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/134888/000986821.pdf?sequence=1&isAllowed=y>; Acesso em: 16 nov de 2021;

SARLET, Gabrielle Bezerra Sales. FERNANDES, Márcia Santana. RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. *In: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;*

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021.*

TEFFÉ, Chiara Spadaccini de. VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510/384> Acesso em: 16 nov. 2021;

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito, Estado e Sociedade: Políticas Públicas e Democracia), Universidade Nacional de Brasília – UNB, Brasília, 2007. Disponível em: [https://repositorio.unb.br/bitstream/10482/3358/1/2007\\_TatianaMaltaVieira.pdf](https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf). Acesso em: 09 jun. 2021.

VIOLA, Mario. TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º E 11. *In: Tratado de proteção de dados pessoais / coordenadores Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021;*