



UNIVERSIDADE DO SUL DE SANTA CATARINA
HENDRI NOGUEIRA

**A UTILIZAÇÃO DE DADOS PESSOAIS NO MEIO DIGITAL E A
(IM)POSSIBILIDADE DE LESÃO AO DIREITO À PRIVACIDADE**

Florianópolis
2019

HENDRI NOGUEIRA

**A UTILIZAÇÃO DE DADOS PESSOAIS NO MEIO DIGITAL E A
(IM)POSSIBILIDADE DE LESÃO AO DIREITO À PRIVACIDADE**

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina, como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Jeferson Puel, Msc.

Florianópolis

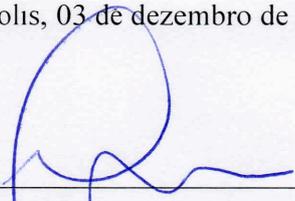
2019

HENDRI NOGUEIRA

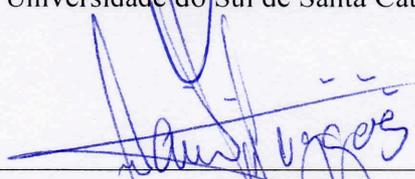
**A UTILIZAÇÃO DE DADOS PESSOAIS NO MEIO DIGITAL E A
(IM)POSSIBILIDADE DE LESÃO AO DIREITO À PRIVACIDADE**

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de bacharel em Direito e aprovado em sua forma final pelo Curso de Direito da Universidade do Sul de Santa Catarina.

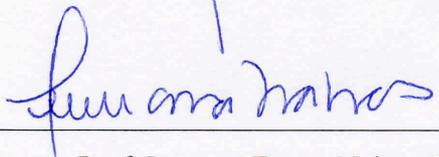
Florianópolis, 03 de dezembro de 2019



Prof. e orientador Jeferson Puel, Msc
Universidade do Sul de Santa Catarina



Prof. Wânio Wiggers, Msc.
Universidade do Sul de Santa Catarina



Prof Luciana Faisca Nahas, Dra.
Universidade do Sul de Santa Catarina

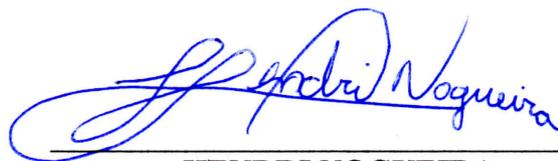
TERMO DE ISENÇÃO DE RESPONSABILIDADE

A UTILIZAÇÃO DE DADOS PESSOAIS NO MEIO DIGITAL E A (IM)POSSIBILIDADE DE LESÃO AO DIREITO À PRIVACIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico e referencial conferido ao presente trabalho, isentando a Universidade do Sul de Santa Catarina, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de todo e qualquer reflexo acerca deste Trabalho de Conclusão de Curso.

Estou ciente de que poderei responder administrativa, civil e criminalmente em caso de plágio comprovado do trabalho monográfico.

Florianópolis, 13 de novembro de 2019.



HENDRI NOGUEIRA

Dedico às minhas gatas, Késsia, Preta e Quindin.

AGRADECIMENTOS

Agradeço a todos aqueles que participaram desse projeto de vida, em especial à minha companheira Késsia Gomes de Lima, que juntos, ingressamos nesse desafio e me ajudou nas mais diversas etapas do processo.

Agradeço ao Professor Jeferson por ter acolhido a proposta de me orientar neste trabalho, esteve presente em todas os momentos requisitados, por ter me ensinado no decorrer do curso de graduação e mostrado ótimas técnicas para conclusão deste trabalho.

Aos meus pais, que apoiaram, insistiram e conseguiram formar um advogado na família, completando um super time (Engenheiro, Dentista, Médico e Advogado).

Aos meus colegas de classe e extraclasse, que pude compartilhar momentos divertidos com diversos *board games*, comida boa e papo de alto nível.

“Não devemos pedir aos nossos clientes que façam um equilíbrio entre privacidade e segurança. Precisamos oferecer-lhes o melhor de ambos. Em última análise, proteger os dados de outra pessoa é proteger a todos nós.” (Tim Cook).

RESUMO

O presente estudo tem por objetivo demonstrar em que hipóteses a utilização de dados pessoais caracteriza lesão ao direito à privacidade. Utiliza-se como método de abordagem o de pensamento dedutivo e de natureza qualitativa, viabilizado por meio do procedimento monográfico. A técnica de pesquisa adotada é a bibliográfica, com base em doutrinas, artigos científicos e a legislação. No desenvolver deste trabalho apresenta-se o conceito dos dados pessoais no meio digital, as formas de tratamento, a proteção caracterizada pelo consentimento, dados sensíveis e princípios, bem como a importância dos dados pessoais na contemporaneidade. Destaca-se a definição de direito à privacidade, a proteção constitucional subdividida em fundamento e titularidade, a privacidade no meio digital e a eficácia horizontal dos direitos fundamentais. Verifica-se, ainda, em que hipóteses a utilização de dados pessoais caracteriza-se lesão ao direito à privacidade, por meio de aspectos legais em vigor, com atenção ao Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. São mencionados pontos relevantes sobre a dignidade da pessoa humana e exemplos de decisões judiciais condizentes com o tema. Como resultado da presente pesquisa monográfica, ficou demonstrado que há possibilidade de lesão ao direito à privacidade nos termos das leis vigentes no país, quando não houver a utilização e o tratamento adequado dos dados pessoais.

Palavras-chave: Dados Pessoais. Privacidade. LGPD.

SUMÁRIO

1	INTRODUÇÃO.....	9
2	DADOS PESSOAIS NO MEIO DIGITAL.....	11
2.1	CONCEITO	11
2.2	FORMAS DE TRATAMENTO DE DADOS PESSOAIS.....	15
2.3	PROTEÇÃO	18
2.3.1	Consentimento	19
2.3.2	Dados sensíveis	21
2.3.3	Princípios	23
2.4	IMPORTÂNCIA DOS DADOS PESSOAIS NA CONTEMPORANEIDADE	25
3	DIREITO A PRIVACIDADE.....	29
3.1	CONCEITO	29
3.2	PROTEÇÃO CONSTITUCIONAL.....	33
3.2.1	Fundamento	33
3.2.2	Titularidade	35
3.3	PRIVACIDADE NO MEIO DIGITAL	38
3.4	EFICÁCIA HORIZONTAL DOS DIREITOS FUNDAMENTAIS.....	41
4	UTILIZAÇÃO DE DADOS PESSOAIS NO MEIO DIGITAL E A	
	(IM)POSSIBILIDADE DE LESÃO AO DIREITO À PRIVACIDADE	46
4.1	LEGISLAÇÃO	46
4.1.1	Marco Civil da Internet	47
4.1.2	Lei Geral de Proteção de Dados Pessoais.....	51
4.2	DIGNIDADE DA PESSOA HUMANA	55
4.3	DADOS PESSOAIS NO MEIO DIGITAL E A LESÃO AO DIREITO À	
	PRIVACIDADE	57
4.4	DECISÕES JUDICIAIS A RESPEITO DO TEMA.....	63
4.4.1	Recurso especial nº 1348532 / SP (2012/0210805-4)	63
4.4.2	Apelação cível nº 0703448-33.2017.8.07.0014 - Indenização por Dano Moral.....	65
5	CONCLUSÃO.....	67
	REFERÊNCIAS	69

1 INTRODUÇÃO

O consumo de serviços no meio digital está em crescimento e tomando proporções cada vez maiores. A transição de dados pela *internet* ocorre de uma maneira rápida e descomplicada. Com base nesse fato, os provedores de serviços no meio digital possuem a intenção de atrair cada vez mais usuários e consumidores, além de aumentar a divulgação de suas funções pela rede. Entretanto, a maioria dos serviços providos na rede requer a identificação dos usuários, solicitando dados pessoais para a realização de um cadastro. Os dados pessoais são informações desejadas pelos provedores, com o intuito de fornecer trabalhos personalizados, aumentar a visibilidade, prover o *marketing* e a propaganda, ou até mesmo ser utilizado para o envio de brindes.

A quantidade de cadastros realizados pelo usuário e a forma desenfreada de obtenção de dados pessoais pelos provedores de serviços, torna difícil o controle de quem as possuem, como utilizam e armazenam. Outra questão relevante é a captura de determinadas informações do usuário, sem o devido consentimento, o que culmina na utilização de forma irrestrita, influenciando na sua privacidade.

A partir dessas considerações, foi elaborado o seguinte problema de pesquisa: em que hipóteses a utilização de dados pessoais caracteriza lesão ao direito à privacidade?

O objetivo geral da presente monografia é demonstrar em que situações a utilização de dados pessoais caracteriza lesão ao direito à privacidade, permeado pelos seguintes objetivos específicos: descrever sobre os dados pessoais no meio digital; apresentar o direito à privacidade e suas principais particularidades; e verificar em que hipóteses a utilização de dados pessoais caracteriza lesão ao direito à privacidade.

A motivação do pesquisador está em conhecer meios legais que possa regularizar as atividades, obrigações e limites dos provedores de serviços, ao armazenarem, utilizarem e agregarem os dados dos usuários, além de verificar quais as possíveis sanções e penalidades podem ser atribuídas para aqueles que descumprem a norma. Essas medidas devem ser expostas para a sociedade como forma de prevenção e, também, de conhecimento dos direitos, para que possam requerê-los de forma adequada e ainda evitar que informações pessoais sejam fornecidas à terceiros sem o consentimento do titular ou de forma mal-intencionada.

O método de abordagem utilizado é de pensamento dedutivo, em razão da abordagem das situações gerais relacionados ao uso de dados pessoais e suas consequências. A partir dessas hipóteses, surgem questionamentos sobre quais normas na legislação brasileira podem fornecer subsídios para o usuário buscar os seus direitos. O método de abordagem

quanto à sua natureza é qualitativa, utilizando-se das informações e dos dados coletados. O método de procedimento utilizado é o monográfico com técnica de pesquisa bibliográfica, uma vez que efetua a coleta de informações em doutrinas, jurisprudências, leis, artigos científicos, dissertações e conteúdo de notícias dispostos em mídias virtuais.

A monografia está segmentada em três capítulos de desenvolvimento teórico, denominados respectivamente de dados pessoais no meio digital, direito à privacidade e a utilização de dados pessoais no meio digital e a (im)possibilidade de lesão ao direito à privacidade. No primeiro capítulo de desenvolvimento será retratado o conceito dos dados pessoais no meio digital, as formas de tratamento, a proteção caracterizada pelo consentimento, dados sensíveis e princípios, bem como a importância dos dados pessoais na contemporaneidade.

No segundo capítulo será apresentado a importância do estudo direito à privacidade, os conceitos do direito à privacidade (vida privada, honra e imagem) e a proteção constitucional subdividida em fundamento e titularidade, a privacidade no meio digital e a eficácia horizontal dos direitos fundamentais.

E, no terceiro capítulo, será verificado em que hipóteses a utilização de dados pessoais caracteriza-se lesão ao direito à privacidade, por meio de aspectos legais como Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD), bem como pontos relevantes sobre a dignidade da pessoa humana e a apresentação de decisões judiciais condizentes com o tema.

A pesquisa elaborada tem como colaboração a exposição sobre o tema e o alerta sobre a importância que os dados pessoais possuem na contemporaneidade. Os dados pessoais são valiosos e devem ser mantidos em segurança, seja no meio digital ou físico. Somente aqueles que possuem o controle, permissão ou consentimento devem ter acesso. O presente trabalho explicitará a utilização dos dados pessoais no meio digital e a (im)possibilidade de lesão ao direito à privacidade. A sociedade mundial está cada vez mais conferindo importância sobre os dados pessoais e a privacidade no meio digital, por isso é de suma importância o conhecimento dos seus direitos e a forma adequada de reivindicá-los.

2 DADOS PESSOAIS NO MEIO DIGITAL

A internet contempla serviços das mais variadas matizes para diversos objetivos e necessidades, das quais as pessoas sequer imaginariam que fossem utilizar. Os dados pessoais são utilizados nos cadastros dos serviços para identificação, autenticação e autorização dos usuários no meio digital. As empresas de *marketing* digital¹ realizam análises e tratamento dos dados sobre as pessoas, com o objetivo de conduzir propagandas e ofertas direcionadas. Outras, podem tratar dados sobre as pessoas para obter estatísticas e criar perfis (separando em grupos com características em comum).² Dessa forma, os dados pessoais são elementos valiosos no meio digital.³

Este capítulo dedica-se em descrever os principais conceitos acerca de dados pessoais no meio digital, explanar as diferentes formas de tratamento destes, bem como meios de proteção sob o viés do consentimento, os dados sensíveis e os princípios definidos na doutrina e na legislação brasileira. Por fim, será abordada a importância dessa temática na contemporaneidade.

2.1 CONCEITO

O dado pessoal está associado e relacionado a uma pessoa. Por meio de um (ou conjunto de) dado, deve ser capaz de identificar a pessoa, ou seja, o titular. É importante deixar expressa a diferença do conceito entre dados e informação. Um dado é uma palavra, sem qualquer significado relevante. Uma vez que se torna compreendido, com um significado e contexto, se transforma em informação. Os dados pessoais são informações, fatos, ações,

¹ Um conjunto de ações com objetivo de propagar a existência de produtos e serviços de uma empresa para possíveis clientes, realizar campanhas de propaganda, análise de viabilidade mercadológica e financeira, análise da demanda, pesquisar sobre o público alvo, auxiliar na captação de novos clientes, fazer atuais clientes a consumirem outros produtos, entre outros (TURCHI, 2019).

² BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 10 mar. 2019.

³ MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano B. S. A proteção de dados e o direito de personalidade da pessoa jurídica. **Revista de Direito Empresarial - RDEmp.** Belo Horizonte, ano 15, n. 3, p. 31-47, 2018. Disponível em: https://www.academia.edu/38017824/A_prote%C3%A7%C3%A3o_de_dados_e_o_direito_de_personalidade_d_a_pessoa_jur%C3%ADdica. Acesso em: 01 abr. 2019.

vontades e preferências que se referem um indivíduo identificado ou identificável.⁴ Por estarem relacionados a uma pessoa, são atributos que caracterizam a personalidade do indivíduo.

Os atributos, com características identificadoras, permitem reconhecer uma pessoa de forma única em um determinado contexto. No âmbito social e civil, por exemplo, o nome⁵ pode ser considerado um dado pessoal identificador. A agregação com outros dados é relevante e necessária para, de fato, identificar unicamente a pessoa, quando há mais de um indivíduo com o mesmo nome. O número de Cadastro de Pessoas Físicas (CPF) seria outro exemplo de dado pessoal, por ser único para cada cidadão brasileiro⁶ e, também, em razão do uso ser constante em cadastros e para a identificação do cidadão, principalmente em serviços públicos.⁷

A identificação e a associação de uma pessoa com seus dados podem ser minimizadas e até eliminadas. Há mecanismos para evitar a identificação direta e indireta dos dados à pessoa no meio digital: a pseudonimização e a anonimização dos dados. A primeira permite que os dados pessoais estejam associados ao titular de uma forma indireta. O mapeamento com a identificação do titular do dado pseudonimizado é realizado por intermédio de tratamentos complementares. Este mecanismo permite dificultar a associação direta dos dados pessoais a uma pessoa identificada ou identificável, por terceiros não autorizados. Um exemplo de pseudominimização poderá ocorrer durante a coleta de uma biometria. No procedimento da coleta, a biometria estaria associada diretamente a um número aleatório e, em outra estrutura de dados, ocorre o mapeamento desse número aleatório com o seu titular. O Regulamento Geral de Proteção de Dados da União Europeia (RGPD) definiu e normatizou o uso de pseudônimos no tratamento de dados pessoais.⁸

⁴ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

⁵ O nome é composto pelo prenome (nome próprio) e pelo patronímico (ou apelido de família). (MONTEIRO, 2016).

⁶ BRASIL. **Instrução Normativa RFB nº 1548, de 13 de fevereiro de 2015**. Dispõe sobre o Cadastro de Pessoas Físicas (CPF). Brasília, DF: Secretário da Receita Federal do Brasil, 2018. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=61197>. Acesso em: 13 abr. 2019.

⁷ BRASIL. **Decreto nº 9.723, de 11 de março de 2019**. Altera o Decreto nº 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto nº 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF (...). Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9723.htm. Acesso em: 13 abr. 2019.

⁸ UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia. 2016; L (119):1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 01 abr. 2019.

Os dados anonimizados já não permitem, por qualquer meio, que o seu titular seja identificado ou identificável.⁹ Dados anônimos tendem a ser utilizados para fins estatísticos, como censos demográficos e análises de mercado, que não necessita estar em conjunto com outros dados capazes a identificar a pessoa.

A tecnologia utilizada na contemporaneidade permite que os dados sejam armazenados em bancos de dados centralizados ou descentralizados. Também é possível segmentar a responsabilidade de autenticação, identificação e autorização com diferentes entidades, como o uso de serviços de autenticação de terceiros. Enquanto um fica responsável por prover a identidade do usuário, autenticando-o, o outro proveria o serviço originalmente requerido. Este é denominado como provedor de serviços, enquanto aquele é o provedor de identidade.¹⁰

No meio digital, o compartilhamento (tratamento) de dados pessoais na internet ocorre de forma frequente. Em algumas situações, esse tratamento é descrito, por exemplo, no termo de uso e privacidade do serviço. O *LinkedIn*¹¹ é um exemplo¹². Contudo, há hipóteses em que o tratamento dos dados ocorre sem qualquer cientificação, permissão ou consentimento do titular do dado. Uma tecnologia frequentemente utilizada por serviços na internet, para obter informações sobre o usuário sem qualquer consentimento, são os *cookies*¹³. Estes são utilizados para manter a sessão do usuário em um determinado site, ou seja, para evitar se autenticar frequentemente. Outro exemplo de uso é para promover anúncios publicitários, em que a publicidade ocorre de uma forma mais objetiva, reconhecendo suas preferências e possíveis necessidades e desejos, com anúncios de produtos recentemente pesquisados na internet (caso tenha realizado).¹⁴

⁹ AFFONSO, Elaine Parra. **A insciência do usuário na fase de coleta de dados: privacidade em foco**. 2018. Tese (Doutorado em Ciência da Informação) - Universidade Estadual Paulista, Marília, 2018. Disponível em: <http://hdl.handle.net/11449/154737>. Acesso em: 01 set. 2018.

¹⁰ SANTOS, Alfredo Luiz dos. **Gerenciamento de identidades: Segurança da informação**. Rio de Janeiro: Brasport, 2007.

¹¹ LINKEDIN. **Contrato do Usuário**. 2018. Disponível em: <https://www.linkedin.com/legal/user-agreement>. Acesso em: 05 abr. 2019.

¹² LINKEDIN. **Política de Privacidade**. 2018. Disponível em: <https://www.linkedin.com/legal/privacy-policy>. Acesso em: 05 abr. 2019.

¹³ Cookies é uma estrutura de dados utilizados pelos navegadores (e.g. internet Explorer, Firefox, Chrome) que permite armazenar diversas informações, sobre o dispositivo informático que o usuário está utilizando, o ambiente de rede, o histórico de sites visitados por exemplo. (GOODRICH; TAMASSIA, 2013).

¹⁴ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

Há empresas que possuem no modelo de negócio o tratamento de dados pessoais para agregar valores sobre seus produtos e serviços, dispor sobre a saúde empresarial e detalhes sobre a continuidade dos negócios. As empresas que lidam de forma mais direta com clientes precisam conhecer os perfis, as tendências, opiniões e preferências dos consumidores. As análises são realizadas com o tratamento de dados pessoais. O uso de *big data*¹⁵ e a técnica de mineração¹⁶ (*data mining*) permitem o tratamento massivo de dados, o que geram resultados, correlações, padrões de informações e gráficos para análises.¹⁷

Adicionalmente, há a inteligência artificial¹⁸, utilizada para elevar a experiência do usuário no decorrer do uso de serviços, o que permite implementar facilidades e previsões como, por exemplo, indicações no momento em que o consumidor estiver navegando em uma loja *on-line*, auxilia-lo na busca de um determinado produto ou na pesquisa por um restaurante ou lugar para conhecer. A inteligência artificial também é uma ferramenta importante para questões de segurança nacional, no sentido de analisar dados e informações histórica e a respeito das pessoas no meio digital, com o objetivo de prever atentados e crimes.¹⁹

Dessa maneira, prover serviços na internet significa que será acessado por qualquer pessoa que esteja conectada. A exposição é perigosa e o administrador do sistema deve aplicar meios tecnológicos suficientes, para proteger o conteúdo armazenado contra acessos indevidos. Os dados pessoais possuem um valor de mercado elevado e, por essa razão, determinadas condutas podem caracterizar crime como, por exemplo, acesso ilegítimo, interceptação ilegítima, interferência de dados, interferência em sistemas, falsidade ou fraude informática e furto de dados ou vazamento de informações.²⁰ Os riscos e a falta de controle que permeiam no

¹⁵ Definição dada para tratar e gerenciar um grande volume de dados com o objetivo de obter diversas informações para análises diversas. (MARÇULA; BENINI FILHO, 2019)

¹⁶ Técnica que utiliza a análise estatística e modelagens para descobrir padrões de relacionamentos desconhecidos em grandes bases de dados. (DE SORDI; MEIRELES, 2019)

¹⁷ BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 10 mar. 2019.

¹⁸ Inteligência Artificial é a reprodução do comportamento e da inteligência humana e de outros animais por meio de algoritmos computacionais para solucionar problemas complexos. (COPPIN, 2017).

¹⁹ MELO, Ricardo Rebelo Silva. Aplicabilidade de Inteligência Artificial nos dispositivos de Defesa das Forças Armadas. **O Comunicante**. Brasília-DF, v. 8, n. 3, p. 32-39, 2018. Disponível em: <http://www.ebrevistas.eb.mil.br/index.php/OC/article/view/1795>. Acesso em: 03 maio 2019.

²⁰ JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

meio digital, na internet, devem ser estudados e norteados pela legislação brasileira. Conseqüentemente, os cidadãos brasileiros terão segurança jurídica²¹ sobre seus dados.

A seguir será contextualizado a respeito das formas de tratamento de dados pessoais.

2.2 FORMAS DE TRATAMENTO DE DADOS PESSOAIS

O tratamento de dados pessoais é um conjunto de operações que podem ser realizadas com dados pessoais. A Lei nº 13.709/2018 que trata do regulamento de dados pessoais, define no art. 5º, inciso X que o tratamento é:

[...] 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.²²

O tratamento de dados pessoais ocorre em diversos setores, começando pela coleta. Nas relações de consumo, por exemplo, os dados dos consumidores possuem como principais fontes as transações comerciais, os censos e registros públicos, as pesquisas de mercado e de estilo de vida, os sorteios e concursos, concessão de créditos e os recursos exclusivamente informáticos.²³ Um ponto em comum, com exceção dos recursos exclusivamente informáticos, é a obtenção dos dados do consumidor por meio de um cadastro ou preenchimento de um formulário.

A publicidade direcionada, individualizada e personalizada é uma atividade utilizada com frequência.²⁴ Esse tipo de *marketing* e propaganda é possível se a empresa souber de informações a respeito de seus clientes (atuais e futuros).²⁵ Essas informações podem ser

²¹ Segurança jurídica, segundo Paulo Nader, ocorre "na hipótese de o Estado apresentar uma ordem jurídica bem definida, acessível ao conhecimento do cidadão comum e protetora dos direitos humanos fundamentais" (NADER, 2019, p. 78).

²² BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

²³ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

²⁴ OLSEN, Wendy. **Coleta de dados:** debates e métodos fundamentais em pesquisa social. Porto Alegre: Penso, 2015. *E-book*. Acesso restrito via Minha Biblioteca.

²⁵ NIQUE, Walter; LADEIRA, Wagner. **Como fazer pesquisa de marketing:** um guia prático para a realidade brasileira. 2. ed. São Paulo: Atlas, 2017. *E-book*. Acesso restrito via Minha Biblioteca.

obtidas a partir de uma pesquisa com a própria pessoa, que já teve algum contato com a loja ou produto. Alternativas de obtenção de dados ocorrem por meios indiretos, seja em razão das análises no meio virtual (por exemplo, detectar que o cliente acessou seu site e determinados produtos), por compartilhamento de dados com outras empresas ou até compra de dados com aqueles que o fazem.²⁶

Com os dados do indivíduo, as empresas podem realizar ações de *marketing*. Como exemplos pode-se citar o evento de *e-mails* com informações dos produtos que possui interesse, promoções, informativos, ligações e mensagem de texto ofertando planos. Entretanto, há empresas que exageram nessas ações de *marketing* que se tornam importunos e incomodam as pessoas.²⁷ Uma das atividades realizadas pelas empresas com o tratamento dos dados é a criação de perfis, por meio da técnica de *profiling*^{28,29}. Esse método utiliza-se de análises estatísticas e de técnicas de inteligência artificial, organiza e sintetiza hábitos, preferências pessoais e outros registros da pessoa.

Uma pessoa, no decorrer de sua vida, deverá disponibilizar seus dados pessoais ao poder público, seja por algum ato originário de uma obrigação pelo uso de um serviço público, seja por procedimentos perante a legislação comercial, trabalhista, previdenciária e o fisco (federal, estadual ou municipal), de forma direta ou indireta. Desse modo, os dados pessoais do cidadão estarão em mais de um banco de dados, armazenados e gerenciados por diferentes órgãos e entidades públicas. Cada entidade pública deve ter e manter uma política de segurança da informação, para evitar o tratamento e compartilhamento dos dados dos cidadãos além dos procedimentos previstos em lei.³⁰ A quantidade de dados que o setor público possui faz com que os órgãos sejam suscetíveis aos ataques de pessoas mal-intencionadas, vazamento, uso inadequado e não autorizado dos dados que possui sob sua custódia.

²⁶ SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 217-230, 2016. Disponível em: <http://revista.ibict.br/liinc/article/view/3719/3138>. Acesso em: 08 set. 2019.

²⁷ PRATES, Cristina Cantú. Privacidade e intimidade na internet: a legalidade dos cookies e spam. **Revista FMU Direito**. São Paulo, v 28, n. 42, p. 29-45, 2014. Disponível em: <http://revistaseletronicas.fmu.br/index.php/FMUD/article/view/676>. Acesso em: 10 jun. 2019.

²⁸ Técnica para elaborar perfis de comportamento de uma pessoa utilizando dados que ela disponibiliza sobre si. (DONEDA, 2006).

²⁹ MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. *E-book*. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y>. Acesso em: 04 abr. 2019.

³⁰ BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília, DF: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 31 ago. 2019.

Um exemplo de tratamento de dados que envolve a relação de consumo, as obrigações tributárias e de fiscalização pelo poder público, políticas públicas e programas sociais são os programas de notas fiscais. Estes programas foram criados para estimular os consumidores a exigirem a entrega do documento fiscal no momento da compra. Com esse documento, fazem os devidos registros do Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e a coleta pelo Estado. Entretanto, o funcionamento do programa necessita obter informações do consumidor, como o CPF e os dados da compra (itens adquiridos, quantidades, valores, local, dia e hora). Esses dados são armazenados tanto pelo estabelecimento quanto pela respectiva Secretaria da Fazenda Estadual.³¹ Com tantos dados pessoais coletados e armazenados em banco de dados de domínios distintos, permitem às entidades tratem os dados da maneira que desejarem, sem limitação e consentimento do consumidor final.

Desse modo, o tratamento dos dados pessoais, para a segurança pública, é uma questão controversa. De um lado está a necessidade de proteger a comunidade, a sociedade e a nação, que são importantes nas sociedades civilizadas, em especial em um Estado Democrático de Direito³². Do outro lado está o monitoramento constante das pessoas, sendo vigiadas pelas câmeras instaladas nas ruas, nos ônibus, para análise do que consomem, das atividades realizadas na internet com troca de *e-mails*, mensagens e nas redes sociais.³³ Por ser uma questão sensível, há um aumento de discussões que envolve os setores públicos e aqueles defensores contra o uso da tecnologia de reconhecimento facial pelo Estado.³⁴

Outra forma de tratamento de dados, que ocorre na sociedade contemporânea, são os sistemas de avaliação (*scoring*). Um sistema de avaliação de se destacar é o “*crediscore*” (ou “*credit scoring*”), que analisa dados dos consumidores e traçam perfis com o objetivo de auxiliar na concessão de crédito aos consumidores, de maneira a criar projeções das possibilidades do

³¹ MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de nota fiscal: um estudo de caso da Nota Fiscal paulista. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 351-365, 2016. Disponível em: <http://dx.doi.org/10.18617/liinc.v12i2.919>. Acesso em 04 abr. 2019.

³² “O Estado Democrático de Direito é a modalidade do Estado constitucional e internacional de direito que, com o objetivo de promover e assegurar a mais ampla proteção dos direitos fundamentais, tem na dignidade humana o seu elemento nuclear e na soberania popular, na democracia e na justiça social os seus fundamentos”. (RANIERI, 2019, p. 332).

³³ PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

³⁴ VARON, Joana. Bem na sua cara: a ilusão do reconhecimento facial para segurança pública. **Medium**, 04 maio 2019. Disponível em: <https://medium.com/codingrights/bem-na-sua-cara-a-ilus%C3%A3o-do-reconhecimento-facial-para-seguran%C3%A7a-p%C3%BAblica-47c708b34820>. Acesso em: 08 set. 2019.

indivíduo se tornar inadimplente.³⁵ Como resultado, cria-se um modelo de pontuação sobre o risco de inadimplência que o consumidor poderá ser incluído.

A inteligência artificial é uma tecnologia que poderá ser aplicada para tornar as análises dos dados pessoais automatizadas, com rapidez e precisão, na medida em que recebem os dados e as transformam em informações.³⁶ Uma tomada de decisão equivocada e incoerente poderá ser considerada como uma ação discriminatória, classificando incorretamente uma pessoa a partir de seus dados analisados.³⁷ Por esse motivo, é necessário limitar que as automatizações sejam configuradas ao ponto de alcançar em um resultado inadequado.

Com essas considerações, será contextualizada a proteção de dados.

2.3 PROTEÇÃO

A sociedade da informação do século XXI possui, como um dos principais ativos de maior valor, os dados pessoais.³⁸ A massificação do uso dos dados, nos diferentes contextos e finalidades, exige que sejam aplicados meios de proteção jurídica, para que as partes envolvidas (titular dos dados e os entes que os utilizam) possam ter garantias da plena liberdade da finalidade ao qual foi atribuída.³⁹

Neste tópico serão descritos a respeito do consentimento, como um instrumento de controle entre as partes envolvidas, a definição de dados sensíveis e a importância de uma maior proteção nessa classificação de dados e, por último, os princípios que fundamentam o tratamento de dados pessoais.

³⁵ PEZZELLA, Maria C. C.; GHISI, Silvano. A manipulação de dados pessoais nas relações de consumo e o sistema “crediscor”. **Civilistica.com**. Rio de Janeiro. v. 4, n. 1, p. 1-29, 2014. Disponível em <http://civilistica.emnuvens.com.br/redc/article/view/201>. Acesso em: 01 abr. 2019.

³⁶ COPPIN, Ben. **Inteligência artificial**. Rio de Janeiro: LTC, 2017. *E-book*. Acesso restrito via Minha Biblioteca.

³⁷ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

³⁸ SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 217-230, 2016. Disponível em: <http://revista.ibict.br/liinc/article/view/3719/3138>. Acesso em: 08 set. 2019.

³⁹ GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito**. Curitiba, v. 47, n. 0, p. 141-153, 2008. Disponível em: <https://www.revistas.ufpr.br/direito/article/view/15738>. Acesso em: 03 nov. 2019.

2.3.1 Consentimento

A disciplina da proteção de dados teve consequências em diversos setores econômicos, sociais e tecnológicos, de maneira que trouxe desafios para a tutela jurídica dos dados pessoais. No decorrer do século XX, houve quatro gerações de normas de proteção de dados pessoais na história global.⁴⁰

A primeira surgiu na década de 70 e foi contra a concepção de centralização de bancos de dados nos países. A segunda geração está relacionada ao consentimento do cidadão e o real exercício de sua liberdade de escolha. A terceira (iniciada na década de 80) é marcada pela formulação de um direito à autodeterminação informativa, fornecendo uma participação maior do cidadão sobre seus dados pessoais desde a coleta, o armazenamento e a transmissão. A quarta geração surgiu para tentar melhorar as gerações anteriores. Nesta última geração, algumas normas fortaleceram a posição do indivíduo por meio de normativas.⁴¹

De acordo com Laura Mendes⁴², alguns exemplos de leis que surgiram nesta geração: Lei Federal de Proteção de Dados alemã, legislação da Noruega, da Finlândia, da Dinamarca, da França, da Grã-Bretanha, da Suíça e a Diretiva Europeia sobre proteção de dados pessoais de 1995. A quarta geração caracteriza-se por fornecer aos cidadãos um melhor autocontrole sobre os dados pessoais, com a preocupação de não permitir que o titular dos dados considerados sensíveis possa decidir se fornece ou não, ou seja, cria-se uma imposição para a proteção dos dados sensíveis. O aumento de normas setoriais sobre a proteção de dados pessoais visa à complementação das normas gerais, fornecendo detalhes específicos e culturais para a proteção dos dados dos cidadãos dos respectivos países.⁴³

O consentimento do indivíduo sobre seus dados ganhou a devida importância na segunda geração de normas sobre os dados pessoais. Além das leis definidas nos países

⁴⁰ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

⁴¹ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**. Chapecó, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 maio 2019.

⁴² MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. Monografia (Dissertação de Mestrado em Direito) Universidade de Brasília, Brasília, 2008. Disponível em: <http://www.repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso em: 03 maio 2019.

⁴³ BEZERRA, Maria Ruth Borges. Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. **Caderno Virtual**. Brasília, v. 2, n. 44, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 03 nov. 2019.

normatizando mais poderes aos indivíduos, nas organizações internacionais também havia preocupação com o assunto, de modo que criaram guias (*guidelines*) e documentos estabelecendo padrões normativos. A Organização para Cooperação e Desenvolvimento Econômico (OCDE)⁴⁴ é um exemplo de organismo internacional multilateral que, desde 1980, percebeu-se que a tecnologia da informação estava influenciando o desenvolvimento econômico e social, de maneira a se fazer o uso de processamento dos dados pessoais dos cidadãos.⁴⁵

A OCDE emitiu, na década de 1980, dois importantes documentos: *privacy guidelines*⁴⁶ em 1980 e *declaration on transborder data flows*⁴⁷ em 1985. Esses documentos tiveram influência mundial no desenvolvimento da proteção dos dados pessoais, estabelecendo padrões normativos e princípios objetivando que todos os países membro tenham um ambiente regulatório uniforme, além de disseminar as orientações normativas no mundo.⁴⁸ Depois de 30 anos, as *guidelines* foram atualizadas e uma nova versão disponibilizada em 2013.

No decorrer das diferentes fases e o amadurecimento das legislações a respeito da proteção dos dados pessoais, o indivíduo ganhou liberdade para ter autodeterminação informativa, de maneira a controlar quais dados podem ser processados para suas respectivas finalidades.⁴⁹ No Brasil, a LGPD conceitua o consentimento no artigo 5º, inciso XII como sendo a “[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.”⁵⁰

A seguir serão efetuadas as considerações a respeito dos dados sensíveis.

⁴⁴ A missão da OCDE é promover políticas e normas que melhoram o bem-estar da economia e o social das pessoas ao redor do globo e atualmente é composta de 36 países membros. (OECD, 2019).

⁴⁵ VENTURA, Ivan. A relação entre a Lei de proteção de dados e o ingresso do Brasil na OCDE. **Consumidor Moderno**, São Paulo, mar. 2019. Disponível em: <https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/>. Acesso em: 09 set. 2019.

⁴⁶ OECD. **The OECD privacy framework**. Paris, 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 abr. 2019.

⁴⁷ OECD. **Declaration on transborder data flows**. Paris, 1985. Disponível em: <http://www.oecd.org/sti/ieconomy/declarationontransborderdataflows.htm>. Acesso em: 10 abr. 2019.

⁴⁸ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

⁴⁹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

⁵⁰ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 abr. 2019.

2.3.2 Dados sensíveis

Os dados podem ser classificados como sensíveis ou não. A LGPD conceituou no artigo 5º, inciso II que os dados sensíveis são aqueles “[...] sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.⁵¹ O objetivo dessa conceituação é a classificação dos dados que possam causar algum tipo de problema ou risco ao titular, como ser vítima de um ato preconceituoso, injúria ou discriminação em um eventual tratamento de dados.⁵²

Diferentemente da LGPD, o RGPD não conceitua os dados pessoais sensíveis de forma explícita. Por outro lado, no artigo 9º da RGPD⁵³ há normatização sobre os tratamentos de “categorias especiais de dados pessoais”, o que estabelece sobre a proibição do tratamento de dados pessoais.⁵⁴ É possível perceber uma similaridade nos tipos de dados que a regulamentação europeia normatiza, a respeito dos tratamentos de dados e na conceituação dos dados sensíveis da LGPD.

A proteção diferenciada quanto aos dados sensíveis reforça a preservação do direito à personalidade do indivíduo, à privacidade, à intimidade e à igualdade.⁵⁵ Os cuidados e as restrições quanto aos dados sensíveis devem ser mais exigentes, pois os efeitos de um tratamento indevido podem conduzir a vulneração dos princípios da dignidade da pessoa

⁵¹ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 abr. 2019.

⁵² SOUZA, Allan Rocha de *et al.* **Marcos legais nacionais em face da abertura de dados para pesquisa em saúde: dados pessoais, sensíveis ou sigilosos e propriedade intelectual**. Rio de Janeiro: Fiocruz, 2018. 123 p. Disponível em: https://www.arca.fiocruz.br/bitstream/icict/28838/4/Guanaes_Paulo_Org_Marcos_Legais_Presid%c3%aancia_2018.pdf. Acesso em: 14 ago. 2019.

⁵³ UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 01 abr. 2019.

⁵⁴ No inciso 1º do artigo 9º diz: “É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.” (UNIÃO EUROPÉIA, 2016).

⁵⁵ COPETTI, Rafael; MIRANDA, Marcel Andreatta de. Autodeterminação Informativa e Proteção de Dados: Uma Análise Crítica da Jurisprudência Brasileira. **Revista de Direito, Governança e Novas Tecnologias**. Minas Gerais, v. 1, n. 2, p. 28-48, 2015. Disponível em: <https://www.indexlaw.org/index.php/revistadgnt/article/view/46/43>. Acesso em: 30 mar. 2019.

humana⁵⁶ e os direitos fundamentais à intimidade e à vida privada.⁵⁷ Na hipótese de uma tomada de decisão baseada em análises dos dados sensíveis das pessoas, utilizando um procedimento manual ou automatizado (com a inteligência artificial, por exemplo), pode haver um efeito indesejado.⁵⁸ Esse resultado não esperado deve ser evitado para não causar consequências graves.

Nesse sentido, os dados pessoais genéticos trazem uma identidade (genética), de forma que revelam quatro diferentes vertentes: é conferida à humanidade, ou seja, todos a possuem; é involuntária e intrínseca à existência humana; é indestrutível e permanente; e singular.⁵⁹ Dessa forma, os dados genéticos podem revelar diversas informações intrínsecas ao titular, para o fim de identificá-los perante os outros, viabilizar o diagnóstico de enfermidades genéricas, detectar doenças graves e traçar históricos pessoais e familiares. Os dados genéticos são considerados sensíveis e devem ser manipulados com cautela.

Os dados pessoais relacionados à saúde, como os resultados de exames realizados em laboratórios e clínicas, prontuários dos pacientes nos hospitais e postos de saúde estão cada vez mais informatizados e digitais.⁶⁰ Estas informações denotam concepções sensíveis de seu titular, sendo que devem ter cuidado que os dados genéticos.

A seguir serão contextualizados os princípios aplicáveis a proteção dos dados pessoais.

⁵⁶ Art. 1º “A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...] III - a dignidade da pessoa humana [...]” (BRASIL, 1988).

⁵⁷ MACHADO, Joana de Moraes Souza. A tutela da privacidade no controle de dados pessoais no direito brasileiro. **Revista Jurídica Eletrônica da UFPI**. Teresina, v. 2, n. 02, p. 43-65, 2016. Disponível em: <http://www.ojs.ufpi.br/index.php/raj/article/viewFile/4671/2694>. Acesso em: 05 abr. 2019.

⁵⁸ DE LUCA, Cristina. Quem culpar quando a Inteligência Artificial falhar? **UOL**, São Paulo, 30 mar. 2019. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/03/30/quem-culpar-quando-a-inteligencia-artificial-falhar/>. Acesso em: 6 jun. 2019.

⁵⁹ COLUSSI, Fernando A. M.; SANTOS, Tomlyta L. V. dos. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. **Rev. de Biodireito e Direito dos Animais**. Porto Alegre, v. 4, n. 2, p. 1–21, 2019. Disponível em: https://www.researchgate.net/publication/330979819_NOVAS_TECNOLOGIAS_E_LIBERDADE_DE_EXPR_ESSAO_NA_PESQUISA_CIENTIFICA_UMA_ANALISE_SOBRE_A_PROTECAO_DE_DADOS_GENETICOS_E_DE_SAUDE. Acesso em: 30 mar. 2019.

⁶⁰ LIMA, M. I. Do Direito À Proteção De Dados Em Matéria De Saúde Na Sociedade De Informação. **Revista Arquivo Jurídico**. Teresina, v. 4, n. 1, p. 1-24, 2018. Disponível em: <http://www.ojs.ufpi.br/index.php/raj/article/view/7416/4303>. Acesso em: 30 mar. 2019.

2.3.3 Princípios

A proteção dos dados pessoais deve ser fundada em por princípios para orientação nas normativas e nos procedimentos. Para Canotilho, “princípios são normas que exigem a realização de algo, da melhor forma possível, de acordo com as possibilidades fácticas e jurídicas, [...] não proibem, permitem ou exigem algo em termos de “tudo ou nada”; impõem a otimização de um direito ou de um bem jurídico [...]”.⁶¹ Os princípios estabelecem um fim a ser atingido, uma finalidade, a fixação do conteúdo a ser atingido.⁶²

Os princípios de maior destaque para proteção de dados pessoais são: boa-fé; finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. A LGPD conceitua estes princípios no artigo 6º.⁶³

O primeiro princípio é o da boa-fé. Citado no *caput* do artigo 6º da lei, é basilar, geral do Direito, de maneira que se presume que as pessoas agem com boas intenções, com valores ético-jurídicos da probidade, honestidade, lealdade, o que segue o pacto contratual definido pelas partes.⁶⁴ No inciso primeiro, traz o princípio da finalidade cujo objetivo é garantir que o tratamento dos dados deve ter um propósito claro, objetivo, específico e legítimo. Para qualquer tratamento que vier a ser realizado, deve ser informado ao titular.⁶⁵ Dessa forma, aquele que coletou os dados não poderá realizar outro tipo de tratamento posterior que seja incompatível com as finalidades inicialmente definidas, ou seja, um *e-mail* coletado para fins de autenticação não poderá ser utilizado para enviar publicidade posteriormente.

O princípio da adequação diz respeito à compatibilidade que o tratamento dos dados é aplicado às finalidades que foram informadas ao titular. Em outras palavras, os dados solicitados pela empresa devem estar de acordo com as finalidades informadas.⁶⁶ Uma empresa

⁶¹ CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2010.

⁶² ÁVILA, Humberto. **Teoria dos Princípios: da Definição à Aplicação dos Princípios Jurídicos**. 4. ed. São Paulo: Malheiros Editores, 2015.

⁶³ “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios”(BRASIL, 2018).

⁶⁴ MARTINS-COSTA, Judith. **A boa-fé no direito privado: critérios para a sua aplicação**. 2. ed. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

⁶⁵ DONEDA, Danilo. A proteção da privacidade e de dados pessoais no brasil. **Revista Observatório Itaú Cultural**. São Paulo, n. 16, p. 136-150, 2014. Disponível em: <https://www.itaucultural.org.br/revista-observatorio-ic-n-16>. Acesso em: 04 jun. 2019.

⁶⁶ BORELLI, Alessandra; OLIVEIRA, Caio; MENDONÇA, Helena C. F. Coelho. Impactos da nova lei de proteção de dados pessoais nas instituições de ensino. **Revista Escola Particular**. São Paulo, v. 22, n. 249, p. 1-10, 2018. Disponível em:

que atua no setor de vendas on-line (*e-commerce*) não poderá solicitar, por exemplo, dados sobre a saúde do usuário.

Com o princípio da necessidade visa estabelecer uma limitação ao tratamento mínimo necessário para atingir às finalidades.⁶⁷ O do livre acesso permite que os titulares tenham acesso aos seus dados de forma fácil e gratuita, conhecendo sobre a forma, a duração do tratamento e a integralidade de seus dados mantidos pelas empresas.⁶⁸ Tanto o princípio da necessidade quanto o do livre acesso permitem garantir uma maior transparência dos controladores dos dados das pessoas, por limitar objetivamente os tratamentos dos dados pessoais às atividades específicas, poder mostrar ao titular quais dados possuem e como são tratados.

O princípio da qualidade dos dados garante aos titulares ter a ciência, de forma clara, exata e relevante sobre a atualização de seus dados nas empresas que as obtém. Os dados devem ser verdadeiros, atualizados e de acordo com a necessidade em cumprimento das finalidades de seu tratamento, sendo que complementa o princípio do livre acesso.⁶⁹ O princípio da transparência permite que os titulares tenham informações claras, precisas e de fácil acesso sobre a forma que os tratamentos são realizados, e quem são os agentes que possuem acesso aos dados.⁷⁰ A empresa não poderá compartilhar dados pessoais com pessoas e terceiros (operadores) sem ter informado ao titular.

O princípio da segurança garante ao titular que as empresas utilizarão medidas técnicas e administrativas, necessárias para proteger os dados pessoais de acessos não

https://www.academia.edu/38279183/Impactos_da_LGPD_para_Institui%C3%A7%C3%B5es_de_ensino. Acesso em: 20 out. 2019.

⁶⁷ MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de nota fiscal: um estudo de caso da Nota Fiscal paulista. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 351-365, 2016. Disponível em: <http://dx.doi.org/10.18617/liinc.v12i2.919>. Acesso em: 04 abr. 2019.

⁶⁸ BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protacao-de-dados-pessoais.pdf>. Acesso em: 10 mar. 2019.

⁶⁹ ARTESE, Gustavo. Compliance digital: proteção de dados pessoais. In: CARVALHO, André Castro *et al.* (org.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019. p. 477-501. *E-book*. Acesso restrito via Minha Biblioteca.

⁷⁰ REIS, Beatriz de Felipe; GRAMINHO, Vivian Maria Caxambu. A inteligência artificial no recrutamento de trabalhadores: o caso amazon analisado sob a ótica dos direitos fundamentais. In: XVI SEMINÁRIO INTERNACIONAL DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, 16. 2019, Santa Catarina. **XII Mostra Internacional de trabalhos Científicos**. Santa Catarina: EDUNISC, 2019. Disponível em: <https://online.unisc.br/acadnet/anais/index.php/sidsp/article/view/19599/1192612314>. Acesso em: 30 set. 2019.

autorizados.⁷¹ O da prevenção é a garantia de que as empresas adotarão as medidas cabíveis para prevenir a ocorrência de qualquer dano, em virtude do tratamento de dados pessoais.⁷² O princípio da não discriminação garante aos titulares que as empresas não realizarão, de forma alguma, tratamentos dos dados para fins discriminatórios, ilícitos ou abusivos.⁷³

O princípio da responsabilização e prestação de contas estabelece, por sua vez, que os agentes das empresas, ou seja, aqueles que terão acesso aos dados (controlador ou operador) devem adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, e sua eficácia.⁷⁴ Este princípio estabelece que as empresas devem provar e evidenciar que seguem às normas na sua integridade, mostrando as medidas adotadas, sua boa-fé e diligência.

A seguir será tratado a respeito da importância dos dados pessoais na contemporaneidade.

2.4 IMPORTÂNCIA DOS DADOS PESSOAIS NA CONTEMPORANEIDADE

O advento da era da informatização e a internet resultaram em uma mudança significativa na revolução industrial, na sociedade, nos novos paradigmas da comunicação, da informação e na globalização.⁷⁵ As mudanças surgiram para facilitar o dia a dia das pessoas. Por outro lado, o mau uso desses novos recursos poderá resultar em consequências danosas em diferentes esferas físicas e lógicas⁷⁶, sociais e pessoais.⁷⁷ Com uma concepção global cada vez mais digital, as informações estão sendo digitalizadas e mantidas nesse meio.

⁷¹ DONEDA, Danilo. A proteção da privacidade e de dados pessoais no Brasil. **Revista Observatório Itaú Cultural**. São Paulo, n. 16, p. 136-150, 2014. Disponível em: <https://www.itaucultural.org.br/revista-observatorio-ic-n-16>. Acesso em: 04 jun. 2019.

⁷² RUARO, Regina Linden. Direito fundamental à liberdade de pesquisa genética e à proteção de dados pessoais: os princípios da prevenção e da precaução como garantia do direito à vida privada. **Revista do direito público**. Londrina, v. 10, n. 2, p. 9-38, 2015. Disponível em: <http://www.uel.br/revistas/uel/index.php/direitopub/article/view/22298/16895>. Acesso em: 30 mar. 2019.

⁷³ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

⁷⁴ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

⁷⁵ LÉVY, Pierre. A revolução contemporânea em matéria de comunicação. **Revista Famecos**. Porto Alegre, v. 5, n. 9, p. 37-49, 1998. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/3009/>. Acesso em: 30 mar. 2019.

⁷⁶ GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores**. Porto Alegre: Bookman, 2013. *E-book*. Acesso restrito via Minha Biblioteca.

⁷⁷ PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 7. ed. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

O crescimento do desenvolvimento tecnológico e a disponibilização de serviços na internet traz o aumento de usuários e consumidores no meio digital. Essa massificação teve sérios impactos sobre os dados pessoais, na forma de armazenamento, manipulação, na quantidade e na qualidade dos dados⁷⁸. Houve uma mudança de visão no sentido de que se verificou que não é suficiente armazenar os dados para um fim específico, seria necessário utilizá-los para agregar valores aos negócios e à empresa.⁷⁹

Os serviços providos no meio digital são inúmeros, assim como as relações de consumo, modelos de negócios e *marketing* envolvidos. Alguns são acessíveis de forma “gratuita”, ao passo que outros exigem que o usuário pague para acessar determinados serviços e conteúdo. Os “gratuitos” são aqueles em que não há contraprestação pecuniária direta para o consumo do conteúdo por parte do usuário.⁸⁰

Na hipótese de um provedor de serviço e aplicativo o fornece de forma gratuita, e sabendo que há um custo a proporcionar e disponibilizar esses serviços, como que se consegue subsídios para manter os negócios e até obter lucro? A resposta está no uso dos dados pessoais na economia da informação, com foco na publicidade e *marketing*, nas diversas modalidades, como a publicidade direcionada, contextual, segmentada e comportamental on-line.⁸¹

Não é difícil perceber que na maioria dos sites, serviços e aplicativos disponíveis de forma gratuita no meio on-line (por exemplo, serviços de streaming de vídeo e música), há uma propaganda de um produto ou serviço, seja do mesmo provedor ou de terceiros. Há hipóteses em que a propaganda ocorre de forma consciente pelo usuário (pois teve que realizar um cadastro e consentir com os termos de uso) e, há situações em que a coleta dos dados e o

⁷⁸ FORTES, Vinícius Borges. **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**. 2015. Tese (Doutorado em Direito) - Universidade Estácio de Sá, Rio de Janeiro, 2015. Disponível em: <http://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf>. Acesso em: 22 set. 2019.

⁷⁹ SILVA, Norma Lúcia da. **Marketing digital como estratégia competitiva: o uso do portal digital do Banco do Brasil S.A.** 2016. Dissertação (Mestrado Profissional em Gestão Organizacional) - Universidade Federal de Goiás, Catalão, 2016. Disponível em: <https://repositorio.bc.ufg.br/tede/handle/tede/5828>. Acesso em: 22 set. 2019.

⁸⁰ DE ARAUJO, Luiz Ernani Bonesso; CAVALHEIRO, Larissa Nunes. A proteção de dados pessoais na sociedade informacional brasileira: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. **Revista Do Direito Público**, Londrina, v.9, n.1, p.209-226, jan./abr. 2014. Disponível em: <http://www.uel.br/revistas/uel/index.php/direitopub/article/view/16870/14321>. Acesso em: 30 mar. 2019.

⁸¹ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

seu tratamento ocorrem sem qualquer conhecimento do usuário/titular.⁸² Um dos métodos utilizados nessa hipótese seria o uso de *cookies*.

A relação de troca-troca, entre provedor e usuário, é relevante. O fornecimento de dados pessoais pelo usuário, em troca de funcionalidades e facilidades dos serviços providos, está cada vez mais presente. Em contrapartida, uma vez que o usuário decida não fornecer esses dados, fica proibido de utilizar/consumir esses serviços. O fato de poder utilizar, por exemplo, o serviço de geolocalização, por meio do Sistema de Posicionamento Global (GPS), presente nos *smartphones*, em conjunto com o aplicativo “*Google Maps*”⁸³, permite que o aplicativo conheça de sua localização e outros dados pessoais para prover o que foi requisitado.⁸⁴

O modelo de negócio, nesse momento da sociedade da informação, perfectibiliza a importância sobre os dados pessoais, monetizando-as, o que torna coerente a equação econômica daqueles produtos e serviços que são “gratuitamente” disponibilizados na internet.⁸⁵ O papel do consumidor elevou sua importância e estabelece as regras, de modo que o mercado deve pautar-se na constante atualização para suprir as necessidades do consumidor. Diversas técnicas permitem que sejam monitorados os hábitos de navegação dos usuários, suas atividades nas redes sociais e na internet.⁸⁶

A internet das coisas⁸⁷ é uma revolução, sendo que a tendência é que seu uso e consumo cresçam.⁸⁸ A aplicabilidade pode ocorrer nos mais variados ambientes e setores. Na saúde, por exemplo, dispositivos móveis com sensores podem monitorar pacientes, controlar o

⁸² MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

⁸³ Aplicativo e serviço de pesquisa e visualização de mapas e imagens de satélite da terra fornecido de forma gratuita pela empresa Google e está incluso, de forma nativa, nos smartphones cujo sistema operacional é o Android. (GOOGLE, 2019).

⁸⁴ JONES, Rhett. Ação judicial sobre rastreamento de localização escondido do Google pode ser um divisor de águas. **Gizmodo**, São Paulo, 21 ago. 2018. Disponível em: <https://gizmodo.uol.com.br/acao-judicial-rastreamento-localizacao-google-divisor-de-aguas/>. Acesso em: 5 abr. 2019.

⁸⁵ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

⁸⁶ SOUZA, Clayton de Almeida. Estratégia de Dados e Marketing Digital: Novas Formas de Aumentar Receitas e Diminuir Custos. **Revista IPTEC**. São Paulo, v. 6, n. 2, p. 92-107, 2018. Disponível em: <http://www6.uninove.br/ojs/journaliji/index.php/iptec/article/view/101/190>. Acesso em: 02 maio 2019.

⁸⁷ Internet das coisas é todo dispositivo computacional capaz de se conectar com outros dispositivos por meio de tecnologias e protocolos, em rede de comunicação para diversos fins, por exemplo: obter dados, controlar ações autônomas e monitorar ambientes. (MAGRANI, 2018).

⁸⁸ MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. *E-book*. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y>. Acesso em 04 abr. 2019.

fornecimento de medicação, qualidade do ar e a salubridade do ambiente.⁸⁹ Desse modo, poderiam facilitar a gestão de um hospital e trazer maior qualidade do serviço prestado.

Os carros autônomos são uma realidade. Os serviços de entrega e transporte permitem que a encomenda seja entregue diretamente no local desejado pelo consumidor, seja na via terrestre ou aérea utilizando-se de *drones*⁹⁰. Outro exemplo de uso seria nas zonas rurais, em que há diversos dispositivos espalhados pelo território e comunicando-se entre si, realizando o monitoramento e leitura das características do ar, do solo e do plantio.⁹¹

Para o ser humano, os dados pessoais fazem parte de um conjunto de elementos que moldam a sua personalidade, o que inclui a opção sexual, religião, local que estuda, local onde trabalha, até os produtos e os serviços que consome. Os dados permitem realizar uma análise sobre a personalidade da pessoa, “conhecendo-a” e classificando perfis de acordo com cada circunstância e momento. A sociedade da informação é dependente de dados pessoais para estabelecer as regras do mercado do consumo, promovendo o consumidor em um patamar diferenciado com o objetivo de receber, em troca a necessidade criada de consumir um produto, serviço ou conteúdo.⁹²

Este capítulo apresentou conceitos sobre dados pessoais no meio digital, os principais elementos que estão associados ao dado pessoal, características dos atributos, seja de um perfil de identificar ou caracterizar. Denota-se pelo exposto, que existem formas para a realização dos tratamentos de dados pessoais, de modo que há princípios a serem respeitados para que o tratamento dos dados.

O capítulo seguinte abordará sobre o direito à privacidade na contemporaneidade, os conceitos que envolvem essa temática e, além disso, a normatização existente na Constituição da República Federativa do Brasil a respeito da proteção à privacidade. Na sequência, serão abordados os da privacidade no meio digital e a eficácia horizontal dos direitos fundamentais.

⁸⁹ A INTERNET das Coisas na saúde. **Setor saúde**, Rio Grande do Sul, 22 out. 2015. Disponível em: <https://setorsaude.com.br/a-internet-das-coisas-na-saude/>. Acesso em: 30 abr. 2019.

⁹⁰ Veículo aéreo não tripulado que é controlado à distância por um piloto não embarcado ou de forma autônoma. (PRIEBE; PETRY, 2018).

⁹¹ GONÇALVES, Claudiana Freitas Botelho *et al.* Um estudo sobre a influência da IOT no agronegócio. **Revista Gestão, Inovação e Empreendedorismo**, v. 1, n. 1, 2018. Disponível em: <http://ojs.ciebe.com.br/index.php/GIE-METRO/article/view/2/4>. Acesso em: 30 abr. 2019.

⁹² ROSA, Renato de Oliveira; CASAGRANDA, Yasmin Gomes; SPINELLI, Fernando Elias. A importância do marketing digital utilizando a influência do comportamento do consumidor. **Revista de tecnologia aplicada**, v.6, n.2, p. 28-39, 2017. Disponível em: <http://www.cc.faccamp.br/ojs-2.4.8-2/index.php/RTA/article/view/1044/525>. Acesso em: 12 set. 2019.

3 DIREITO A PRIVACIDADE

Os dados pessoais fazem parte de um conjunto de elementos que moldam a personalidade. Por trás de um conjunto de dados, há uma série de informações que conferem significado à personalidade do seu titular. Do nome até a opção sexual, religiosa, locais que frequenta, estuda e trabalha, podem se tornar informações valiosas para diversos fins, principalmente para as empresas cujos produtos e soluções dependam dos dados pessoais.⁹³ Por esse motivo, os dados pessoais são bens que ganham cada vez mais valor, o que gera uma economia de dados pessoais de modo que a fonte deve ser protegida pelo titular.

Este capítulo abordará o conceito, a origem do direito à privacidade, de maneira a ilustrar a história e como iniciou a preocupação das pessoas com a privacidade. Na sequência, serão apresentados os fundamentos da Constituição da República Federativa do Brasil (CRFB), a respeito da garantia à privacidade e a sua titularidade. Por fim, são trazidos para a discussão elementos a respeito da privacidade no meio digital e a eficácia horizontal dos direitos fundamentais.

3.1 CONCEITO

No século XIX, o direito à privacidade começou a ser debatido na época em que novas tecnologias começaram a se tornar acessíveis ao público, sendo que se possibilitou que fizessem registros de fatos e a divulgação de forma que a esfera privada do indivíduo fosse invadida.⁹⁴ Na época, houve denúncias sobre imagens fotográficas em jornais e meios de comunicação sobre a vida privada. Desde então surgiu a necessidade de se discutir o “direito de ser deixado só”. O que era considerada uma atividade do dia a dia, caminhar pelas ruas sem incomodo ou registro, deixou de ser, pois alguém poderia utilizar-se da tecnologia para registrar e divulgar situações em momentos que o outro desejasse manter em segredo.⁹⁵

O termo privacidade contém algumas matizes de conceito. A obra de João Carlos Zanon aprofunda nessas diferenças de terminologias e semântica, sendo que a origem do termo

⁹³ SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 217-230, 2016. Disponível em: <http://revista.ibict.br/liinc/article/view/3719/3138>. Acesso em: 08 set. 2019.

⁹⁴ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

⁹⁵ WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, p. 195, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 01 abr. 2019.

a *privacy* trata da expressão de “privatividade” (de privativo), ao passo que há também sustentação no sentido de que o uso do termo “privacidade” se difundiu por ser utilizado na Constituição de Portugal e no Código Penal da República Portuguesa.⁹⁶ Para Danilo Doneda, em relação a doutrina brasileira, costuma-se utilizar alguns termos para se referir ao contexto de privacidade como, por exemplo: vida privada, intimidade, segredo, sigilo, recato, reserva, solidão e soledade.⁹⁷ Dessa forma, é possível verificar que o conceito de privacidade é amplo, sendo esta inerente em cada indivíduo.

O direito à privacidade, além de ser essencial para o livre desenvolvimento da personalidade humana, objetiva resguardar o comportamento e os acontecimentos relacionados à pessoa (o seu íntimo interior), que escolhe não ser de conhecimento público.⁹⁸ O direito à privacidade deve ser verificado como uma prerrogativa fundamental a ser resguardada. A personalidade humana, a dignidade e a intimidade também compõem este direito. A defesa da personalidade humana é fundamento para o direito à privacidade, contra injunções ou intromissões alheias.⁹⁹ Nesse sentido, a personalidade humana deve ter seu “espaço”, livre para poder desenvolver sem intromissões indesejadas de terceiros.¹⁰⁰

Em outras palavras, o domínio particular do ser humano deve ser protegido e garantido pela norma, pois o desenvolvimento da sua personalidade é um direito. Alexandre de Moraes destaca que a privacidade deve proteger o ser humano contra:

(a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional.¹⁰¹

No direito à personalidade, há elementos subjetivos de caráter individual como, por exemplo, o “[...] direito de buscar a paz de espírito e a tranquilidade, o direito de ser deixado só

⁹⁶ ZANON, João Carlos. **Direito à proteção dos dados pessoais**. São Paulo: Revista dos Tribunais, 2013.

⁹⁷ DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

⁹⁸ MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 14. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

⁹⁹ PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 7. ed. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰⁰ MOTTA, Sylvio. **Direito Constitucional: Teoria, Jurisprudência e Questões**. 28. ed. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰¹ MORAES, Alexandre de. **Direito constitucional**. 35. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

[...], o direito de não ser bisbilhotado, de não ter a vida íntima e familiar devassada, de não ter detalhes pessoais divulgados, nem de ter a imagem e o nome expostos contra a vontade da pessoa”¹⁰². Esses elementos são primordiais para o pleno desenvolvimento do ser humano, sem influências de terceiros e do próprio meio em que se desenvolve, de forma que lhe cabe a espontaneidade da livre escolha no decorrer da vida.

Para Sylvio Motta, a garantia constitucional da intimidade, “[...] qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em reconhecer, em favor da pessoa, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros na esfera de sua vida privada”¹⁰³.

A honra da pessoa humana deve ser protegida, pois nela está a dignidade, o bom nome e a sua reputação.¹⁰⁴ Um dos modos de se proteger de crimes contra a honra é a proibição em poder estar anônimo no meio digital. O anonimato dificulta a identificação das pessoas, caso cometam crime de difamação ou injúria. Não poder estar anônimo é uma limitação necessária da privacidade, pois o reconhecimento do autor contra possíveis danos causado contra alguém deve ser reparado.¹⁰⁵

Além da inviolabilidade da intimidade, a vida privada e da honra, a imagem também deve ser protegida. O direito à imagem pode ser dividido em duas modalidades: imagem retrato e imagem atributo. A imagem implica na reprodução gráfica (foto, desenho, filmagem) e também pode ser atributo, ou seja, um conjunto de características físicas desenvolvido pelo indivíduo e reconhecidas por terceiros. Em uma imagem há diversos dados pessoais, inclusive aqueles sensíveis (biometria facial, por exemplo).¹⁰⁶

O direito à imagem pode “[...] ser entendido em sentido objetivo, com relação à reprodução gráfica da pessoa, por meio de fotografias, filmagens, desenhos, ou em sentido subjetivo, significando o conjunto de qualidades cultivadas pela pessoa e reconhecidas como suas pelo grupo social.” Sendo assim, uma pessoa que teve sua imagem registrada por foto ou

¹⁰² MARMELSTEIN, George. **Curso de direitos fundamentais**. 8. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰³ MOTTA, Sylvio. **Direito Constitucional: Teoria, Jurisprudência e Questões**. 28. ed. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰⁴ SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰⁵ JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰⁶ CRUZ, Ariele Chagas; SARMENTO, George; SEIXAS, Taysa Matos. **Direitos humanos fundamentais: estudos sobre o art. 5º da Constituição de 1988**. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

vídeo, porém o material foi divulgado de forma pública sem o seu consentimento, tem a sua privacidade violada. Por outro lado, na hipótese desse registro ser realizado em um ambiente público, a violação à privacidade poderá não se caracterizar.¹⁰⁷

Na esfera do direito à privacidade, é interessante tratar a respeito do direito ao esquecimento. Segundo Maria Vital da Rocha:

O direito ao esquecimento aborda elementos do direito da privacidade de um lado e, do outro, garantias relacionado ao passado judicial, à repercussão social, aspectos da Lei de Acesso à informação, liberdade de informação, o respeito à intimidade, discussão entre fatos privados e públicos, fatos históricos, a principiologia decorrente dos direitos fundamentais e a dignidade da pessoa humana, interesse histórico e interesse público.¹⁰⁸

No Brasil, o direito ao esquecimento ganhou importância para discussão nas demandas judiciais, nas situações concretas com pedidos julgados pelo colendo Superior Tribunal de Justiça (STJ), envolvendo a chamada “Chacina da Candelária”¹⁰⁹ e o caso “Aida Curi”¹¹⁰. A complexidade dessa temática pelo tema faz com que haja a multidisciplinaridade com os diversos ramos do direito. No Brasil, ainda não se tem uma lei específica para exercício do direito ao esquecimento, porém em algumas leis esparsas como a LGPD e o Marco Civil da Internet há a normatização da eliminação dos dados dos usuários.¹¹¹ Estas leis serão demonstradas com mais detalhes no decorrer deste trabalho.

¹⁰⁷ MOTTA, Sylvio. **Direito Constitucional: Teoria, Jurisprudência e Questões**. 28. ed. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁰⁸ ROCHA, Maria Vital da; CUNHA, Isaac Rodrigues; OLIVEIRA, Karin de Fátima Rodrigues. Esquecimento, internet e “preferência” da informação: possibilidades de aplicação da doutrina dos preferred rights da jurisprudência norte-americana ao caso brasileiro. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, n. 3, 2017, p. 483-509. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4969/3674>. Acesso em: 30 mar. 2019.

¹⁰⁹ BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.335.153, Nelson Curi E Outros**. Relator: Ministro Luís Felipe Salomão. 28 de maio de 2013. Disponível em: <https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj-aida.pdf>. Acesso em: 05 nov. 2019.

¹¹⁰ BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.334.097, Globo Comunicações E Participações S/A**. Relator: Ministro Luís Felipe Salomão. 28 de maio de 2013. Disponível em: <https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj.pdf>. Acesso em: 05 nov. 2019.

¹¹¹ PORTO, Noemia Aparecida Garcia. Direito ao esquecimento: memória, vida privada e espaço público. **Revista do Tribunal Regional do Trabalho da 10ª Região**, Brasília, DF, v. 19, n. 20, p. 104-122, 2015. Disponível em: <https://hdl.handle.net/20.500.12178/85646>. Acesso em: 30 abr. 2019.

3.2 PROTEÇÃO CONSTITUCIONAL

A Constituição da República Federativa do Brasil normatiza os direitos fundamentais para proteção como, por exemplo, quanto a intimidade, a vida privada, a honra, a imagem, além do sigilo da correspondência e das comunicações. Há também regulamento no Texto Constitucional específicos para a proteção de dados das pessoas que possuem registros em banco de dados de entidades governamentais. Entretanto, os dispositivos constitucionais (que já possuem mais de trinta anos) não foram positivados de forma expressa, de modo a possibilitar uma interpretação mais consistente sobre o nível de proteção constitucional a respeito das matérias da privacidade e proteção de dados pessoais.¹¹²

Neste tópico será abordada a proteção constitucional no tocante da privacidade e aos dados pessoais, subdividida em dois itens: Fundamento e Titularidade. No primeiro serão destacadas as regras legais contidas na Constituição da República Federativa do Brasil a respeito dessa temática, e no segundo quem seriam aqueles que estão protegidos pelo ordenamento jurídico.

3.2.1 Fundamento

A Constituição da República Federativa do Brasil traz no inciso X do artigo 5º a seguinte redação: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação”¹¹³. Segundo Moraes, a proteção constitucional à vida privada inclui os direitos à intimidade e à própria imagem, considerado um espaço íntimo intransponível por intromissões ilícitas e externas. A intimidade trata da relação subjetiva do íntimo da pessoa, seja nas relações familiares, amizades, ou nas relações objetivas como, por exemplo, as comerciais e de trabalho.¹¹⁴

¹¹² SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹¹³ BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 mar. 2019.

¹¹⁴ MORAES, Alexandre de. **Direito constitucional**. 35. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

A garantia a inviolabilidade da intimidade, a vida privada, a honra e a imagem das pessoas são definidas no inciso X do artigo 5º da Constituição da República Federativa do Brasil. Porém, qual seria a compreensão de dados pessoais dentro dessas garantias expressas? A palavra “dados”, sem a associação expressa com a palavra “pessoais”, está pouco presente no Texto Constitucional. Em apenas três dispositivos constitucionais está presente: no inciso XII do artigo 5º¹¹⁵ e nas alíneas “a” e “b” do inciso LXXII desse mesmo dispositivo constitucional.¹¹⁶

No inciso XII do artigo 5º da Constituição da República Federativa do Brasil é mencionado o termo “dados”, porém não esclarecido a respeito de sua verdadeira origem e aplicabilidade. Segundo Tercio Sampaio Ferraz Jr, a expressão “os dados” que está no inciso não são objetos de proteção constitucional, de forma que essa referência trata da comunicação, no interesse da defesa da privacidade.¹¹⁷ Assim, os dados estariam estritamente associados ao conteúdo de uma comunicação.

Gilmar Mendes sustenta que não se pode confundir a comunicação e registros telefônicos, pois ambos recebem uma proteção jurídica distinta, ou seja, a proteção constitucional é da comunicação de dados e não dos dados.¹¹⁸ Assim, a garantia geral de proteção de dados pessoais pode ser interpretada constitucionalmente, por meio da verificação no sistema de direitos fundamentais, com o uso da ação de *habeas data* e do princípio fundamental da dignidade humana, o que amplia a garantia de inviolabilidade da intimidade e da vida privada.¹¹⁹ Dessa forma, Walter Claudius Rothenburg explica que:

O habeas data tem a natureza jurídica de uma ação judicial e funciona como uma garantia constitucional ao direito de informação (CR, art. 5º, XIV) a respeito de dados pessoais – estejam eles sob sigilo (o que é mais comum) ou não; ao direito de

¹¹⁵ “Art. 5º [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]” (BRASIL, 1988).

¹¹⁶ “Art. 5º [...] 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, 1988).

¹¹⁷ FERRAZ JÚNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Da Faculdade De Direito**. São Paulo, v. 88, p. 439-459, 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 15 jul. 2019.

¹¹⁸ MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 14. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹¹⁹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

privacidade e de imagem (CR, art. 5º, V e X), bem como ao direito de petição (CR, 5º, XXXIV).¹²⁰

Desse modo, o *habeas data* é a proteção constitucional que mais se aproxima do termo “dados” como “dados pessoais”. A primeira parte da lei faz relação aos dados pessoais que estão associados aos bancos de dados de entidades governamentais ou de caráter público (conforme alínea ‘a’ do inciso LXXII). Na alínea ‘b’, a palavra pode ter sido empregada com o sentido similar ao de informação.¹²¹ O fato é que o *habeas data* não pode ser utilizado para dados pessoais em entidades privadas.

Em se tratando de proteção dos dados pessoais e as regras sobre o tratamento, as leis e garantias constitucionais são genéricas, insatisfatórias, sendo necessária uma regulamentação por legislação específica.¹²² Por outro lado, com uma visão contrária, Patrícia Peck comenta que a maior controvérsia está na “[...] falta de entendimento quanto à aplicação de leis em vigor para questões relativamente novas, que exigem uma interpretação da norma e sua adequação ao caso concreto [...]”¹²³, e não nas leis propriamente dito. Apesar dessas diferenças, deve-se destacar a importância da legislação em atender as mudanças que a sociedade transpassa no decorrer dos anos, com a influência de novas tecnologia e paradigmas.

Com essas considerações, a seguir será tratado a respeito da titularidade alusiva a proteção constitucional.

3.2.2 Titularidade

O artigo 5ª da Constituição da República Federativa do Brasil estabelece no *caput* o seguinte trecho: “[...] garantindo-se aos brasileiros e aos estrangeiros residentes no País [...]”.¹²⁴ Inicialmente parece uma regra bem restritiva, porém essa questão foi verificada pelos

¹²⁰ ROTHENBURG, Walter Claudius. **Direitos fundamentais**. Rio de Janeiro: Forense, São Paulo: MÉTODO, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

¹²¹ SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro**: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. São Paulo: LTr, 2014. 192 p.

¹²² MACHADO, Joana de Moraes Souza. A tutela da privacidade no controle de dados pessoais no direito brasileiro. **Revista Jurídica Eletrônica da UFPI**, Teresina, v. 2, n. 02, p. 43-65, 2016. Disponível em: <http://www.ojs.ufpi.br/index.php/raj/article/viewFile/4671/2694>. Acesso em: 05 abr. 2019.

¹²³ PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

¹²⁴ “Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]” (BRASIL, 1988).

doutrinadores e juristas com o objetivo de esclarecer, se os direitos fundamentais são para aqueles definidos estritamente no dispositivo constitucional em questão, ou há outros elementos capazes de abranger as pessoas, independentemente de sua nacionalidade e residência.¹²⁵ No decorrer deste tópico, serão abordadas essas questões.

Primeiramente, é importante destacar a diferença entre ser titular de um direito e ter capacidade de direito, e de fato. Capacidade de direito seria a aptidão para ser titular de direitos e obrigações, ao passo que a capacidade de fato é a aptidão concreta para o seu exercício¹²⁶. Pode-se ter condições para ser titular de um direito, mas não ter a capacidade para exercer as faculdades inerentes a essa prerrogativa. Crianças e adolescentes, por exemplo, são titulares de direitos, porém a capacidade (de fato) para exercê-los não possuem em razão de sua condição de pessoa em desenvolvimento.¹²⁷

Apesar do *caput* do artigo 5º da Constituição da República Federativa do Brasil garantir os direitos fundamentais aos brasileiros e aos estrangeiros residentes no país, na jurisprudência¹²⁸ já se discutiu o assunto, de forma a se estabelecer que os direitos fundamentais se aplicam a todos os seres humanos, ou seja, a Constituição da República Federativa do Brasil garante o princípio da universalidade. Ingo Sarlet, Luiz Marinoni e Daniel Mitidiero definem que no princípio da universalidade inclui:

[...] todas as pessoas, pelo fato de serem pessoas são titulares de direitos e deveres fundamentais, o que por sua vez, não significa que não possa haver diferenças a serem consideradas, inclusive, em alguns casos, por força do próprio princípio da igualdade, além de exceções expressamente estabelecidas pela Constituição, como dá conta a distinção entre brasileiro nato e naturalizado, algumas distinções relativas aos estrangeiros, entre outras.¹²⁹

Para Guilherme Peña de Moraes “[...] os direitos fundamentais podem ser titularizados por pessoas enquanto tais, brasileiras, estrangeiras ou apátridas, naturais ou jurídicas, que disponham de capacidade de fato ou de exercício, ou não”. Essa titularidade, no

¹²⁵ NUNES JÚNIOR, Flávio Martins Alves. **Curso de direito constitucional**. 3. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹²⁶ MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 14. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹²⁷ ZAPATER, Máira. **Direito da criança e do adolescente**. São Paulo: Saraiva Educação, 2019.

¹²⁸ BRASIL. Supremo Tribunal Federal. **Recurso Especial nº 587.970, Instituto Nacional Do Seguro Social - INSS**. Relator: Min. Marco Aurélio. 20 de abr. de 2017. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=2621386>. Acesso em: 01 nov. 2019.

¹²⁹ SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

âmbito dos direitos fundamentais, também não se restringe à nacionalidade, cor, crença, ou opção sexual.¹³⁰ Não há restrição nessa vertente para ser titular de direitos fundamentais. Nesse sentido George Marmelstein comenta:

Qualquer pessoa, em regra, pode ser titular de direitos fundamentais, não importando a cor da pele, a condição financeira, a orientação sexual, a idade, a nacionalidade ou qualquer outro atributo. Não é necessário sequer que a pessoa seja plenamente capaz. Pode ser menor de idade, idoso, portador de deficiência mental etc. Basta que seja um ser humano.¹³¹

O princípio da dignidade da pessoa humana (artigo 1º, III da CRFB) permite abranger diversos direitos, sendo que não se excepciona em razão da nacionalidade.¹³² Não se pode confundir, todavia, essa universalidade verificada nos direitos fundamentais com outras prerrogativas cuja limitação se faz necessária, como os direitos políticos e sociais (como o direito ao trabalho), que são limitados aos brasileiros ou estrangeiros residentes no País.¹³³

É oportuno destacar que o estrangeiro não residente no Brasil pode ter a sua titularidade atribuída aos direitos fundamentais por, pelo menos, três critérios: por força do princípio da universalidade, em conjunto com o da dignidade da pessoa humana; pela própria Constituição da República Federativa do Brasil; e pelos direitos previstos nos tratados internacionais dos quais o Brasil seja parte (art. 5º, § 2º, da CRFB).¹³⁴ Um exemplo de tratado internacional seria o Pacto de San José da Costa Rica¹³⁵ que, no artigo 1º normatiza a obrigação de respeitar os direitos do ser humano.¹³⁶ Assim os pactos internacionais têm uma importância nas relações e garantias aos direitos fundamentais.

¹³⁰ MORAES, Guilherme Peña de. **Curso de Direito Constitucional**. 11. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹³¹ MARMELSTEIN, George. **Curso de direitos fundamentais**. 8. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹³² MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 14. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹³³ NUNES JÚNIOR, Flávio Martins Alves. **Curso de direito constitucional**. 3. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹³⁴ SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹³⁵ BRASIL. **Decreto nº 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 1992. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1992/decreto-678-6-novembro-1992-449028-publicacaooriginal-1-pe.html>. Acesso em: 22 de set. 2019.

¹³⁶ “Art. 1º- Obrigação de respeitar os direitos: 1. Os Estados-partes nesta Convenção comprometem-se a respeitar os direitos e liberdades nela reconhecidos e a garantir seu livre e pleno exercício a toda pessoa que esteja sujeita à sua jurisdição, sem discriminação alguma, por motivo de raça, cor, sexo, idioma, religião, opiniões políticas ou de qualquer natureza, origem nacional ou social, posição econômica, nascimento ou qualquer outra condição social. 2. Para efeitos desta Convenção, pessoa é todo ser humano.” (BRASIL, 1992).

A seguir será tratado a respeito da privacidade no meio digital.

3.3 PRIVACIDADE NO MEIO DIGITAL

A Era da Informação, que iniciou no final do século XIX, trouxe novas tecnologias e permitiu facilitar a comunicação. Ocorreu um aumento do tráfego do volume de informações por meio do uso de telefone, cinema, rádio e a televisão.¹³⁷ Na sociedade verificou-se ampla inclusão às novas tecnologias digitais no século XX, na década de 70 com a informatização, início da popularização da *internet* na década de 80, acessibilidade ao microcomputador (computador doméstico) e da *internet* na década de 90. No início do século XXI, a expansão das tecnologias sem fio (equipamentos de rádio frequência, telefones móveis, etc).¹³⁸ Não demorou para que se migrasse do analógico para o digital, de maneira a fornecer uma maior velocidade na comunicação e um modelo descentralizado no compartilhamento das informações.¹³⁹

Com a tecnologia disponível para as pessoas, com mecanismos que facilitam o dia a dia, a realização de determinadas atividades pessoais e profissionais, será possível estar a margem do mundo digital? Já imaginou a vida contemporânea sem equipamentos e solução digital ao seu redor? Redes sociais, *smartphones*, *e-mail*, aplicativos de mensagens (por exemplo, o *whatsApp*), documentos pessoais digitais, serviços público prestados em um ambiente cada vez mais virtualizado, monitoramento público, formas alternativas de pagamento (por exemplo cartão de créditos virtuais e *chips* sem contato), instituições financeiras “virtuais”, são exemplos de possíveis serviços e equipamentos que uma pessoa pode utilizar no dia a dia.

Uma vez que os dados de uma pessoa estão no meio digital (não apenas os dados em si, mas as imagens, vídeos e mensagens), sua privacidade pode ser comprometida. Um simples “vazamento” daquelas informações para um ambiente não controlado é o suficiente para perder a privacidade.¹⁴⁰ Com tantas empresas e serviços disponíveis na *internet*, fica difícil obter um controle sobre os dados e a privacidade que cada fornecedor diz cumprir e fornecer

¹³⁷ PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

¹³⁸ FREIRE, Emerson; BATISTA, Sueli Soares dos Santos. **Sociedade e tecnologia na era digital**. São Paulo: Érica, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

¹³⁹ PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁴⁰ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

para o usuário. Em 2019, a *Electronic Frontier Foundation* (EFF) publicou o resultado de uma de suas pesquisas, em que avalia seis itens sobre a privacidade das organizações:

A transparência em reportar as requisições de remoção do governo com base nas solicitações legais; a transparência em reportar as requisições de remoção do governo alegando as violações na plataforma de políticas; o fornecimento de notificações aos usuários sobre cada remoção de conteúdo e suspensão de conta; se fornece aos usuários um processo de questionamento para contestar quedas e suspensões; a transparência em relação ao número de recursos; se tem apoio público aos Princípios de Santa Clara¹⁴¹.¹⁴²

Essa pesquisa da EFF, de 2019, demonstra que poucas empresas ainda estão em total conformidade com os itens esperados, no tocante a privacidade do usuário de forma transparente.

Outra pesquisa realizada pela EFF, é na proteção dos dados dos usuários relacionados às requisições que o governo dos Estados Unidos faz para as empresas. A última pesquisa desta natureza foi realizada em 2017.¹⁴³ Nessa pesquisa, a EFF avalia se as empresas seguem as melhores práticas sobre as requisições de dados dos usuários pelo governo, se avisam seus usuários sobre essas requisições, se prometem aos usuários que não comercializam os dados pessoais, se publicam pedidos toda e qualquer solicitação do governo em obter dados do usuário e, ainda, se a empresa tem posição alinhada as mudanças nas regras do governo sobre a obrigação no fornecimento dos dados pessoais. Verifica-se dessa modalidade de pesquisa o aumento da segurança das empresas ao proteger os dados pessoais de seus usuários contra as requisições do governo americano.

Assim, o ambiente digital pode ser um paradoxo difícil de administrar. Por um lado, há uma gama de ferramentas e serviços disponíveis para o uso na *internet*, que auxiliam o dia a dia em diversas atividades. Esse ambiente e as próprias ferramentas podem conter lacunas na segurança, ou, por vezes, o usuário não tem habilidade suficiente para gerenciar de forma segura toda essa tecnologia. As pessoas que possuem um perfil mal-intencionado tendem a aproveitar dessas lacunas e da falta de experiência dos usuários, para aplicar golpes, furto de dados,

¹⁴¹ Princípios de Santa Clara são elementos iniciais para prover níveis mínimos de transparência e prestação de contas que se espera de uma organização. (SANTA CLARA UNIVERSITY, 2019).

¹⁴² GEBHART, Gennie *et al.* **Who has your back? Censorship Edition** 2019. San Francisco, 2019. Disponível em: <https://www.eff.org/wp/who-has-your-back-2019>. Acesso em: 06 out. 2019. Tradução nossa.

¹⁴³ REITMAN, Rainey *et al.* **Who has your back? Government Data Requests** 2017. San Francisco, 2017. Disponível em: <https://www.eff.org/who-has-your-back-2017>. Acesso em: 06 out. 2019.

estelionatos e outros crimes informáticos. Muitos desses delitos envolvem a obtenção de dados pessoais, para se chegar ao objetivo de consumir o crime.¹⁴⁴

A falta de privacidade no meio digital é um assunto conhecido, porém pouco discutido no Brasil até a segunda década do século XXI. Uma demanda que ganhou projeção popular e da mídia, foi o caso da atriz brasileira Carolina Dieckmann, que teve seu equipamento informático invadido, subtraído arquivos pessoais e publicados na *internet*.¹⁴⁵ Alguns desses arquivos continham fotos íntimas. Essa situação fática resultou em elemento para se realizar alterações no Código Penal em 2012, para tipificar os crimes de invasão de dispositivo informático¹⁴⁶. Esse tipo de crime ocorre a invasão de qualquer equipamento informático de terceiros, com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização, ou instalar vulnerabilidades para obter vantagem ilícita. A lei também incluiu a falsificação de cartão de crédito ou débito como crime de falsificação de documentos particular.¹⁴⁷

No cenário mundial, um dos escândalos com grandes proporções foi aquele relativo à espionagem e vigilância cibernética pela *internet* e outros meios de comunicação, que atingiram a Agência Nacional de Segurança (ANS) dos EUA em 2013. Essa demanda foi revelada por Edward Snowden, que trabalhava na ANS e divulgou informações sigilosas, formas como os cidadãos americanos estavam sendo vigiados, além de autoridades de outros países também.¹⁴⁸ A vigilância que os órgãos do governo americano realizaram fez com que surgisse um alerta para as autoridades mundiais, especialistas da área e nas relações

¹⁴⁴ JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁴⁵ OLIVEIRA, Jane Resina F. de. **Lei Carolina Dieckmann: antes tarde do que nunca**. São Paulo, 2012. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI169090,41046-Lei+Carolina+Dieckmann+antes+tarde+do+que+nunca>. Acesso em: 08 out. 2019.

¹⁴⁶ “Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.” (BRASIL, 1940).

¹⁴⁷ BRASIL. **Lei nº 12.737, DE 30 DE NOVEMBRO DE 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 08 out. 2019.

¹⁴⁸ FAVERA, Rafaela Bolson Dalla; SILVA, Rosane Leal da. Cibersegurança na União Europeia e no Mercosul: Big Data e Surveillance Versus Privacidade e Proteção de Dados na Internet. *Revista de Direito, Governança e Novas Tecnologias*. Curitiba, v. 2, n. 2, p. 112-134, 2016. Disponível em: <https://www.indexlaw.org/index.php/revistadgnt/article/view/1490/pdf> Acesso em: 30 mar. 2019.

internacionais. A divulgação foi no sentido de demonstrar à população mundial, que as potências mundiais podem vigiar qualquer pessoa.¹⁴⁹

As mensagens de texto escritas em aplicativos de *chat*, *e-mails*, arquivos e documentos, mensagens de voz, ligações telefônicas, imagens e vídeos de equipamentos de monitoramento de vigilância, os *sites* na *internet* são exemplos do que a ANS pode vigiar as pessoas e verificar comportamentos.¹⁵⁰ Mesmo estando “*offline*”, a vigilância das pessoas ainda pode ocorrer através de serviços disponíveis pelo próprio Estado, seja uma câmera instalada na rua, no ônibus ou ao realizar uma compra em uma loja.¹⁵¹

Conforme ficou apurado, a privacidade no meio digital é uma questão complexa. Enquanto a tecnologia, por um lado pode ajudar nas atividades diárias, por outro é de permitir a invasão da privacidade das pessoas. Meios técnicos podem ser utilizados para prover uma maior segurança (o uso de criptografia, por exemplo), porém é limitado para algumas situações como, por exemplo, para promover integridade, confidencialidade e autenticidade. Para serviços de terceiros e do Estado, não é possível garantir a privacidade plena. O Estado teria que garantir níveis de privacidade aos cidadãos por meio de normas técnicas e leis que exijam o dever de fazer e não fazer das entidades, garantia dos direitos ao cidadão.¹⁵²

Com essas considerações, a seguir será tratado a respeito da eficácia horizontal dos direitos fundamentais.

3.4 EFICÁCIA HORIZONTAL DOS DIREITOS FUNDAMENTAIS

Direitos fundamentais são “[...] posições jurídicas reconhecidas e protegidas na perspectiva do direito constitucional interno dos Estados.”¹⁵³ De acordo com a lição de José Afonso da Silva, direitos fundamentais se referem àquelas “[...] prerrogativas e instituições que

¹⁴⁹ MACASKILL, Ewen; DANCE, Gabriel. **NSA files decoded**: What the revelations mean for you. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Acesso em: 28 jan. 2019.

¹⁵⁰ BALL, James; BORGER, Julian; GREENWALD Glenn. **Revealed**: how US and UK spy agencies defeat internet privacy and security. Nova York, 2013. Disponível em: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 28 jan. 2019.

¹⁵¹ MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. *E-book*. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y>. Acesso em 04 abr. de 2019.

¹⁵² RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito UFPR**. Curitiba, v. 53, p. 45-66, 2011. Disponível em: <https://revistas.ufpr.br/direito/article/view/30768>. Acesso em: 01 nov. 2019.

¹⁵³ SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

o direito positivo concretiza em garantias de uma convivência digna, livre e igual de todas as pessoas.”¹⁵⁴ Essas prerrogativas são vislumbradas como fundamentais porque tratam de situações jurídicas, sem as quais a pessoa humana não se desenvolve em sua vida pessoal e em sociedade.

Os direitos fundamentais podem ser classificados em dimensões (ou gerações) para retratar a sua evolução histórica. George Marmelsteins classifica em três gerações: a primeira se destaca pelos direitos civis e políticos (fundamentos da liberdade), com origem nas revoluções burguesas; a segunda geração ocorreu durante a Revolução Industrial, de modo que desenvolveu os direitos econômicos, sociais e culturais, com base na igualdade; e na última estão os direitos de solidariedade, em especial o direito ao desenvolvimento, à paz e ao meio ambiente, que se desenvolveram após a Segunda Guerra Mundial. Há a classificação de um quarta dimensão, que seria a respeito dos direitos relacionados ao próprio patrimônio genético¹⁵⁵ ou à globalização política, o que envolve o direito à democracia, informação e pluralismo¹⁵⁶. Por último, Bonavides¹⁵⁷ classifica a quinta dimensão dos direitos fundamentais, tendo como essência o direito à paz, ao passo que Pedro Lenza¹⁵⁸ enverada pela democracia participativa, de maneira a enaltecer o direito da humanidade.

Antes de destacar a eficácia horizontal dos direitos fundamentais, é importante tratar sobre a eficácia vertical. Para Carlos Leite, a eficácia vertical dos direitos fundamentais é “[...] a limitação imposta pelo ordenamento jurídico à atuação dos governantes em relação aos governados, na medida em que se reconhece que entre eles há uma relação vertical de poder, ou seja, de um lado o Estado (mais forte) e de outro lado o indivíduo (mais fraco).”¹⁵⁹ Desse modo, as questões que envolvem os direitos fundamentais entre o cidadão e o Estado, de maneira a se entender o Estado em um patamar superior em relação ao indivíduo, chama-se eficácia vertical dos direitos fundamentais.

¹⁵⁴ SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2012, p. 178.

¹⁵⁵ BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

¹⁵⁶ NOVELINO, Marcelo. **Direito Constitucional**. 2.ed. São Paulo: Método, 2008.

¹⁵⁷ BONAVIDES, Paulo. **A quinta geração de direitos fundamentais**. Revista Brasileira de Direitos Fundamentais & Justiça, v. 2, n. 3, p. 82-93, 2008. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/534>. Acesso em: 01 nov. 2019.

¹⁵⁸ LENZA, Pedro. **Direito constitucional esquematizado**. 20 ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁵⁹ LEITE, Carlos Henrique Bezerra. Eficácia horizontal dos direitos fundamentais na relação de emprego. **Revista Brasileira de Direito Constitucional**. São Paulo, n. 17, p. 33 - 45, 2011. Disponível em:

[http://www.esdc.com.br/RBDC/RBDC-17/RBDC-17-033-](http://www.esdc.com.br/RBDC/RBDC-17/RBDC-17-033-Artigo_Carlos_Henrique_Bezerra_Leite_(Eficacia_Horizontal_dos_Direitos_Fundamentais_na_relacao_de_Emprego).pdf)

[Artigo_Carlos_Henrique_Bezerra_Leite_\(Eficacia_Horizontal_dos_Direitos_Fundamentais_na_relacao_de_Emprego\).pdf](http://www.esdc.com.br/RBDC/RBDC-17/RBDC-17-033-Artigo_Carlos_Henrique_Bezerra_Leite_(Eficacia_Horizontal_dos_Direitos_Fundamentais_na_relacao_de_Emprego).pdf). Acesso em: 19 set. 2019.

A eficácia horizontal ou privada ocorre no âmbito privado, com o objetivo de evitar abusos na garantia e aplicabilidade dos direitos fundamentais de uma das partes, o que ultrapassaria os limites dos direitos constitucionais. De acordo com George Marmelstein¹⁶⁰, a primeira oportunidade em que se apurou a eficácia horizontal dos direitos fundamentais ocorreu em 1958, na Alemanha, com o caso Luth. Erich Luth (presidente do Clube de Imprensa de Hamburgo) que pretendia boicotar o filme *Unsterbliche Geliebte* (“Amada Imortal”). Foram pressionados os distribuidores e donos de cinema para não permitir a exibição e, na hipótese de ocorrer, que os cidadãos alemães não assistissem ao filme. Nessa demanda, a Corte Estadual havia decidido de modo a acolher o pedido da produtora e da distribuidora para exibição do filme. Em razão da interposição de recurso, o processo foi encaminhado às instâncias superiores, em que se decidiu pelo acolhimento do pleito de Luth, sendo acatada a tese de defesa de que estava exercendo seu direito de liberdade de expressão.¹⁶¹

George Marmelstein destaca a classificação de três matizes relacionadas a eficácia horizontal nas relações privadas: a ação estatal (*state action*), o efeito indireto e o efeito direto. Segundo o autor, a ação estatal verifica-se predominantemente nos Estados Unidos da América, sendo a negação da existência desse efeito se houver norma expressamente prevendo essa aplicabilidade, ou na hipótese do agente privado estiver exercendo uma função estatal. Por outro lado, o autor sustenta que o efeito indireto da aplicabilidade dos direitos fundamentais nas relações privadas permite uma melhor interpretação do direito infraconstitucional, o que ocorre, por exemplo, na Alemanha. A terceira possibilidade é o efeito direto, que independe de lei para sua aplicação.¹⁶²

Essa eficácia direta dos direitos fundamentais nas relações privadas, possui algumas ponderações importantes para serem discutidas. Daniel Sarmiento defende que um dos parâmetros nessa questão está associado, ao grau de desigualdade fática entre as partes da relação jurídica.¹⁶³ A parte mais fraca tende a ter uma maior probabilidade de risco, no tocante a ausência de garantia a respeito de seus direitos fundamentais. Por outro lado, Virgílio Afonso

¹⁶⁰ MARMELSTEIN, George. **Curso de direitos fundamentais**. 8. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁶¹ PINHO, Rodrigo César Rebello. **Direito constitucional: teoria geral da constituição e direitos fundamentais**. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁶² MARMELSTEIN, George. **Curso de direitos fundamentais**. 8. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁶³ SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. Rio de Janeiro: Lumen Juris, 2006, p. 329.

da Silva esclarece que aquele considerado a parte mais fraca (desigualdade material) da relação jurídica, deverá ter maior proteção dos direitos.¹⁶⁴

No Brasil, há decisões judiciais que se fundamentam na eficácia horizontal dos direitos fundamentais, de forma a permitir a resolução do litígio. Uma hipótese relacionada à isonomia, no tocante a equiparação de direitos trabalhistas, é o recurso especial nº 161.243/DF. Nessa hipótese concreta, um empregado brasileiro que trabalhava na companhia aérea francesa requereu isonomia salarial, em relação aos empregados franceses da mesma empresa. Segundo o relato, os empregados desempenhavam as mesmas funções, com a mesma carga horária, porém os franceses recebiam vantagens em relação ao brasileiro, devido ao estatuto da empresa prever vantagens somente para empregados de nacionalidade francesa. O recurso foi conhecido e provido para determinar a aplicação dos mesmos direitos dos empregados franceses ao brasileiro.¹⁶⁵

Há outro exemplo que está relacionado à aplicação do direito ao contraditório e à ampla defesa¹⁶⁶ nas relações entre particulares, e o devido processo legal¹⁶⁷. O recurso extraordinário nº 201.819/RJ trata de uma ação judicial visando anular um ato de expulsão de sócio de uma sociedade civil. No decorrer da análise do recurso, o Ministro Gilmar Mendes diverge da Ministra Relatora, fornecendo um estudo sobre a temática da eficácia horizontal dos direitos fundamentais. Foi realizada a comparação com outras situações históricas e com doutrina, de modo a embasar o seu entendimento, acolhido também pelo então Ministro Joaquim Barbosa, o que fez com que, no âmbito da segunda Turma, foi conhecido e desprovido o recurso extraordinário por votação majoritária.¹⁶⁸

A Ação Direta de Inconstitucionalidade nº 1.229/SC representa um exemplo de aplicação de direitos fundamentais em sua eficácia horizontal, que envolve a cidadania¹⁶⁹ como

¹⁶⁴ SILVA, Virgílio Afonso da. Direitos fundamentais e relações entre particulares. **Revista Direito GV**, São Paulo, v. 1, n. 1, p. 173-180, 2005. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/35274/34067>. Acesso em: 22 set. 2019.

¹⁶⁵ BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 161.243, Comagnie Nationale Air France**. Relator: Min. Carlos Velloso. 19 de dezembro de 1997. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=213655>. Acesso em: 24 set. 2019.

¹⁶⁶ “Art. 5º LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;” (BRASIL, 1988).

¹⁶⁷ “Art. 5º LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal;” (BRASIL, 1988).

¹⁶⁸ BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 201.819, União Brasileira De Compositores**. Relatora: Min. Ellen Gracie. 11 de outubro de 2005. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=388784>. Acesso em: 24 set. 2019.

¹⁶⁹ “Art 1º [...] II - a cidadania;” (BRASIL, 1988).

fundamento do Estado brasileiro, e o instrumento de gestão democrática. Essa hipótese se resume na verificação acerca da constitucionalidade da exigência contida na Constituição do Estado de Santa Catarina, sobre a participação de um representante dos empregados, por estes indicados para eleição, no conselho de administração e na diretoria das empresas públicas, sociedades de economia mista e suas subsidiárias. Essa norma, definida pela legislação estadual, não viola o modelo societário definido pela Constituição da República Federativa do Brasil.¹⁷⁰

No decorrer desse capítulo, demonstrou-se que a privacidade é um direito previsto no Texto Constitucional. Sua disposição está nos direitos e garantias fundamentais (artigo 5º, inciso X, CRFB), ainda que de forma abrangente, sendo aplicável em diferentes aspectos em que a privacidade poderá ser vislumbrada, seja na vida privada, honra e/ou imagem das pessoas. A proteção da privacidade passou a ter maior abrangência de discussão, em especial a partir do avanço da tecnologia utilizada pelas pessoas, seja pelo uso de câmeras fotográficas ou a ampliação dos meios de comunicação (por exemplo, jornais, rádios, televisão, mensagens de texto, smartphones, *internet* e nas redes sociais). Nessas duas décadas do século XXI, a privacidade é uma prerrogativa relevante de forma a se destacar no meio digital.

Nessa perspectiva, o direito à privacidade é uma importante prerrogativa a se preservar. O livre desenvolvimento da personalidade humana se faz a partir do momento que a liberdade seja preservada no decorrer da vida, seja perante o Estado ou terceiros. A proteção que envolve a privacidade da pessoa humana é disposta como uma garantia constitucional, com discussão amplamente realizada pela doutrina e nas decisões judiciais. Por outro lado, há a necessidade de se vislumbrar a evolução da humanidade e das novas tecnologias, seja no meio físico ou digital.

No próximo capítulo será abordada a utilização de dados pessoais no meio digital, de forma a apurar a possibilidade (ou não) de culminar em lesão ao direito à privacidade. O estudo se propaga na verificação da legislação brasileira como: o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Será destacada a importância da dignidade da pessoa humana no âmbito da privacidade e os dados pessoais no meio digital, e a lesão ao direito à privacidade. Por último, serão exemplificadas decisões no âmbito do Poder Judiciário brasileiro.

¹⁷⁰ BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 1.229/SC, Governador Do Estado De Santa Catarina**. Relator: Min. Carlos Velloso. 19 de dezembro de 2013. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=630051>. Acesso em: 24 set. 2019.

4 UTILIZAÇÃO DE DADOS PESSOAIS NO MEIO DIGITAL E A (IM)POSSIBILIDADE DE LESÃO AO DIREITO À PRIVACIDADE

A evolução da tecnologia permite que sejam utilizadas novas ferramentas e metodologias, de modo a permitir maior interatividade no dia a dia das pessoas e na sociedade global. Como consequência, a sociedade também sofre transformações e pode influenciar nos mais variados setores como, por exemplo, aspectos da vida social, nas relações de consumo, nas esferas jurídicas e trabalhistas.¹⁷¹ Seguindo a linha da inovação, os dados pessoais tomaram grandes proporções e permitiu o surgimento de formas de monetizar os dados pessoais, ou seja, criou-se uma economia dos dados pessoais.¹⁷² Com o crescimento destas práticas faz-se necessário conhecer os direitos do cidadão a respeito aos seus dados e sua privacidade.

Ao longo do presente trabalho foi apresentado os conceitos acerca dos dados pessoais no meio digital e o direito à privacidade. Neste capítulo serão apresentadas as legislações que normatizam as matérias relacionadas à privacidade e dados pessoais (Marco Civil da Internet e Lei Geral de Proteção de Dados Pessoais), a relação da dignidade da pessoa humana sobre os aspectos da privacidade e, também, a interseção dos dados pessoais no meio digital com a lesão ao direito à privacidade. São apresentadas, também, as decisões judiciais acerca do assunto.

4.1 LEGISLAÇÃO

A privacidade é tratada na Constituição da República Federativa do Brasil, conforme demonstrado anteriormente, nas suas limitações e áreas de atuação. Há outras leis esparsas que permitiram progressos na matéria, ou seja, adicionaram normas com os devidos critérios sobre a privacidade nos contextos, ou acrescentaram os dados pessoais como elementos a serem protegidos como, por exemplo, o Código de Defesa do Consumidor.¹⁷³

Até 2013 não havia, na legislação brasileira, regra específica para tratar sobre direitos e deveres para o uso da *internet*. Em 2014 foi sancionada a Lei nº 12.965/2014,

¹⁷¹ WEISS, Marcos. Sociedade sensoriada: a sociedade da transformação digital. **Estudos Avançados**, v. 33, n. 95, p. 203-214, 28 jun. 2019.

¹⁷² RAPOSO, João Francisco. Reflexões sobre a Economia dos Dados, a Racionalização do Real e o Consumidor Datafocado. **7º Encontro de GTS de Pós-Graduação, Congresso Internacional Comunicação e Consumo (COMUNICON)**, 2018. Disponível em: http://anais-comunicon2018.espm.br/GTs/GTPOS/GT4/GT04_RAPOSO.pdf. Acesso em: 20 out. 2019.

¹⁷³ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

considerada como Marco Civil da Internet, que contextualizou essa lacuna. Em seguida, em 2018 foi sancionada a Lei nº 13.709/2018, que modificou o Marco Civil da Internet e dispõe sobre a proteção de dados pessoais. Essa última é denominada como Lei Geral de Proteção de Dados Pessoais (LGPD)¹⁷⁴. Por se tratarem de duas leis principais para a realização deste trabalho, a seguir serão descritas com mais detalhes.

4.1.1 Marco Civil da Internet

O Marco Civil da Internet surgiu em 2009, a partir da iniciativa de diversas discussões, sobre a necessidade da criação de uma lei que regulasse os direitos e deveres de usuário e provedores, no uso da *internet* no país. Em seguida surgiu o Projeto de Lei nº 2.126/2011¹⁷⁵, com projeção robusta após a divulgação do famoso escândalo de violação de privacidade pelo Edward Snowden, em 2013. Foi aprovado pelo Congresso Nacional, depois pelo Senado e por fim, sancionado pela então presidente Dilma Rousseff em 2014.¹⁷⁶

O objetivo do Marco Civil da Internet (Lei nº 12.965/2014)¹⁷⁷ é regular as relações virtuais, o uso da *internet* no Brasil e a forma de atuação das entidades da União, Estados, Distrito Federal e Municípios, conforme descrito no artigo 1º da respectiva lei.¹⁷⁸ Em 2016 foi publicado o Decreto nº 8.771/2016¹⁷⁹, cujo objetivo foi regulamentar as hipóteses de exceções à neutralidade da rede, inibir condutas unilaterais ou acordos que possam comprometer os

¹⁷⁴ BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

¹⁷⁵ BRASIL. **Projeto de lei nº 2.126, de 2011**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Câmara dos Deputados, 2011. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 20 out. 2019.

¹⁷⁶ SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016. *E-book*. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em: 20 de out. 2019.

¹⁷⁷ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 abr. 2019.

¹⁷⁸ “Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.” (BRASIL, 2014).

¹⁷⁹ BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 15 abr. 2019.

princípios e os objetivos do uso da *internet* no Brasil, de forma a permitir que as autoridades administrativas solicitem dados cadastrais dos usuários aos provedores. Esse tipo de solicitação deverá ser motivada, fundamentada, registrada e informada publicamente todo e qualquer pedido realizado aos provedores (art. 11 do Decreto nº 8.771/2016)¹⁸⁰.¹⁸¹

Sobre os dados pessoais, o referido Decreto normatiza que os provedores deverão reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, e excluir assim que atingir a finalidade da qual foi definida ou no encerramento do prazo legal de sua guarda (art. 13, § 2º do Decreto nº 8.771/2016)¹⁸².

A Lei nº 12.965/2014, no artigo 3º, lista alguns princípios que disciplina o uso da *internet* no Brasil. Essa lista, que não é taxativa, destaca-se três principais: “garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; e proteção dos dados pessoais, na forma da lei.”¹⁸³ A garantia de liberdade de expressão, comunicação e manifestação de pensamento é a reafirmação de que os direitos fundamentais se mantêm, independentemente do ambiente (virtual ou real), devendo seguir as prerrogativas constituintes¹⁸⁴. A privacidade no Marco Civil da Internet está diretamente associada à proteção dos dados pessoais, armazenados e transitados pela *internet* e daqueles que controlam os dados.¹⁸⁵ A definição de dado pessoal surgiu somente no Decreto nº 8.771/2016, ou seja, durante dois anos de vigência desta lei, o conceito ficou sem uma delimitação mais precisa.¹⁸⁶

¹⁸⁰ “Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.” (BRASIL, 2016).

¹⁸¹ LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁸² “Art. 13 [...] § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos.” (BRASIL, 2016).

¹⁸³ BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 15 ago. 2018.

¹⁸⁴ SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016. *E-book*. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em: 20 de out. 2019.

¹⁸⁵ OLIVEIRA, Mike Henrique Jacinto de. Marco regulatório da internet brasileira: a proteção ao direito à privacidade com elemento fundamental nas relações de comércio eletrônico. **Iuris in mente: revista de direito fundamentais e políticas públicas**. Itumbiara, ano II, n. 2, p. 40-61, 2017. Disponível em: <http://www.periodicos.ulbra.br/index.php/iuris/article/view/2735>. Acesso em: 20 out. 2019.

¹⁸⁶ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

No rol de direitos e garantias dos usuários, está disposto no artigo 7º do Marco Civil da Internet, os elementos inéditos que fazem relação direta com o meio digital, comunicações pela *internet* e dados pessoais. Há uma proteção quanto à inviolabilidade da intimidade e da vida privada (inciso I) e, ainda, a previsão de indenização pelo dano material ou moral decorrente de sua violação. Há garantia de que os dados pessoais não poderão ser compartilhados a terceiros, incluindo os dados relativos à conexão de *internet* e acesso às aplicações, salvo consentimento do titular. O consentimento deve ser livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, inciso VII). Adicionalmente, no inciso VIII há previsão no sentido de que o usuário deve ter informações claras e completas a respeito da coleta de seus dados, a finalidade do uso, formas de armazenamento e tratamento, com segurança, com a devida justificativa e de acordo com o que foi acordado entre as partes.¹⁸⁷

O inciso X do artigo 7º regula o direito de exclusão definitiva dos dados pessoais, que o indivíduo forneceu a qualquer aplicação na *internet*. Dessa forma, com exceção das hipóteses de guarda obrigatória de dados e registros previstos em lei, o usuário poderá solicitar que seus dados sejam excluídos de forma definitiva, conforme regulado em lei.

Na seção II da lei, que diz respeito a proteção aos registros, aos dados pessoais e às comunicações privadas, deve haver a preservação da privacidade do usuário em todas as etapas de acesso a um serviço na *internet*, desde a conexão, o acesso a aplicações de *internet* que trata a lei, do registro para obter esse acesso ao serviço, e dos registros gerados no provedor de *internet* durante todo o uso.¹⁸⁸ O art. 12 define que haverá sanção caso haja infrações às normas previstas nessa seção (sem prejuízo das demais sanções cíveis, criminais ou administrativas):

- [...] I - advertência, com indicação de prazo para adoção de medidas corretivas;
 - II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
 - III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
 - IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
- Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o *caput* sua filial, sucursal, escritório ou estabelecimento situado no País.¹⁸⁹

¹⁸⁷ JESUS, Damásio de. MILAGRE, José Antônio. **Marco Civil da Internet**: comentários à Lei n. 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁸⁸ LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁸⁹ BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 15 ago. 2018.

Apesar do art. 12 da Lei nº 12.965/2014 versar sobre as sanções previstas, o parágrafo 4º do art. 11 prevê que o procedimento da apuração de infrações será regulado por decreto. O texto permite que se estabeleçam, para um momento futuro, as definições de como será aplicada a infração em cada situação concreta, de acordo com as possibilidades contempladas em lei e os procedimentos de fiscalização dos órgãos competentes.¹⁹⁰ Em 2016, o Decreto nº 8.771/2016 normatizou, dentre outras hipóteses, a respeito da fiscalização no artigo 20:

Os órgãos e as entidades da administração pública federal com competências específicas quanto aos assuntos relacionados a este Decreto atuarão de forma colaborativa, consideradas as diretrizes do CGIbr, e deverão zelar pelo cumprimento da legislação brasileira, inclusive quanto à aplicação das sanções cabíveis, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, nos termos do art. 11 da Lei nº 12.965, de 2014.¹⁹¹

O fato é que regulou, com maiores detalhes, as responsabilidades e atribuições dos órgãos competentes: Conselho Administrativo de Defesa Econômica (CADE), no artigo 17; a Secretaria Nacional de Defesa do Consumidor (SENACON), no artigo 18; e a Agência Nacional de Telecomunicações (ANATEL), no artigo 19. O referido decreto mantém a generalidade da fiscalização e a aplicação das sanções, para que os órgãos competentes façam de forma colaborativa, com o zelo de manter o equilíbrio e o cumprimento da legislação brasileira.¹⁹²

O Marco Civil da Internet foi pioneiro na regulamentação do uso da *internet* no Brasil, além de que, até 2018, foi “a primeira lei infraconstitucional que regulamenta o tema e bem esclarece ser cabível indenização por dano moral ou material decorrente de violações à intimidade e vida privada no âmbito da internet.”¹⁹³ Em conformidade com as legislações que

¹⁹⁰ REDONDO, Bruno Garcia. Infrações e Sanções cíveis, penais e administrativas. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 727-736. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁹¹ BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 15 abr. 2019.

¹⁹² SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação**. Juiz de Fora: Editar Editora Associada Ltda, 2016. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em: 20 de out. 2019.

¹⁹³ JESUS, Damásio de. MILAGRE, José Antônio. **Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014**. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

tratam de proteção de dados pessoais e privacidade, em 2018 foi sancionada a lei específica que regulamenta o assunto. No próximo tópico será disposto a respeito da Lei Geral de Proteção de Dados Pessoais.

4.1.2 Lei Geral de Proteção de Dados Pessoais

A Lei nº 13.709/2018¹⁹⁴, intitulada como Lei Geral de Proteção de Dados Pessoais (LGPD), foi sancionada pelo então presidente Michel Temer no dia 14 de agosto de 2018, com o prazo para entrar em vigência de dezoito meses. A LGPD foi inspirada no Regulamento Geral de Proteção de Dados Pessoais da União Europeia, sendo considerada como um marco legal brasileiro que traz um grande impacto, de como deverão ser tratados os dados pessoais em todos os setores, sejam públicos ou privados, empresas de pequeno ou grande porte e, ainda, independentemente se os dados pessoais são tratados no meio físico (fichamentos, papel) ou no meio virtual (planilhas no computador, sistemas e aplicativos de gestão, banco de dados).¹⁹⁵

Desde que a LGPD foi sancionada até o momento da apresentação desta monografia, diversas modificações foram realizadas. Para facilitar o entendimento da importância desta lei, vale destacar alguns acontecimentos históricos a seu respeito. O processo de discussão e criação da lei surgiu em 2012, com a proposta de Projeto de Lei nº 4.060/2012¹⁹⁶, cujo principal objetivo era dispor sobre a proteção dos dados pessoais. De 2016 a 2018, diversos outros projetos de leis foram propostos e discutidos sobre essa mesma temática.¹⁹⁷ Em maio de 2018, o Projeto Lei 4.060/2012 foi anunciado para apreciação e aprovação do Senado federal, o que originou no Projeto de Lei da Câmara (PLC) 53/2018¹⁹⁸. Em julho de 2018, o Senado

¹⁹⁴ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

¹⁹⁵ PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

¹⁹⁶ BRASIL. **Projeto de lei nº 4.060**, de 2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília, DF: Câmara dos Deputados, 2012. Disponível em: <https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 20 out. 2019.

¹⁹⁷ CUNHA, Juliana Falci Sousa Rocha. Direito à proteção de dados pessoais: a recente evolução legislativa brasileira. **Revista de Propriedade Intelectual - Direito Contemporâneo e Constituição**. Aracaju, ano 8, v. 13, n. 2, p. 115-145, 2019. Disponível em: <http://pidcc.com.br/br/component/content/article/2-uncategorised/347-direito-a-protecao-de-dados-pessoais-a-recente-evolucao-legislativa-brasileira>. Acesso em: 10 out. 2019.

¹⁹⁸ BRASIL. **Projeto de lei da câmara nº 53, de 2018 (nº 4.060/2012, na Câmara dos Deputados)**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Senado Federal. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 20 out. 2019.

Federal aprovou o PLC 53/2018 e em 14 de agosto de 2018 foi sancionada a Lei nº 13.709/2018 com alguns vetos pelo então Presidente da República Michel Temer.

No decorrer de 2018, ainda foram editados dois dispositivos para complementar a recém lei de proteção de dados. Em 26 de dezembro houve aprovação do Decreto nº 9.637/2018¹⁹⁹, que institui a Política Nacional de Segurança da Informação (PNSI). Em 27 de dezembro de 2018 foi editada a medida provisória nº 869/2018²⁰⁰, que autorizou a criação da Autoridade Nacional de Proteção de Dados (ANPD), aumentou o prazo de entrada em vigor para 24 meses após publicação e, ademais, alterou a obrigatoriedade de revisão humana das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

A medida provisória nº 869/2018 teve, em fevereiro de 2019, a apresentação de 176 propostas de emendas²⁰¹. Em abril de 2019 foi sancionada a Lei Complementar nº 166/2019²⁰² que dispõe sobre os cadastros positivos de crédito e o tratamento de dados pessoais dos cadastrados. Em 02 de junho de 2019 o Senado Federal aprovou a Proposta de Emenda à Constituição (PEC) 17/2019²⁰³, que assegura o direito à proteção de dados pessoais, por incluir entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Em 08 de julho de 2019, o Presidente da República Jair Bolsonaro sancionou a Lei nº 13.853/2019, oriunda da conversão, em lei da medida provisória nº 869/2018, de maneira a confirmar a criação da ANPD e o prazo de 24 meses para LGPD entrar em vigor.

¹⁹⁹ BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 20 out. 2019.

²⁰⁰ BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 20 out. 2019.

²⁰¹ BRASIL. **Congresso Nacional. Medida Provisória nº 869, de 2018 (Proteção de dados pessoais)**. Brasília, DF: Congresso Nacional, 2019. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>. Acesso em: 20 de out. 2019.

²⁰² BRASIL. **Lei complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.htm. Acesso em: 10 jul. 2019.

²⁰³ BRASIL. **Proposta de emenda à constituição nº 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 20 out. 2019.

Em 24 de julho de 2019, foi editado o Decreto nº 9.936/2019²⁰⁴, que regulamenta a Lei nº 12.414/2011 (Lei do Cadastro Positivo) no que diz a respeito da formação e consulta aos bancos de dados, bem como o seu tratamento, incluindo dados pessoais, para formação de histórico de crédito. As medidas provisórias e decretos tem relação (de alguma forma) com a LGPD, por envolver cadastros de dados pessoais, manipulação ou tratamentos. Recentemente, foi permitida a criação de um Cadastro Base do Cidadão, de acordo com o Decreto nº 10.046/2019²⁰⁵ que trata a forma que será conduzida em conjunto com a LGPD.

A LGPD, além de trazer segurança jurídica em relação a essa temática, dado que não havia normativa similar na esfera de regulação jurídica no Brasil, tem o objetivo de suprir necessidades internacionais para fins comerciais e políticas. De acordo com Patrícia Peck:

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 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.²⁰⁶

No âmbito das relações comerciais e políticas, a LGPD surgiu com destaque para os seguintes objetivos²⁰⁷: adequar o Brasil para relações internacionais e extraterritorial, com os países que fazem parte da União Europeia (por ter a RGPD como regulamento; regular sobre vazamento de dados pessoais que ocorre com mais intensidade desde o envolvimento da Cambridge Analytica e o Facebook²⁰⁸; a intenção do Brasil em fazer parte da Organização para

²⁰⁴ BRASIL. **Decreto nº 9.936, de 24 de julho de 2019**. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9936.htm. Acesso em: 20 out. 2019.

²⁰⁵ BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 nov. 2019.

²⁰⁶ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

²⁰⁷ CUNHA, Juliana Falci Sousa Rocha. Direito à proteção de dados pessoais: a recente evolução legislativa brasileira. **Revista de Propriedade Intelectual - Direito Contemporâneo e Constituição**. Aracaju, ano 8, v. 13, n. 2, p. 115-145, 2019. Disponível em: <http://pidcc.com.br/br/component/content/article/2-uncategorised/347-direito-a-protecao-de-dados-pessoais-a-recente-evolucao-legislativa-brasileira>. Acesso em: 10 out. 2019.

²⁰⁸ MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Facebook como o novo big brother: uma abertura para a responsabilização civil por violação à autodeterminação informativa. **Quaestio Iuris**, v. 10, n. 4, p. 2319 -

a Cooperação e Desenvolvimento Econômico, em que se exige que os países membros possuam uma legislação de proteção de dados em consonância com a visão da entidade.

A LGPD define alguns conceitos e princípios que já foram tratados no capítulo 2 deste trabalho. Entretanto, vale destacar o papel dos agentes de tratamento dos dados pessoais: operador, controlador e o encarregado. O operador é a pessoa (natural ou jurídica) que possui contato com qualquer dado pessoal durante o tratamento. O controlador é aquele que toma as decisões referentes ao tratamento, ou seja, o responsável pela empresa, setor, órgão. Para a necessidade de comunicação entre o controlador, os titulares dos dados e a ANPD, haverá uma pessoa designada um encarregado para realizar esse vínculo de comunicação.²⁰⁹

A ANPD, de acordo com o art. 55-A da LGPD, é um “[...] órgão da administração pública federal, integrante da Presidência da República”²¹⁰, com autonomia técnica e decisória, sendo que possui com competência para elaborar diretrizes para uma política nacional de proteção de dados pessoais e da privacidade, fiscalizar e aplicar sanções definidos em lei, editar regulamentos e procedimentos, além das demais responsabilidades contidas no art. 55-J.

Em relação as regras que a lei traz sobre as características e obrigações para o tratamento de dados pessoais, para uma empresa realizar a coleta e tratamento de dados de seus usuários e funcionários, deverá obter e comprovar uma (ou mais) das seguintes hipóteses (art. 7º): consentimento pelo titular; cumprimento de obrigação legal ou regulatória; execução de políticas públicas pela administração pública; estudos por órgão de pesquisa; execução de documentos contratuais ou diligências pré-contratuais; exercício regulares de direitos; proteção da vida ou bem-estar físico do titular; tutela da saúde; legítimo interesse do controlador; ou proteção do crédito.²¹¹

Apesar das normativas dispostas na LGPD, ainda há a necessidade de aguardar até que os integrantes da ANPD sejam definidos, e a agência possa realizar suas funções de regular e orientar. Diversos estudos são realizados com base no Regulamento Geral de Proteção de

2338, 2017. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/22579/21888>. Acesso em: 30 mar. 2019.

²⁰⁹ MALDONADO, Viviane Nóbrega; BLUM, Renato M. S. Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, 2019.

²¹⁰ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

²¹¹ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

Dados Pessoais da União Europeia, pois se acredita que alguns esclarecimentos poderão ser análogos aos que estão na lei europeia.²¹² A LGPD entrará em vigor em agosto de 2020.

A seguir será tratado a respeito da dignidade da pessoa humana.

4.2 DIGNIDADE DA PESSOA HUMANA

O princípio da dignidade humana foi positivado nos ordenamentos jurídicos a partir do século XX, por meio da Constituição de Weimar de 1919, na Alemanha, da Constituição Portuguesa de 1933 e da Constituição da Irlanda, de 1937.²¹³ De acordo com Bonavides, a Constituição da República Federativa do Brasil foi umas das recentes Constituições em que formulou o preceito de aplicabilidade imediata dos direitos fundamentais, incluindo o princípio da dignidade humana no art. 1º, inciso III^{214, 215}

Mesmo sendo um dos fundamentos basilares do Estado Democrático de Direito, destaca-se que não há um conceito definido do princípio da dignidade humana. Para Ingo Wolfgang Sarlet, o princípio da dignidade humana é:

[...] a qualidade intrínseca e distintiva reconhecida em cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo ato e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos, mediante o devido respeito aos demais seres que integram a rede da vida.²¹⁶

²¹² CÉSAR, Ana Carolina Moreira; ASPIS, Fábio Lara; CHAVES, Luis Fernando Prado. **1 ano da GDPR: o que podemos aprender com os erros e acertos da Europa.** São Paulo, 2019. Disponível em: <https://www.conjur.com.br/2019-mai-31/opiniao-podemos-aprender-europa-ano-gdpr>. Acesso em: 05 nov. 2019.

²¹³ RIBEIRO, Bárbara M. D. Mendes. **Uma análise dos aspectos gerais do princípio da dignidade humana.** 2018. Disponível em: <https://jus.com.br/artigos/67466/uma-analise-dos-aspectos-gerais-do-principio-da-dignidade-da-pessoa-humana>. Acesso em: 11 nov. 2019

²¹⁴ “Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...] III - a dignidade da pessoa humana;” (BRASIL, 1988).

²¹⁵ LENZA, Pedro. **Direito constitucional esquematizado.** 20 ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

²¹⁶ SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988.** 8 ed. Porto Alegre: Livraria do Advogado Editora, 2010.

Nesse sentido, a dignidade da pessoa humana fundamenta as garantias que concerne aos direitos da personalidade, assim como o direito à liberdade de expressão, à informação, inviabilidade da vida privada e da intimidade.²¹⁷

Alexandre de Moraes explana que a dignidade:

[...] é um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que, somente excepcionalmente, possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos e a busca ao Direito à Felicidade.²¹⁸

A proteção de dados é vislumbrada em alguns ordenamentos jurídicos como instrumento essencial para a proteção da dignidade da pessoa humana, sendo considerada um direito humano. Os direitos humanos, por exemplo, a liberdade, a privacidade e, especialmente, a igualdade, podem ser colocados em risco pelas tecnologias da informação e comunicação, que permitem a coleta, armazenamento, processamento, análise e transmissão de uma expressiva quantidade de dados (pessoais ou não).²¹⁹

De forma a garantir o exercício pleno da autonomia e personalidade de cada indivíduo, a Declaração Universal dos Direitos Humanos, no artigo XII²²⁰, expressamente aduz que ninguém estará sujeito à interferência em sua vida privada, influência direta da Declaração Universal de Direitos Humanos da ONU.²²¹

Com essas considerações, a seguir serão contextualizados os dados pessoais no meio digital e a lesão ao direito à privacidade.

²¹⁷ SPINELLI, Ana Claudia Marassi. Dos Direitos da Personalidade e o Princípio da Dignidade da Pessoa Humana. **Revista Jurídica Cesumar**, Maringá, v. 8, n. 2, 2008.

²¹⁸ MORAES, Alexandre de. **Direito constitucional**. 35. ed. São Paulo: Atlas, 2017. *E-book*. Acesso restrito via Minha Biblioteca.

²¹⁹ CUNHA, Juliana Falci Sousa Rocha. Direito à proteção de dados pessoais: a recente evolução legislativa brasileira. **Revista de Propriedade Intelectual - Direito Contemporâneo e Constituição**. Aracaju, ano 8, v. 13, n. 2, p. 115-145, 2019. Disponível em: <http://pidcc.com.br/br/component/content/article/2-uncategorised/347-direito-a-protecao-de-dados-pessoais-a-recente-evolucao-legislativa-brasileira>. Acesso em: 10 out. 2019.

²²⁰ "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques." (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).

²²¹ SILVA, Alexandre Ribeiro da. **A proteção de dados no Brasil: a tutela do direito à privacidade na sociedade de informação**. 2017. Dissertação (Mestrado em Direito) - Universidade Federal de Juiz de Fora, Juiz de Fora, 2017. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/5374>. Acesso em: 01 set. 2018.

4.3 DADOS PESSOAIS NO MEIO DIGITAL E A LESÃO AO DIREITO À PRIVACIDADE

Antes de ser sancionado o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, os litígios eram resolvidos com normas que faziam alguma referência na proteção de dados e garantia da privacidade. Algumas leis, como o Código de Defesa do Consumidor, o Código Civil e a própria Constituição da República Federativa do Brasil eram utilizadas de dispositivo legal para realizar a fundamentação dessa matéria.²²²

O Código de Defesa do Consumidor inovou, ao tratar sobre a privacidade e a proteção de dados pessoais de forma moderna. Na relação de consumo ocorre, na maioria das vezes, a inclusão de dados pessoais do cliente no banco de dados do fornecedor. Esta lei regulou (mesmo que de forma simples) como os dados devem ser tratados, quais regras sobre o compartilhamento e privacidade a dos dados pessoais dos clientes. Na seção VI do Código de Defesa do Consumidor (composto pelos artigos 43 e 44)²²³ estão as normativas para informar os direitos do consumidor, em relação aos cadastros realizados nos serviços no meio digital e os bancos de dados que serão usados para armazená-los.

No art. 43, estão as garantias do consumidor em ter acesso às informações existentes em cadastros, fichas e dados, bem como suas respectivas fontes. A partir desse dispositivo legal é possível destacar a legalidade de manter um fichamento em banco de dados com os dados dos clientes, porém deve-se seguir as regras (definidas no art. 43), conceder acesso à informação para titular dos dados, seguindo os princípios da qualidade dos dados e da transparência, ao direito de retificação e cancelamento dos dados que estão incorretos.²²⁴ O dispositivo de lei também define que os registros dos cadastros relativos aos consumidores são considerados entidades de caráter público, ou seja, não serão estritamente particulares aos fornecedores na relação do consumo.²²⁵

²²² MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

²²³ BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078.htm. Acesso em: 01 abr. 2019.

²²⁴ FALK, MATHEUS. **A necessidade de proteção aos dados pessoais no direito brasileiro**: tutela jurídica na era da modernidade líquida e da surveillance. 2017. Dissertação (Mestrado em Direito) - Universidade Federal do Paraná, Curitiba, 2017. Disponível em: <https://acervodigital.ufpr.br/handle/1884/47787>. Acesso em: 02 nov. 2019.

²²⁵ BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. Disponível em:

Além da Constituição da República Federativa do Brasil, a preservação da vida privada também é regulada no Código Civil, no artigo 21²²⁶. Nesse dispositivo legal, garante-se o resguardo na preservação da vida privada, sendo inviolável, de modo que se permite que o juiz, a requerimento do interessado, possa adotar atitudes necessárias para evitar ou interromper a violação dessa proteção.²²⁷

O *habeas data* seria outro recurso para tratar de demandas sobre privacidade e dados pessoais. De acordo com Jéffson, o *habeas data* possui algumas particularidades que, para o colendo Supremo Tribunal Federal: não é reconhecido como mecanismo de efetivação do direito à proteção de dados pessoais, porém pode ser usado enquanto remédio constitucional que tutela os dados pessoais, para a proteção destes porque incluídos no conceito de privacidade, para ter direito aos registros (incluem-se os direitos de retificação e complementação dos registros).²²⁸

Há normas que regulam a prevalência do bem da coletividade a favor do bem individual, e a privacidade pode ser desconsiderada por não ter a garantia do direito. A Lei Complementar nº 105 de 2001²²⁹, denominada de Lei do Sigilo das Operações Bancárias, normatiza quando e como devem ser o acesso direto aos dados do contribuinte que constem do acervo de informações de intuições financeiras. Esta lei permite a quebra do sigilo de dados sigilosos e seu acesso pelo poder público, sem que haja necessidade de autorização judicial para fins processuais na esfera administrativa. Os dados financeiros seriam pertinentes às relações estabelecidas entre o indivíduo e as instituições correspondentes (banco, receita federal, empregador). Essa regulamentação é baseada no sentido de definir essas modalidades de dados

<https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 10 mar. 2019.

²²⁶ “Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.” (BRASIL, 2002).

²²⁷ LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

²²⁸ SOUSA, Jéffson Menezes de; CUNHA E CRUZ, Marco Aurélio Rodrigues da; OLIVEIRA, Liziane Paixão Silva. A (in)efetividade do habeas data como garantia da proteção de dados pessoais no STF. **Revista Direitos Emergentes na Sociedade Global**, v. 4, n. 2, p. 171-189, 2016. Disponível em: <https://periodicos.ufsm.br/REDESG/article/view/19429>. Acesso em: 30 mar. 2019.

²²⁹ BRASIL. **Lei complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm. Acesso em: 13 mar. 2019.

como não pertencentes ao âmbito da intimidade, e sim ao âmbito da privacidade de uma relação específica, com os devidos regramentos de sigilo e segurança²³⁰.

O Cadastro Base do Cidadão, instituído pelo Decreto nº 10.046/2019²³¹, compõe uma base central, integradora, de dados pessoais de todos os brasileiros. Esse dado será constituído por dados biográficos (nome, data de nascimento, sexo, filiação, endereço e vínculos empregatícios), CPF, CNPJ (quando houver), dados cadastrais perante os órgãos públicos (número de identificação social, inscrição no programa de integração social, inscrição no programa de formação do patrimônio do servidor público, título de eleitor), atributos genéticos e dados biométricos (mapeamento facial, da palma da mão, digitais, retina ou íris dos olhos, voz e maneira de andar). Este decreto pode contrariar os requisitos alusivos à privacidade, e deve ser verificado em conjunto com a LGPD.²³²

O Decreto nº 9.936/2019²³³, que regulamenta o novo cadastro positivo, foi inicialmente criado pela Lei nº 12.414/2011²³⁴. A Lei Complementar nº 166/2019²³⁵ alterou o Decreto nº 9.936/2019. O novo cadastro positivo permite o tratamento do histórico de crédito e contas de consumo, sendo que o cidadão está automaticamente cadastrado no banco de dados e se ele quiser que seus dados deixem de ser coletados, então deverá realizar a solicitação aos órgãos e empresas de análises de créditos.

²³⁰ AVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. *Rev. Investig. Const., Curitiba*, v. 4, n. 3, p. 167-200, 2017. Disponível em: <http://dx.doi.org/10.5380/rinc.v4i3.51295>. Acesso em: 10 out. 2019.

²³¹ BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 nov. 2019.

²³² SOPRANA, Paula. Governo interliga bases e permite cruzamento de dados biométricos. **Folha de S. Paulo**. São Paulo, 10 out. 2019. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/10/governo-cria-base-de-dados-unificada-de-todos-os-brasileiros.shtml>. Acesso em: 01 nov. 2019.

²³³ BRASIL. **Decreto nº 9.936, de 24 de julho de 2019**. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9936.htm. Acesso em: 20 out. 2019.

²³⁴ BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 01 abr. 2019.

²³⁵ BRASIL. **Lei complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.htm. Acesso em: 10 jul. 2019.

A LGPD prevê a aplicação de algumas sanções administrativas na ocorrência de infração às normas previstas nesta lei, ou seja, na hipótese de vazamento de dados pessoais ou o tratamento que não esteja de acordo com o definido em lei, uma sanção poderá ser aplicada. Dentro da lista taxativa no art. 52 desta lei²³⁶, pode ser aplicado desde uma advertência com uma indicação de quando será corrigida a infração, multa de 2% até 50 milhões de reais por infração, multa diária, publicização da infração ou bloqueio dos dados pessoais ou, ainda, eliminação dos dados pessoais a que se refere a infração. A ANPD será a responsável por regular, entre outros itens, as sanções administrativas a infrações a LGPD.

Oportuno destacar, outrossim, que o monitoramento facial está sendo amplamente utilizando em diversos países. No Brasil, iniciou-se no ano de 2019 o uso de tecnologia de reconhecimento facial pelos setores públicos, nas cidades do Rio de Janeiro, Salvador, com o objetivo de auxiliar na segurança pública.²³⁷ Apesar dos benefícios dessa tecnologia, há ocorrências de que o reconhecimento facial realizado pelo sistema poderá falhar e identificar uma pessoa erroneamente.²³⁸ No Brasil, por exemplo, houve casos de falha nesse sistema.²³⁹ Devido aos problemas gerados pela tecnologia de reconhecimento facial²⁴⁰ (falsos positivos²⁴¹ e os potenciais vieses discriminatórios), a cidade de São Francisco, nos Estados Unidos, proibiu o uso dessa tecnologia para evitar erros desnecessários.²⁴²

Nos últimos cinco anos, foram publicizadas situações em que há compartilhamento de dados pessoais de forma ilegal ou vazamento de dados. Há hipótese de que as operadoras de

²³⁶ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 abr. 2019.

²³⁷ SANTOS, Alexandre. Câmeras de reconhecimento facial acham criminoso no Carnaval de Salvador. **UOL**, Salvador, 05 mar. 2019. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/03/05/cameras-de-reconhecimento-facial-acham-criminoso-no-carnaval-de-salvador.htm>. Acesso em: 08 set. 2019.

²³⁸ VARON, Joana. Bem na sua cara: a ilusão do reconhecimento facial para segurança pública. **Medium**, 04 maio 2019. Disponível em: <https://medium.com/codingrights/bem-na-sua-cara-a-ilus%C3%A3o-do-reconhecimento-facial-para-seguran%C3%A7a-p%C3%BAblica-47c708b34820>. Acesso em: 08 set. 2019.

²³⁹ G1 RIO. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **G1 Rio**, Rio de Janeiro, 11 jul. 2019. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 08 set. 2019.

²⁴⁰ SCHUPPE, Jon. **Facial recognition gives police a powerful new tracking tool: it's also raising alarms**. Washington, 2018. Disponível em: <https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936>. Acesso em: 01 out. 2019.

²⁴¹ BURGESS, Matt. **Facial recognition tech used by UK police is making a ton of mistakes**. Condé Nast, 2018. Disponível em: <https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>. Acesso em: 01 out. 2019.

²⁴² LEE, Dave. San Francisco is first US city to ban facial recognition. **BBC**, Londres, 15 maio 2019. Disponível em: <https://www.bbc.com/news/technology-48276660>. Acesso em: 01 nov. 2019.

telefonia, *internet* ou TV por assinatura, realizem compartilhamento ilegal de dados de consumidores²⁴³. A seguir, serão destacados alguns exemplos de situações concretas, em que empresas e organizações tiveram dados pessoais de seus usuários vazados.

O Instituto Nacional de Colonização e Reforma Agrária deixou exposto um conjunto de arquivos, contendo dados pessoais de famílias rurais e diversos planos de desapropriações, criações de assentamentos e concessão de créditos.²⁴⁴ No caso do Detran do Rio Grande do Norte, em torno de 70 milhões de dados pessoais de brasileiros vazaram devido a uma falha de segurança no sistema. Alguns dos dados obtidos foram: endereço residencial, telefone, operadora e dados da Carteira Nacional de Habilitação (categoria, validade, emissão, restrição e registro).²⁴⁵

A empresa Hering instalou diversos aparatos tecnológicos na loja em São Paulo, contendo sensores e câmeras faciais com o objetivo de coletar dados dos clientes enquanto estão na loja. Entre os dados coletados estão às reações faciais e ondas de calor, na medida em que o cliente andava, olhava e escolhia os produtos na loja.²⁴⁶ A controvérsia a respeito dessa situação é na falta de transparência ao consumidor sobre a divulgação desse tipo de monitoramento, bem como a existência do tratamento dos dados pessoais, os objetivos dessa coleta e os procedimentos de segurança na gestão dos dados.²⁴⁷

Em 2018 a concessionária ViaQuatro, responsável pela linha 4-Amarela do metrô de São Paulo, instalou câmeras e “portas interativas digitais” nas plataformas de embarque e desembarque. O sistema de câmeras reconhece a presença humana, e realiza a coleta de dados relacionados às emoções das pessoas junto aos anúncios publicitários.²⁴⁸ Assim, enquanto uma

²⁴³ PAYÃO, Felipe. Vivo, Net e Oi trocam dados pessoais de clientes sem autorização. **TECMUNDO**, 07 fev. 2019. Disponível em: <https://www.tecmundo.com.br/seguranca/138501-vivo-net-oi-trocam-dados-pessoais-clientes-autorizacao.htm>. Acesso em: 01 nov. 2019.

²⁴⁴ SOUZA, Ramon de. **Exclusivo**: órgão público de reforma agrária expõe 1,4 GB de documentos sensíveis. 2019. Disponível em: <https://thehack.com.br/exclusivo-incra-expoe-1-4-gb-de-documentos-sensiveis/>. Acesso em: 01 nov. 2019.

²⁴⁵ GAVIOLI, Allan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. **InfoMoney**, São Paulo, 10 out. 2019. Disponível em: <https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detrn-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/>. Acesso em: 01 nov. 2019.

²⁴⁶ MERCADO & CONSUMO. **Hering inaugura loja conceito no Shopping Morumbi, em São Paulo**. 2018. Disponível em: <https://www.mercadoeconsumo.com.br/2018/10/12/hering-inaugura-loja-conceito-no-shopping-morumbi-em-sao-paulo/>. Acesso em: 01 nov. 2019.

²⁴⁷ IDEC. **Idec notifica Hering por coleta de dados faciais para publicidade**. 2019. Disponível em: <https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-faciais-para-publicidade>. Acesso em: 01 nov. 2019.

²⁴⁸ IDEC. **Idec vai à Justiça contra coleta de emoções de usuários do metrô de SP**. 2018. Disponível em: <https://idec.org.br/noticia/idec-vai-justica-contra-coleta-de-emocoes-de-usuarios-do-metro-de-sp>. Acesso em: 01 nov. 2019.

determinada propaganda é mostrada no painel interativo, as câmeras coletam se a pessoa está feliz, satisfeita, surpresa, entre outras emoções. Todavia, que esse tipo de coleta de dados não permite que o usuário escolha não ser captado, sendo que, também, não foi informado sobre essa coleta de dados e seu real uso e tratamento.

Em 2016, ocorreu o vazamento de dados pessoais de 57 milhões de usuário do Uber, sendo que a Justiça Norte Americana decretou o pagamento de uma multa de 148 milhões de dólares, em razão do incidente. No Brasil, o Ministério Público do Distrito Federal e Territórios está pleiteando esclarecimentos do Uber sobre os impactos de vazamentos de dados pessoais, de brasileiros que usavam a plataforma.²⁴⁹ O fato ainda está em curso de investigação.

O Ministério Público do Distrito Federal e Territórios firmou um acordo com a empresa Netshoes, em virtude do vazamento de dados ocorrido em 2018, que atingiu 2 milhões de clientes. O valor da indenização foi de 500 mil reais que serão depositados no Fundo de Defesa de Direitos Difusos.²⁵⁰ Além da multa, o MPDFT exigiu que a Netshoes implantasse medidas adicionais para a proteção dos dados pessoais, além de medidas educativas junto aos seus consumidores, para conscientizar sobre a segurança da informação, os riscos e as medidas protetivas. Os dados vazados foram nomes, CPF, *e-mail*, data de nascimento e histórico de compras.

Como pode ser apurado, uma série de situações em que ocorreram vazamento de dados pessoais, compartilhamento ou tratamento inadequado sem o consentimento do titular, são objetos de investigação e de ações das autoridades competentes, com o objetivo de garantir um equilíbrio e controle da segurança das informações e os direitos dos usuários e clientes. No capítulo a seguir, serão apresentadas decisões judiciais a respeito do tema.

²⁴⁹ BRASIL. Ministério Público do Distrito Federal e Territórios. **MPDFT cobra esclarecimentos da Uber sobre impacto de vazamentos de dados pessoais para usuários brasileiros**. Brasília, DF: Ministério Público do Distrito Federal e Territórios, 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9781-mpdft-cobra-esclarecimentos-da-uber-sobre-impacto-de-vazamentos-de-dados-pessoais-para-usuarios-brasileiros>. Acesso em: 01 out. 2019.

²⁵⁰ BRASIL. **MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. Brasília, DF: Ministério Público do Distrito Federal e Territórios, 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>. Acesso em: 01 out. 2019.

4.4 DECISÕES JUDICIAIS A RESPEITO DO TEMA

No decorrer deste tópico serão apresentadas situações que ocorreram no Brasil, cuja matéria esteja relacionada com práticas consideradas abusiva e ilegal de tratamento de dados pessoais, ou seja, o compartilhamento de dados pessoais sem consentimento ou até venda destes.

4.4.1 Recurso especial nº 1348532 / SP (2012/0210805-4)

Após pesquisa diretamente realizada na ferramenta no endereço eletrônico do STJ, no dia 10 de novembro de 2019, no setor de pesquisa de jurisprudência, foram utilizados os seguintes termos: "compartilhamento de dados pessoais". Como resultado da pesquisa, foram encontrados 1(um) acórdão, 7(sete) decisões monocrática e um "Informativo de Jurisprudência". Foi escolhido o recurso especial nº 1348532/SP (2012/0210805-4), porque mais adequado ao objeto de estudo, no qual foi relator o Ministro Luis Felipe Salomão, pela Quarta Turma do STJ, votaram em 10 de outubro de 2017, os Ministros Maria Isabel Gallotti, Antonio Carlos Ferreira (Presidente), Marco Buzzi e Lázaro Guimarães (Desembargador convocado do TRF 5ª Região), em decisão emendada:

RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. 1. É facultado ao Juízo proferir sua decisão, desde que não haja necessidade de produzir provas em audiência, assim como, nos termos do que preceitua o princípio da livre persuasão racional, avaliar as provas requeridas e rejeitar aquelas que protelariam o andamento do processo, em desrespeito ao princípio da celeridade. 2. A Anadec - Associação Nacional de Defesa do Consumidor, da Vida e dos Direitos Civis tem legitimidade para, em ação civil pública, pleitear o reconhecimento de abusividade de cláusulas inseridas em contrato de cartão de crédito. Precedentes. 3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento. 4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança. 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição. 7. Considera-se abusiva a

cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão. 8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44). 9. A orientação fixada pela jurisprudência da Corte Especial do STJ, em recurso repetitivo, no que se refere à abrangência da sentença prolatada em ação civil pública, é que "os efeitos e a eficácia da sentença não estão circunscritos a lindes geográficos, mas aos limites objetivos e subjetivos do que foi decidido, levando-se em conta, para tanto, sempre a extensão do dano e a qualidade dos interesses metaindividuais postos em juízo (arts. 468, 472 e 474, CPC e 93 e 103, CDC)" (REsp 1.243.887/PR, Rel. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, DJe de 12/12/2011). 10. É pacífico o entendimento no sentido de que a revisão da multa fixada, para o caso de descumprimento de ordem judicial, só será possível, nesta instância excepcional, quando se mostrar irrisória ou exorbitante, o que, a meu ver, se verifica na hipótese, haja vista tratar-se de multa diária no valor de R\$10.000,00 (dez mil reais). 11. Recurso especial parcialmente provido. (REsp 1348532/SP, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 10/10/2017, DJe 30/11/2017).²⁵¹

Em suma, trata-se do recurso especial interposto por HSBC Bank Brasil S.A. - Banco Múltiplo com a pretensão de reformar o acórdão proferido em Apelação Cível pelo egrégio Tribunal de Justiça do Estado de São Paulo. A Associação Nacional de Defesa da Cidadania e do Consumidor ajuizou ação civil pública em face de HSBC Bank Brasil S.A. - Banco Múltiplo, para requerer a declaração de nulidade de uma das cláusulas do contrato de prestação de serviços, sobre a utilização e administração do cartão de crédito oferecido pelo réu, alegando cláusulas abusivas à luz do Código de Defesa do Consumidor e da legislação Civil.

Assentou que a autorização (embora obrigado) para que seus dados cadastrais sejam repassados a terceiros, mostra-se nula de pleno direito por ofender o ordenamento jurídico. Já na instância Superior, o Relator destacou como argumento de defesa à proteção de dados pessoais, na forma do o art. 5º do Regulamento Geral de Proteção de Dados europeu, que consagra entre os princípios fundamentais relativos aos dados pessoais. Desse modo, o recolhimento poderá existir para fins específicos, estabelecer a minimização dos dados e em um processo transparente para o titular. Preceituou quanto ao consentimento, que deve ser dado de forma expressa, acessível, e de modo inteligível, de fácil acesso e numa linguagem compreensível. Por fim, a Turma manteve a decisão do segundo grau, porém reduzindo apenas a multa diária estabelecida.

²⁵¹ BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1348532/SP, HSBC Bank Brasil S.A. - Banco Múltiplo**. Relator: Min. Luis Felipe Salomão, 30 de novembro de 2017. DJe, Brasília, 30 outubro 2017.

Disponível em:

<https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%22COMPARTILHAMENTO+DE+DADOS+PESSO AIS%22&b=ACOR&thesaurus=JURIDICO&p=true>. Acesso em: 03 nov. 2019.

Dessa forma, verifica-se que o acordo escolhido proporcionou mais segurança jurídica no tocante ao uso indevido de dados pessoais, cuja relação jurídica deve-se respeitar os dados do titular. O consentimento do uso dos dados pessoais não deve ocorrer por cláusula abusiva e ilegal de uma prestação de serviço, que forneça disponibilidade irrestrita ao provedor do serviço sobre os dados pessoais. Consequentemente, por se tratar de um consentimento em cláusula de contrato, ocorre a impossibilidade de escolha pelo consumidor de se contratar o serviço, sem a necessidade de permitir o compartilhamento de seus dados, de acordo com a imposição unilateral do contratado.

4.4.2 Apelação cível nº 0703448-33.2017.8.07.0014 - Indenização por Dano Moral

Após consulta à jurisprudência do Tribunal de Justiça do Distrito Federal e dos Territórios, no endereço seu eletrônico, em 10 de novembro de 2019, com os termos “divulgação de dados pessoais privacidade”, encontrou-se 7(sete) acórdãos, sendo um escolhido por contemplar com mais clareza a temática abordada na presente monografia. O julgamento foi realizado em apelação cível nº 0703448-33.2017.8.07.0014 da Terceira Turma Cível do TJDF, cujo relator foi o Desembargador Alvaro Ciarlini com participação no julgamento, em 04 de setembro de 2019, Gilberto de Oliveira (Primeiro Vogal) e Fátima Rafael (Segundo Vogal), cuja ementa transcreve-se:

APELAÇÃO CÍVEL. DIREITO DO CONSUMIDOR. DIREITO PROCESSUAL CIVIL. DADOS PESSOAIS. DIVULGAÇÃO. SERVIÇO DE ARMAZENAMENTO DE DADOS. TELEFONIA CELULAR. OPERADORA. DANOS MORAIS. INTIMIDADE. PRIVACIDADE. VIOLAÇÃO. INDENIZAÇÃO. VALOR ARBITRADO. DESPROPORCIONALIDADE. REDUÇÃO. CORREÇÃO MONETÁRIA. TERMO INICIAL. ARBITRAMENTO. RECURSO PARCIALMENTE PROVIDO. 1. Na presente hipótese houve divulgação de dados pessoais (fotos e contatos) de usuário que adquiriu o serviço de armazenamento de dados ofertado por operadora de telefonia celular. 2. A divulgação de dados pessoais é suficiente para causar danos morais a quem experimenta a indevida exposição de sua intimidade. 2.1. O consumidor, ao contratar o serviço de armazenamento de dados, é induzido a criar elevada expectativa de que seus dados serão protegidos. Uma vez frustrada essa expectativa, a vítima tem sua esfera extrapatrimonial diretamente violada. 2.2. A divulgação de dados pessoais consubstancia violação ao direito à intimidade e, portanto, gera dano moral indenizável. 3. De acordo com os princípios da proporcionalidade e da razoabilidade, a indenização pelo dano moral tem a finalidade de punir e alertar o ofensor, a fim de que passe a proceder com maior cautela em situações semelhantes (efeitos sancionador e pedagógico), sem, contudo, ensejar o enriquecimento sem causa do ofendido. 3.1. Diante da aplicação do método bifásico propugnado pelo Colendo Superior Tribunal de Justiça para a quantificação do valor da indenização, o montante fixado na sentença se revela coerente e idôneo à finalidade própria da condenação por danos morais. 4. O montante de vinte mil reais fixado pelo Juízo singular para compensação dos danos morais mostra-se proporcional à gravidade da conduta consistente na divulgação de dados pessoais. 5. Nos termos do enunciado nº 362 da

Súmula do Colendo Superior Tribunal de Justiça, a correção monetária do valor da indenização referente ao dano moral começa a fluir desde a data do arbitramento. 6. Recurso de apelação conhecido e desprovido. (TJDFT, Apelação Cível n. 0703448-33.2017.8.07.0014, Brasília-DF, Rel. Des. Alvaro Ciarlini, 3ª Turma Cível, DJe, 04-09-2019).²⁵²

Trata-se de apelação cível interposta por TIM CELULAR S.A., que buscou a reformulação da sentença em primeiro grau, que julgou os pedidos formulados no processo com a condenação da sociedade anônima ré ao pagamento de indenização por danos morais, bem como estabeleceu a data da citação como termo inicial dos juros de mora. Na origem, a autora ajuizou ação com o objetivo de condenar a ré ao pagamento de indenização por danos morais. A autora relatou ter celebrado um negócio jurídico com a ré, para prestar serviços de armazenamento de dados (fotos, vídeos, músicas e arquivos ou documentos do usuário). O serviço contratado compartilhou os dados pertencentes à demandante, com outra pessoa e vice-versa.

Assim, destaca-se o reconhecimento do órgão colegiado de que a divulgação de dados pessoais é suficiente, para causar danos morais contra aquele que vê exposta sua intimidade. Uma vez que se contrata um serviço para armazenar dados, o consumidor é levado a entender que seus dados serão protegidos. Quando não ocorre dessa forma, frustra-se a expectativa e o consumidor tem sua esfera extrapatrimonial diretamente violada. Por fim, manteve o montante de vinte mil reais como dano moral fixado pelo Juízo singular, assim como não houve alteração sobre a correção monetária e os juros de mora. Ao recurso foi negado provimento.

Desse modo, finaliza-se o presente capítulo. Foram demonstradas decisões judiciais com o objetivo de exemplificar a aplicação do mérito proposto neste trabalho monográfico que, no tocante da privacidade e dados pessoais no meio digital, a segurança jurídica permite garantir ao cidadão, usuário da tecnologia, a salvaguarda dos direitos previstos no ordenamento jurídico. Assim, após a exposição dos objetivos proposto na inicial, passa-se à conclusão deste trabalho.

²⁵² BRASÍLIA. Tribunal de Justiça do Distrito Federal e dos Territórios. **Apelação Cível n. 0703448-33.2017.8.07.0014**. Relator: Des. Alvaro Ciarlini, 16 de setembro de 2017. 3ª Turma Cível, Brasília, 16 setembro 2019. Disponível em:

5 CONCLUSÃO

A transformação da sociedade é inevitável. Diversos países desenvolvem novas tecnologias, fornecendo benefícios tanto para os cidadãos quanto para o Estado. Os serviços e a economia estão inovando e renovando. Novas formas de prestação de serviços eletrônicos, como o transporte privado urbano, *delivery*, compras de produtos pela *internet*, além da possibilidade de vivenciar novas experiências surgem a todo momento. A mudança também atingiu o sistema de dados pessoais, tendo o mercado financeiro se beneficiado dessa transformação para monetizar os dados pessoais, ocasionando um grande fluxo econômico.

As novas tecnologias, como a inteligência artificial, o *big data*, o reconhecimento facial, a automação na saúde, na indústria, no transporte público, bem como no cotidiano das pessoas, nos carros autônomos, e nos aparelhos-drones, são exemplos de inovação que fazem com que os dados pessoais possuam um *status* de relevo. A partir da crescente aplicação dos dados pessoais, a demanda em protegê-los de acessos, usos e compartilhamentos indevidos, principalmente sem o devido consentimento do titular, culminou em dada importância para que o ordenamento jurídico mundial tratasse do assunto.

O Brasil agiu, no decorrer dos últimos anos, para que não fique defasado frente às grandes potências nesse sentido. O país possui duas legislações que foram contextualizadas para tratar do regulamento do uso da *internet*, e do regulamento do tratamento de dados pessoais. O Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para os usuários da *internet* buscarem garantir a segurança, a integridade dos dados pessoais, o consentimento no uso da rede e suas aplicações.

Por outro lado, a Lei Geral de Proteção de Dados Pessoais é mais específica sobre a regulamentação dos dados pessoais, contendo mais princípios e definições tanto para o setor privado quanto para o público. Estabelece poderes e direitos para a Agência Nacional de Proteção de Dados, que será responsável em fiscalizar, criar pareceres e recomendações técnicas, definir e aplicar sanções e outras atribuições. Cumpre enfatizar que, até o momento da apresentação deste trabalho, não há uma formação completa da Autoridade Nacional de Proteção, de modo que não foram instituídas as atividades estabelecidas.

Desde 1990, o Código de Defesa do Consumidor exerce uma importante tarefa em proteger o consumidor, em uma relação consumerista. Em conjunto com o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, essas normas poderão garantir aos cidadãos do país uma orientação voltada à segurança jurídica, necessária para estar em conformidade com outros países que possuem normas sobre a proteção de dados pessoais. Além

disso, para que possam, também, pleitear tratamento similares à matéria, para fins comerciais e políticas.

Desse modo, o presente trabalho monográfico obteve como objetivo geral demonstrar em que situações a utilização de dados pessoais caracteriza lesão ao direito à privacidade.

Diante do exposto, percebeu-se que a lesão do direito à privacidade caracteriza-se quando: ocorre o uso de dados pessoais cujas finalidades não tem o consentimento do titular; nas hipóteses em que os dados pessoais são compartilhados com pessoas ou entidades sem o consentimento, ou em um negócio jurídico, por exemplo, há cláusulas obrigando o consumidor a compartilhar os dados pessoais sem a devida finalidade e transparência; nas situações em que se utiliza os dados pessoais para definir perfis e utilizá-los para discriminar ou difamar (seja diretamente ou indiretamente, por ações humanas ou sistemas automatizados). Há hipóteses em que possa ocorrer vazamento de dados pessoais das entidades que as detém e controlam, que também são passíveis de lesão. Os dados pessoais podem se estender a arquivos digitais pessoais, ou seja, uma foto, vídeo, documentos por exemplo.

É importante destacar que as garantias constitucionais garantem a inviolabilidade à vida, à liberdade, à igualdade, à segurança e à propriedade. O preceito à proteção a intimidade, vida privada, a honra e a imagem das pessoas devem ser garantidas, bem como o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas de acordo com a norma constitucional. O cidadão tem o direito de conhecer de informações relativas a si que estão em bancos de dados de entidades públicas ou privadas, assim como permitir que retifiquem os dados, de modo que foi respondido o problema de pesquisa formulado.

Há normas que regularizam sistemas e procedimentos que envolvam dados pessoais, com objetivo de destacar o bem comum acima do individual. Com esse propósito, a Lei do Cadastro Positivo (12.414/2011) e suas alterações, a criação de um Cadastro Base do Cidadão (Decreto nº 10.046/2019), a Lei de Acesso à Informação (12.527/2011) e a disponibilização de dados pessoais de servidores públicos no portal da transparência podem conflitar, em algum aspecto, com os princípios regulados na Lei Geral de Proteção de Dados Pessoais ou no Marco Civil da Internet? Com base nessa indagação, trabalhos futuros nessa temática poderão ser realizados.

REFERÊNCIAS

- A INTERNET das coisas na saúde. **Setor saúde**, Rio Grande do Sul, 22 out. 2015. Disponível em: <https://setorsaude.com.br/a-internet-das-coisas-na-saude/>. Acesso em: 30 abr. 2019.
- AFFONSO, Elaine Parra. **A insciência do usuário na fase de coleta de dados: privacidade em foco**. 2018. Tese (Doutorado em Ciência da Informação) - Universidade Estadual Paulista, Marília, 2018. Disponível em: <http://hdl.handle.net/11449/154737>. Acesso em: 01 set. 2018.
- ARTESE, Gustavo. Compliance digital: proteção de dados pessoais. In: CARVALHO, André Castro *et. al.* (org.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019. p. 477-501. *E-book*. Acesso restrito via Minha Biblioteca.
- AVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Rev. Investig. Const., Curitiba**, v. 4, n. 3, p. 167-200, 2017. Disponível em: <http://dx.doi.org/10.5380/rinc.v4i3.51295>. Acesso em: 10 out. 2019.
- ÁVILA, Humberto. **Teoria dos Princípios: da Definição à Aplicação dos Princípios Jurídicos**. 4. ed. São Paulo: Malheiros Editores, 2015.
- BALL, James; BORGER, Julian; GREENWALD Glenn. **Revealed: how US and UK spy agencies defeat internet privacy and security**. Nova York, 2013. Disponível em: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 28 jan. 2019.
- BEZERRA, Maria Ruth Borges. Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. **Caderno Virtual**. Brasília, v. 2, n. 44, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3828>. Acesso em: 03 nov. 2019.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.
- BOBBIO, Norberto. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.
- BONAVIDES, Paulo. **A quinta geração de direitos fundamentais**. Revista Brasileira de Direitos Fundamentais & Justiça, v. 2, n. 3, p. 82-93, 2008. Disponível em: <http://dfj.emnuvens.com.br/dfj/article/view/534>. Acesso em: 01 nov. 2019.
- BORELLI, Alessandra; OLIVEIRA, Caio; MENDONÇA, Helena C. F. Coelho. Impactos da nova lei de proteção de dados pessoais nas instituições de ensino. **Revista Escola Particular**. São Paulo, v. 22, n. 249, p. 1-10, 2018. Disponível em: https://www.academia.edu/38279183/Impactos_da_LGPD_para_Institui%C3%A7%C3%B5es_de_ensino. Acesso em: 20 out. 2019.
- BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 mar. 2019.

BRASIL. **Congresso Nacional. Medida Provisória nº 869, de 2018 (Proteção de dados pessoais)**. Brasília, DF: Congresso Nacional, 2019. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062>. Acesso em: 20 de out. 2019.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 nov. 2019.

BRASIL. **Decreto nº 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 1992. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1992/decreto-678-6-novembro-1992-449028-publicacaooriginal-1-pe.html>. Acesso em: 22 de set. 2019.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 15 abr. 2019.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 20 out. 2019.

BRASIL. **Decreto nº 9.723, de 11 de março de 2019**. Altera o Decreto nº 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto nº 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF (...). Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9723.htm. Acesso em: 13 abr. 2019.

BRASIL. **Decreto nº 9.936, de 24 de julho de 2019**. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9936.htm. Acesso em: 20 out. 2019.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 10 ago. 2019.

BRASIL. **Instrução Normativa RFB nº 1548, de 13 de fevereiro de 2015.** Dispõe sobre o Cadastro de Pessoas Físicas (CPF). Brasília, DF: Secretário da Receita Federal do Brasil, 2018. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=61197>. Acesso em: 13 abr. 2019.

BRASIL. **Lei complementar nº 105, de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm. Acesso em: 13 mar. 2019.

BRASIL. **Lei complementar nº 166, de 8 de abril de 2019.** Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp166.htm. Acesso em: 10 jul. 2019.

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/2002/110406.htm. Acesso em: 10 ago. 2018.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 01 abr. 2019.

BRASIL. **Lei nº 12.737, DE 30 DE NOVEMBRO DE 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 08 out. 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 15 ago. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 01 abr. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de

Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 01 abr. 2019.

BRASIL. **Medida Provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 20 out. 2019.

BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 10 mar. 2019.

BRASIL. Ministério Público do Distrito Federal e Territórios. **MPDFT cobra esclarecimentos da Uber sobre impacto de vazamentos de dados pessoais para usuários brasileiros**. Brasília, DF: Ministério Público do Distrito Federal e Territórios, 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9781-mpdft-cobra-esclarecimentos-da-uber-sobre-impacto-de-vazamentos-de-dados-pessoais-para-usuarios-brasileiros>. Acesso em: 01 out. 2019.

BRASIL. **MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. Brasília, DF: Ministério Público do Distrito Federal e Territórios, 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>. Acesso em: 01 out. 2019.

BRASIL. **Projeto de lei da câmara nº 53, de 2018 (nº 4.060/2012, na Câmara dos Deputados)**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Senado Federal. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 20 out. 2019.

BRASIL. **Projeto de lei nº 2.126, de 2011**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Câmara dos Deputados, 2011. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 20 out. 2019.

BRASIL. **Projeto de lei nº 4.060, de 2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Brasília, DF: Câmara dos Deputados, 2012. Disponível em: <https://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 20 out. 2019.

BRASIL. **Proposta de emenda à constituição nº 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 20 out. 2019.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.335.153, Nelson Curi E Outros**. Relator: Ministro Luís Felipe Salomão. 28 de maio de 2013. Disponível em: <https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj-aida.pdf>. Acesso em: 05 nov. 2019.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.334.097, Globo Comunicações E Participações S/A**. Relator: Ministro Luís Felipe Salomão. 28 de maio de 2013. Disponível em: <https://www.conjur.com.br/dl/direito-esquecimento-acordao-stj.pdf>. Acesso em: 05 nov. 2019.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1348532/SP, HSBC Bank Brasil S.A. - Banco Múltiplo**. Relator: Min. Luis Felipe Salomão, 30 de novembro de 2017. DJe, Brasília, 30 outubro 2017. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%22COMPARTILHAMENTO+DE+DADOS+PESSOAIS%22&b=ACOR&thesaurus=JURIDICO&p=true>. Acesso em: 03 nov. 2019.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 1.229/SC, Governador Do Estado De Santa Catarina**. Relator: Min. Carlos Velloso. 19 de dezembro de 2013. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=630051>. Acesso em: 24 set. 2019.

BRASIL. Supremo Tribunal Federal. **Recurso Especial nº 587.970, Instituto Nacional Do Seguro Social - INSS**. Relator: Min. Marco Aurélio. 20 de abr. de 2017. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=2621386>. Acesso em: 01 nov. 2019.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 161.243, Comagnie Nationale Air France**. Relator: Min. Carlos Velloso. 19 de dezembro de 1997. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=213655>. Acesso em: 24 set. 2019.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 201.819, União Brasileira De Compositores**. Relatora: Min. Ellen Gracie. 11 de outubro de 2005. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=388784>. Acesso em: 24 set. 2019.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília, DF: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 31 ago. 2019.

BRASÍLIA. Tribunal de Justiça do Distrito Federal e dos Territórios. **Apelação Cível n. 0703448-33.2017.8.07.0014**. Relator: Des. Alvaro Ciarlini, 16 de setembro de 2017. 3ª Turma

Cível, Brasília, 16 setembro 2019. Disponível em: [BURGESS, Matt. **Facial recognition tech used by UK police is making a ton of mistakes.** Condé Nast, 2018. Disponível em: <https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>. Acesso em: 01 out. 2019.](https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=buscaLivre2&buscaPorQuery=1&baseSelecionada=BASE_ACORDAO_TODAS&filtroAcordaosPublicos=false&camposSelecionados=[ESPELHO]&argumentoDePesquisa=divulgacao%20de%20dados%20pessoais%20privacidade&numero=&tipoDeRelator=TODOS&dataFim=&indexacao=&ramoJuridico=&baseDados=[TURMAS_RECURSAIS,%20BASE_ACORDAOS_IDR,%20BASE_TEMAS,%20BASE_ACORDAOS,%20BASE_INFORMATIVOS]&tipoDeNumero=NumAcordao&tipoDeData=DataPublicacao&ementa=&filtroSegredoDeJustica=false&desembargador=&dataInicio=&legislacao=&orgaoJulgador=&numeroDaPaginaAtual=1&quantidadeDeRegistros=20&totalHits=7. Acesso em: 10 nov. 2019</p>
</div>
<div data-bbox=)

CANOTILHO, J. J. Gomes. **Direito constitucional e teoria da constituição.** 7. ed. Coimbra: Almedina, 2010.

CÉSAR, Ana Carolina Moreira; ASPIS, Fábio Lara; CHAVES, Luis Fernando Prado. **1 ano da GDPR: o que podemos aprender com os erros e acertos da Europa.** São Paulo, 2019. Disponível em: <https://www.conjur.com.br/2019-mai-31/opinio-podemos-aprender-europa-ano-gdpr>. Acesso em: 05 nov. 2019.

COLUSSI, Fernando A. M.; SANTOS, Tomlyta L. V. dos. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. **Rev. de Biodireito e Direito dos Animais.** Porto Alegre, v. 4, n. 2, p. 1–21, 2019. Disponível em: https://www.researchgate.net/publication/330979819_NOVAS_TECNOLOGIAS_E_LIBERDADE_DE_EXPRESSAO_NA_PESQUISA_CIENTIFICA_UMA_ANALISE SOBRE_A_PROTECAO_DE_DADOS_GENETICOS_E_DE_SAUDE. Acesso em: 30 mar. 2019.

COPETTI, Rafael; MIRANDA, Marcel Andreatta de. Autodeterminação Informativa e Proteção de Dados: Uma Análise Crítica da Jurisprudência Brasileira. **Revista de Direito, Governança e Novas Tecnologias.** Minas Gerais, v. 1, n. 2, p. 28-48, 2015. Disponível em: <https://www.indexlaw.org/index.php/revistadgnt/article/view/46/43>. Acesso em: 30 mar. 2019.

COPPIN, Ben. **Inteligência artificial.** Rio de Janeiro: LTC, 2017. *E-book*. Acesso restrito via Minha Biblioteca.

CRUZ, Ariele Chagas; SARMENTO, George; SEIXAS, Taysa Matos. **Direitos humanos fundamentais: estudos sobre o art. 5º da Constituição de 1988.** São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

CUNHA, Juliana Falci Sousa Rocha. Direito à proteção de dados pessoais: a recente evolução legislativa brasileira. **Revista de Propriedade Intelectual - Direito Contemporâneo e Constituição.** Aracaju, ano 8, v. 13, n. 2, p. 115-145, 2019. Disponível em: <http://pidcc.com.br/br/component/content/article/2-uncategorised/347-direito-a-protecao-de-dados-pessoais-a-recente-evolucao-legislativa-brasileira>. Acesso em: 10 out. 2019.

DE ARAUJO, Luiz Ernani Bonesso; CAVALHEIRO, Larissa Nunes. A proteção de dados pessoais na sociedade informacional brasileira: o direito fundamental a privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. **Revista Do Direito Público**, Londrina, v.9, n.1, p.209-226, jan./abr. 2014. Disponível em: <http://www.uel.br/revistas/uel/index.php/direitopub/article/view/16870/14321>. Acesso em: 30 mar. 2019.

DE LUCA, Cristina. Quem culpar quando a Inteligência Artificial falhar? **UOL**, São Paulo, 30 mar. 2019. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/03/30/quem-culpar-quando-a-inteligencia-artificial-falhar/>. Acesso em: 6 jun. 2019.

DE SORDI, José Osvaldo; MEIRELES, Manuel. **Administração de sistemas de informação**. 2. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

DONEDA, Danilo. A proteção da privacidade e de dados pessoais no brasil. **Revista Observatório Itaú Cultural**. São Paulo, n. 16, p. 136-150, 2014. Disponível em: <https://www.itaucultural.org.br/revista-observatorio-ic-n-16>. Acesso em: 04 jun. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**. Chapecó, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 maio 2019.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

FALK, MATHEUS. **A necessidade de proteção aos dados pessoais no direito brasileiro: tutela jurídica na era da modernidade líquida e da surveillance**. 2017. Dissertação (Mestrado em Direito) - Universidade Federal do Paraná, Curitiba, 2017. Disponível em: <https://acervodigital.ufpr.br/handle/1884/47787>. Acesso em: 02 nov. 2019.

FAVERA, Rafaela Bolson Dalla; SILVA, Rosane Leal da. **Cibersegurança na União Europeia e no Mercosul: Big Data e Surveillance Versus Privacidade e Proteção de Dados na Internet**. Revista de Direito, Governança e Novas Tecnologias. Curitiba, v. 2, n. 2, p. 112-134, 2016. Disponível em: <https://www.indexlaw.org/index.php/revistadgnt/article/view/1490/pdf> Acesso em: 30 mar. 2019.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista Da Faculdade De Direito**. São Paulo, v. 88, p. 439-459, 1993. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 15 jul. 2019.

FORTES, Vinícius Borges. **O direito fundamental à privacidade: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil**. 2015. Tese (Doutorado em Direito) - Universidade Estácio de Sá, Rio de Janeiro, 2015. Disponível em: <http://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf>. Acesso em: 22 set. 2019.

FREIRE, Emerson; BATISTA, Sueli Soares dos Santos. **Sociedade e tecnologia na era digital**. São Paulo: Érica, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

G1 RIO. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **G1 Rio**, Rio de Janeiro, 11 jul. 2019. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml>. Acesso em: 08 set. 2019.

GAVIOLI, Allan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. **InfoMoney**, São Paulo, 10 out. 2019. Disponível em: <https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detrans-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/>. Acesso em: 01 nov. 2019.

GEBHART, Gennie *et al.* **Who has your back? Censorship Edition** 2019. San Francisco, 2019. Disponível em: <https://www.eff.org/wp/who-has-your-back-2019>. Acesso em: 06 out. 2019. Tradução nossa.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito**. Curitiba, v. 47, n. 0, p. 141-153, 2008. Disponível em: <https://www.revistas.ufpr.br/direito/article/view/15738>. Acesso em: 03 nov. 2019.

GONÇALVES, Claudiana Freitas Botelho *et al.* Um estudo sobre a influência da IOT no agronegócio. **Revista Gestão, Inovação e Empreendedorismo**, v. 1, n. 1, 2018. Disponível em: <http://ojs.ciebe.com.br/index.php/GIE-METRO/article/view/2/4>. Acesso em: 30 abr. 2019.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores**. Porto Alegre: Bookman, 2013. *E-book*. Acesso restrito via Minha Biblioteca.

GOOGLE. **Google Maps**. 2019. Disponível em: <https://www.google.com/intl/pt-BR/maps/about/>. Acesso em: 22 set. 2019.

GOOGLE. **Nossa missão é organizar as informações do mundo para que sejam universalmente acessíveis e úteis para todos**. Califórnia, 2019. Disponível em: <https://about.google/>. Acesso em: 01 nov. 2019.

IDEC. **Idec notifica Hering por coleta de dados faciais para publicidade**. 2019. Disponível em: <https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-faciais-para-publicidade>. Acesso em: 01 nov. 2019.

IDEC. **Idec vai à Justiça contra coleta de emoções de usuários do metrô de SP**. 2018. Disponível em: <https://idec.org.br/noticia/idec-vai-justica-contracoleta-de-emocoes-de-usuarios-do-metro-de-sp>. Acesso em: 01 nov. 2019.

JESUS, Damásio de. MILAGRE, José Antônio. **Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014**. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

JONES, Rhett. Ação judicial sobre rastreamento de localização escondido do Google pode ser um divisor de águas. **Gizmodo**, São Paulo, 21 ago. 2018. Disponível em:

<https://gizmodo.uol.com.br/acao-judicial-rastreamento-localizacao-google-divisor-de-aguas/>. Acesso em: 5 abr. 2019.

LEE, Dave. San Francisco is first US city to ban facial recognition. **BBC**, Londres, 15 maio 2019. Disponível em: <https://www.bbc.com/news/technology-48276660>. Acesso em: 01 nov. 2019.

LEITE, Carlos Henrique Bezerra. Eficácia horizontal dos direitos fundamentais na relação de emprego. **Revista Brasileira de Direito Constitucional**. São Paulo, n. 17, p. 33 - 45, 2011. Disponível em: [http://www.esdc.com.br/RBDC/RBDC-17/RBDC-17-033-Artigo_Carlos_Henrique_Bezerra_Leite_\(Eficacia_Horizontal_dos_Direitos_Fundamentais_n_a_relacao_de_Emprego\).pdf](http://www.esdc.com.br/RBDC/RBDC-17/RBDC-17-033-Artigo_Carlos_Henrique_Bezerra_Leite_(Eficacia_Horizontal_dos_Direitos_Fundamentais_n_a_relacao_de_Emprego).pdf). Acesso em: 19 set. 2019.

LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

LENZA, Pedro. **Direito constitucional esquematizado**. 20 ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

LÉVY, Pierre. A revolução contemporânea em matéria de comunicação. **Revista Famecos**. Porto Alegre, v. 5, n. 9, p. 37-49, 1998. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/3009/>. Acesso em: 30 mar. 2019.

LIMA, M. I. Do Direito À Proteção De Dados Em Matéria De Saúde Na Sociedade De Informação. **Revista Arquivo Jurídico**. Teresina, v. 4, n. 1, p. 1-24, 2018. Disponível em: <http://www.ojs.ufpi.br/index.php/raj/article/view/7416/4303>. Acesso em: 30 mar. 2019.

LINKEDIN. **Contrato do Usuário**. 2018. Disponível em: <https://www.linkedin.com/legal/user-agreement>. Acesso em: 05 abr. 2019.

LINKEDIN. **Política de Privacidade**. 2018. Disponível em: <https://www.linkedin.com/legal/privacy-policy>. Acesso em: 05 abr. 2019.

MACASKILL, Ewen; DANCE, Gabriel. **NSA files decoded**: What the revelations mean for you. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>. Acesso em: 28 jan. 2019.

MACHADO, Joana de Moraes Souza. A tutela da privacidade no controle de dados pessoais no direito brasileiro. **Revista Jurídica Eletrônica da UFPI**. Teresina, v. 2, n. 02, p. 43-65, 2016. Disponível em: <http://www.ojs.ufpi.br/index.php/raj/article/viewFile/4671/2694>. Acesso em: 05 abr. 2019.

MACHADO, Jorge; BIONI, Bruno Ricardo. A proteção de dados pessoais nos programas de nota fiscal: um estudo de caso da Nota Fiscal paulista. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 351-365, 2016. Disponível em: <http://dx.doi.org/10.18617/liinc.v12i2.919>. Acesso em 04 abr. 2019.

MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano B. S. A proteção de dados e o direito de personalidade da pessoa jurídica. **Revista de Direito Empresarial - RDEmp**. Belo Horizonte, ano 15, n. 3, p. 31-47, 2018. Disponível em:

https://www.academia.edu/38017824/A_prote%C3%A7%C3%A3o_de_dados_e_o_direito_de_personalidade_da_pessoa_jur%C3%ADdica. Acesso em: 01 abr. 2019.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. *E-book*.

Disponível em:

<http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y>. Acesso em: 04 abr. 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato M. S. Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, 2019.

MARÇULA, Marcelo; BENINI FILHO, Pio Armando. **Informática: conceitos e aplicações**. 5. ed. São Paulo: Érica, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

MARMELSTEIN, George. **Curso de direitos fundamentais**. 8. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

MARTINS-COSTA, Judith. **A boa-fé no direito privado: critérios para a sua aplicação**. 2. ed. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

MELO, Ricardo Rebelo Silva. Aplicabilidade de Inteligência Artificial nos dispositivos de Defesa das Forças Armadas. **O Comunicante**. Brasília-DF, v. 8, n. 3, p. 32-39, 2018. Disponível em: <http://www.ebrevistas.eb.mil.br/index.php/OC/article/view/1795>. Acesso em: 03 maio 2019.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 14. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008. Monografia (Dissertação de Mestrado em Direito) Universidade de Brasília, Brasília, 2008. Disponível em: <http://www.repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso em: 03 maio 2019.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Facebook como o novo big brother: uma abertura para a responsabilização civil por violação à autodeterminação informativa. **Quaestio Iuris**, v. 10, n. 4, p. 2319 -2338, 2017. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/22579/21888>. Acesso em: 30 mar. 2019.

MERCADO & CONSUMO. **Hering inaugura loja conceito no Shopping Morumbi, em São Paulo**. 2018. Disponível em: <https://www.mercadoconsumo.com.br/2018/10/12/hering-inaugura-loja-conceito-no-shopping-morumbi-em-sao-paulo/>. Acesso em: 01 nov. 2019.

MONTEIRO, Washington de Barros; PINTO, Ana C. de B. M. F. **Curso de direito civil: parte geral**. v. 1, 45. ed. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

MORAES, Alexandre de. **Direito constitucional**. 35. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

MORAES, Guilherme Peña de. **Curso de Direito Constitucional**. 11. ed. São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

MOTTA, Sylvio. **Direito Constitucional: Teoria, Jurisprudência e Questões**. 28. ed. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

NADER, Paulo. **Filosofia do direito**. Rio de Janeiro: Forense, 2019. *E-book*. Acesso restrito via Minha Biblioteca

NIQUE, Walter; LADEIRA, Wagner. **Como fazer pesquisa de marketing: um guia prático para a realidade brasileira**. 2. ed. São Paulo: Atlas, 2017. *E-book*. Acesso restrito via Minha Biblioteca.

NOVELINO, Marcelo. **Direito Constitucional**. 2.ed. São Paulo: Método, 2008.

NUNES JÚNIOR, Flávio Martins Alves. **Curso de direito constitucional**. 3. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

OECD. **Declaration on transborder data flows**. Paris, 1985. Disponível em: <http://www.oecd.org/sti/ieconomy/declarationontransborderdataflows.htm>. Acesso em: 10 abr. 2019.

OECD. **The OECD privacy framework**. Paris, 2013. Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 10 abr. 2019.

OLIVEIRA, Jane Resina F. de. **Lei Carolina Dieckmann: antes tarde do que nunca**. São Paulo, 2012. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI169090,41046-Lei+Carolina+Dieckmann+antes+tarde+do+que+nunca>. Acesso em: 08 out. 2019.

OLIVEIRA, Mike Henrique Jacinto de. Marco regulatório da internet brasileira: a proteção ao direito à privacidade com elemento fundamental nas relações de comércio eletrônico. **Iuris in mente: revista de direito fundamentais e políticas públicas**. Itumbiara, ano II, n. 2, p. 40-61, 2017. Disponível em: <http://www.periodicos.ulbra.br/index.php/iuris/article/view/2735>. Acesso em: 20 out. 2019.

OLSEN, Wendy. **Coleta de dados: debates e métodos fundamentais em pesquisa social**. Porto Alegre: Penso, 2015. *E-book*. Acesso restrito via Minha Biblioteca.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos. 1948**. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 01 nov. 2019.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 7. ed. São Paulo: Atlas, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

PAYÃO, Felipe. Vivo, Net e Oi trocam dados pessoais de clientes sem autorização. **TECMUNDO**, 07 fev. 2019. Disponível em:

<https://www.tecmundo.com.br/seguranca/138501-vivo-net-oi-trocam-dados-pessoais-clientes-autorizacao.htm>. Acesso em: 01 nov. 2019.

PEZZELLA, Maria C. C.; GHISI, Silvano. A manipulação de dados pessoais nas relações de consumo e o sistema “crediscor”. **Civilistica.com**. Rio de Janeiro. v. 4, n. 1, p. 1-29, 2014. Disponível em <http://civilistica.emnuvens.com.br/redc/article/view/201>. Acesso em: 01 abr. 2019.

PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016. *E-book*. Acesso restrito via Minha Biblioteca.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

PINHO, Rodrigo César Rebello. **Direito constitucional: teoria geral da constituição e direitos fundamentais**. São Paulo: Saraiva Educação, 2018. *E-book*. Acesso restrito via Minha Biblioteca.

PORTO, Noemia Aparecida Garcia. Direito ao esquecimento: memória, vida privada e espaço público. **Revista do Tribunal Regional do Trabalho da 10ª Região**, Brasília, DF, v. 19, n. 20, p. 104-122, 2015. Disponível em: <https://hdl.handle.net/20.500.12178/85646>. Acesso em: 30 abr. 2019.

PRATES, Cristina Cantú. Privacidade e intimidade na internet: a legalidade dos cookies e spam. **Revista FMU Direito**. São Paulo, v 28, n. 42, p. 29-45, 2014. Disponível em: <http://revistaseletronicas.fmu.br/index.php/FMUD/article/view/676>. Acesso em: 10 jun. 2019.

PRIEBE, Leonardo da Costa; PETRY, Alexandre Torres. Big brother is watching you: uma análise da regulação brasileira sobre drones no tocante à violação da privacidade. **Justiça & Sociedade - Revista do Curso de Direito do Centro Universitário Metodista**. Porto Alegre, v. 3, n. 1, p. 9-44, 2018. Disponível em: <https://www.metodista.br/revistas/revistas-ipa/index.php/direito/article/download/679/617>. Acesso em: 14 set. 2019.

RANIERI, Nina. **Teoria do Estado: do Estado de Direito ao Estado Democrático de Direito**. Barueri, SP: Manole, 2019.

RAPOSO, João Francisco. Reflexões sobre a Economia dos Dados, a Racionalização do Real e o Consumidor Datafocado. **7º Encontro de GTs de Pós-Graduação, Congresso Internacional Comunicação e Consumo (COMUNICON)**, 2018. Disponível em: http://anais-comunicon2018.espm.br/GTs/GTPOS/GT4/GT04_RAPOSO.pdf. Acesso em: 20 out. 2019.

REDONDO, Bruno Garcia. Infrações e Sanções cíveis, penais e administrativas. *In*: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 727-736. *E-book*. Acesso restrito via Minha Biblioteca.

REIS, Beatriz de Felipe; GRAMINHO, Vivian Maria Caxambu. A inteligência artificial no recrutamento de trabalhadores: o caso amazon analisado sob a ótica dos direitos fundamentais. *In*: XVI SEMINÁRIO INTERNACIONAL DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, 16. 2019, Santa Catarina. **XII Mostra Internacional de trabalhos Científicos**. Santa Catarina: EDUNISC, 2019. Disponível em:

<https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/19599/1192612314>. Acesso em: 30 set. 2019.

REITMAN, Rainey *et al.* **Who has your back? Government Data Requests** 2017. San Francisco, 2017. Disponível em: <https://www.eff.org/who-has-your-back-2017>. Acesso em: 06 out. 2019.

RIBEIRO, Bárbara M. D. Mendes. **Uma análise dos aspectos gerais do princípio da dignidade humana**. 2018. Disponível em: <https://jus.com.br/artigos/67466/uma-analise-dos-aspectos-gerais-do-principio-da-dignidade-da-pessoa-humana>. Acesso em: 11 nov. 2019

ROCHA, Maria Vital da; CUNHA, Isaac Rodrigues; OLIVEIRA, Karin de Fátima Rodrigues. Esquecimento, internet e “preferência” da informação: possibilidades de aplicação da doutrina dos preferred rights da jurisprudência norte-americana ao caso brasileiro. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, n. 3, 2017, p. 483-509. Disponível em: <https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/4969/3674>. Acesso em: 30 mar. 2019.

ROSA, Renato de Oliveira; CASAGRANDA, Yasmin Gomes; SPINELLI, Fernando Elias. A importância do marketing digital utilizando a influência do comportamento do consumidor. **Revista de tecnologia aplicada**, v.6, n.2, p. 28-39, 2017. Disponível em: <http://www.cc.faccamp.br/ojs-2.4.8-2/index.php/RTA/article/view/1044/525>. Acesso em: 12 set. 2019.

ROTHENBURG, Walter Claudius. **Direitos fundamentais**. Rio de Janeiro: Forense, São Paulo: MÉTODO, 2014. *E-book*. Acesso restrito via Minha Biblioteca.

RUARO, Regina Linden. Direito fundamental à liberdade de pesquisa genética e à proteção de dados pessoais: os princípios da prevenção e da precaução como garantia do direito à vida privada. **Revista do direito público**. Londrina, v. 10, n. 2, p. 9-38, 2015. Disponível em: <http://www.uel.br/revistas/uel/index.php/direitopub/article/view/22298/16895>. Acesso em: 30 mar. 2019.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito UFPR**. Curitiba, v. 53, p. 45-66, 2011. Disponível em: <https://revistas.ufpr.br/direito/article/view/30768>. Acesso em: 01 nov. 2019.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado**. São Paulo: LTr, 2014. 192 p.

SANTA CLARA UNIVERSITY. **The Santa Clara Principles: On Transparency and Accountability in Content Moderation**. Northern California, 2019. Disponível em: <https://santaclaraprinciples.org/>. Acesso em: 05 out. 2019.

SANTOS, Alexandre. Câmeras de reconhecimento facial acham criminoso no Carnaval de Salvador. **UOL**, Salvador, 05 mar. 2019. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/03/05/cameras-de-reconhecimento-facial-acham-criminoso-no-carnaval-de-salvador.htm>. Acesso em: 08 set. 2019.

SANTOS, Alfredo Luiz dos. **Gerenciamento de identidades**: Segurança da informação. Rio de Janeiro: Brasport, 2007.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 8 ed. Porto Alegre: Livraria do Advogado Editora, 2010.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 8. ed. São Paulo: Saraiva Educação, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. Rio de Janeiro: Lumen Juris, 2006, p. 329.

SCHUPPE, Jon. **Facial recognition gives police a powerful new tracking tool**: it's also raising alarms. Washington, 2018. Disponível em: <https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936>. Acesso em: 01 out. 2019.

SILVA, Alexandre Ribeiro da. **A proteção de dados no Brasil**: a tutela do direito à privacidade na sociedade de informação. 2017. Dissertação (Mestrado em Direito) - Universidade Federal de Juiz de Fora, Juiz de Fora, 2017. Disponível em: <https://repositorio.ufjf.br/jspui/handle/ufjf/5374>. Acesso em: 01 set. 2018.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2012, p. 178.

SILVA, Norma Lúcia da. **Marketing digital como estratégia competitiva**: o uso do portal digital do Banco do Brasil S.A. 2016. Dissertação (Mestrado Profissional em Gestão Organizacional) - Universidade Federal de Goiás, Catalão, 2016. Disponível em: <https://repositorio.bc.ufg.br/tede/handle/tede/5828>. Acesso em: 22 set. 2019.

SILVA, Virgílio Afonso da. Direitos fundamentais e relações entre particulares. **Revista Direito GV**, São Paulo, v. 1, n. 1, p. 173-180, 2005. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/35274/34067>. Acesso em: 22 set. 2019.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 217-230, 2016. Disponível em: <http://revista.ibict.br/liinc/article/view/3719/3138>. Acesso em: 08 set. 2019.

SOPRANA, Paula. Governo interliga bases e permite cruzamento de dados biométricos. **Folha de S. Paulo**. São Paulo, 10 out. 2019. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/10/governo-cria-base-de-dados-unificada-de-todos-os-brasileiros.shtml>. Acesso em: 01 nov. 2019.

SOUSA, Jéffson Menezes de; CUNHA E CRUZ, Marco Aurélio Rodrigues da; OLIVEIRA, Liziane Paixão Silva. A (in)efetividade do habeas data como garantia da proteção de dados pessoais no STF. **Revista Direitos Emergentes na Sociedade Global**, v. 4, n. 2, p. 171-189, 2016. Disponível em: <https://periodicos.ufsm.br/REDESG/article/view/19429>. Acesso em: 30 mar. 2019.

SOUZA, Allan Rocha de *et al.* **Marcos legais nacionais em face da abertura de dados para pesquisa em saúde: dados pessoais, sensíveis ou sigilosos e propriedade intelectual.** Rio de Janeiro: Fiocruz, 2018. 123 p. Disponível em:

https://www.arca.fiocruz.br/bitstream/icict/28838/4/Guanaes_Paulo_Org_Marcos_Legais_Presid%3%aancia_2018.pdf. Acesso em: 14 ago. 2019.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação.** Juiz de Fora: Editar Editora Associada Ltda, 2016. *E-book*. Disponível em:

https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em: 20 de out. 2019.

SOUZA, Clayton de Almeida. Estratégia de Dados e Marketing Digital: Novas Formas de Aumentar Receitas e Diminuir Custos. **Revista IPTEC**. São Paulo, v. 6, n. 2, p. 92-107, 2018. Disponível em:

<http://www6.uninove.br/ojs/journaliji/index.php/iptec/article/view/101/190>. Acesso em: 02 maio 2019.

SOUZA, Ramon de. **Exclusivo: órgão público de reforma agrária expõe 1,4 GB de**

documentos sensíveis. 2019. Disponível em: <https://thehack.com.br/exclusivo-incra-expoe-1-4-gb-de-documentos-sensiveis/>. Acesso em: 01 nov. 2019.

SPINELLI, Ana Claudia Marassi. Dos Direitos da Personalidade e o Princípio da Dignidade da Pessoa Humana. **Revista Jurídica Cesumar**, Maringá, v. 8, n. 2, 2008.

TURCHI, Sandra R. **Estratégias de marketing digital e e-commerce.** São Paulo: Atlas, 2019. *E-book*. Acesso restrito via Minha Biblioteca.

UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*. 2016; L (119):1-88. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 01 abr. 2019.

VARON, Joana. Bem na sua cara: a ilusão do reconhecimento facial para segurança pública.

Medium, 04 maio 2019. Disponível em: <https://medium.com/codingrights/bem-na-sua-cara-a-ilus%C3%A3o-do-reconhecimento-facial-para-seguran%C3%A7a-p%C3%BAblica-47c708b34820>. Acesso em: 08 set. 2019.

VENTURA, Ivan. A relação entre a Lei de proteção de dados e o ingresso do Brasil na OCDE. **Consumidor Moderno**, São Paulo, mar. 2019. Disponível em:

<https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/>. Acesso em: 09 set. 2019.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, p. 195, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 01 abr. 2019.

WEISS, Marcos. Sociedade sensoriada: a sociedade da transformação digital. **Estudos Avançados**, v. 33, n. 95, p. 203-214, 28 jun. 2019.

ZANON, João Carlos. **Direito à proteção dos dados pessoais**. São Paulo: Revista dos Tribunais, 2013.

ZAPATER, Máira. **Direito da criança e do adolescente**. São Paulo: Saraiva Educação, 2019.