UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

ALCIVAN SANTOS DE MEDEIROS

PRIVACIDADE E PROTEÇÃO DE DADOS: REGIMES JURÍDICOS DE OBTENÇÃO DE DADOS À LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

MOSSORÓ-RN
2023

ALCIVAN SANTOS DE MEDEIROS

PRIVACIDADE E PROTEÇÃO DE DADOS: REGIMES JURÍDICOS DE OBTENÇÃO DE DADOS À LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Mestre em Direito.

Linha de Pesquisa 2: Estado, conflitos e direitos fundamentais.

Orientador: Prof. Dr. Rodrigo Vieira Costa.

MOSSORÓ-RN

2023

M488p Medeiros , Alcivan Santos de .
Privacidade e proteção de dados: regimes jurídicos de obtenção de dados à luz do ordenamento jurídico brasileiro / Alcivan Santos de Medeiros . - 2023.
115 f. : il.

Orientador: Rodrigo Vieira Costa.
Dissertação (Mestrado) - Universidade Federal Rural do Semi-árido, Programa de Pós-graduação em Direito, 2023.

1. Privacidade. 2. Proteção de dados. 3. Dados. 4. Regime jurídico. 5. Obtenção de dados. I. Costa, Rodrigo Vieira , orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automáto em conformidade com AACR2 e os dados fornecidos pelo) autor(a).
Biblioteca Campus Mossoró / Setor de Informação e Referência
Bibliotecária: Keina Cristina Santos Sousa e Silva
CRB: 15/120

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC´s) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

ALCIVAN SANTOS DE MEDEIROS

PRIVACIDADE E PROTEÇÃO DE DADOS: REGIMES JURÍDICOS DE OBTENÇÃO DE DADOS À LUZ DO ORDENAMENTO JURÍDICO BRASILEIRO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Mestre em Direito.

Linha de Pesquisa 2: Estado, conflitos e direitos fundamentais.

Defendida em: 15/02/2023.

BANCA EXAMINADORA

_____
Prof. Dr. Rodrigo Vieira Costa (UFERSA)
Presidente

_____
Prof. Dr. Ulisses Levy Silvério dos Reis (UFERSA)
Membro Examinador Interno

_____
Prof. Dr. Alexandre Henrique Tavares Saldanha (UPE/UNICAP)
Membro Examinador Externo

"Redes globais não podem ser controladas, mas pessoas usando-as podem, são e serão — a menos que as sociedades optem pela liberdade da Internet, agindo a partir das barricadas de seus libertários nostálgicos, e além dela."

(A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade)

Manuel Castells.

RESUMO

Os avanços tecnológicos trouxeram grande prosperidade para a humanidade, ao passo que também consagraram uma série de novas responsabilidades. Tal realidade não seria diferente com a Internet e o advento dos dispositivos informáticos, os quais viabilizam a interconexão em nível global e a difusão de informações em tempo recorde. Nesse sentido, nota-se o aumento da geração de dados e informações, os quais podem ser utilizados para os mais variados fins. Diante disso, surgem indagações de como viabilizar o uso desses dados sem ferir os direitos fundamentais dos titulares. Seguindo essa linha, para fins de delimitação da pesquisa, este estudo se debruça sobre os regimes jurídicos de obtenção desses dados gerados pelos indivíduos. Pode-se definir como objetivo geral de estudo: compreender os regimes jurídicos de obtenção de dados à luz da atual realidade jurídica brasileira em torno dos direitos à privacidade e à proteção de dados. Já no que se referem aos objetivos específicos, eles giram em torno dos seguintes aspectos: diferenciar os direitos à privacidade digital e à proteção de dados; analisar os dados gerados pelos usuários e como eles se vinculam ao indivíduo dentro do microssistema de proteção de dados; compreender quais são os regimes jurídicos admitidos para obtenção desses dados e a possibilidade de unificação. Já o caminho metodológico perpassa pelo método de pesquisa teórico dedutivo, com o enfoque teórico-normativo, tendo em vista que o estudo se sustenta nas ideias presentes em pesquisas formuladas anteriormente, para então construir a fundamentação específica pertinente aos assuntos abordados. Soma-se a isso o emprego da técnica de pesquisa bibliográfica, uma vez que a pesquisa se debruça sobre a leitura e análise de obras teóricas sobre a privacidade no ambiente digital e a proteção de dados na atualidade. Registre-se que a principal hipótese que a pesquisa espera testar é a de que subsistem no sistema jurídico brasileiro regimes jurídicos de obtenção de dados, os quais tendem a ser unificados à luz das recentes mudanças em torno da privacidade e da proteção de dados, haja vista a grande importância que os dados assumem na atualidade. Finalmente, o estudo resulta na constatação de diferenças marcantes entre privacidade e proteção de dados, o que justifica o reconhecimento de um novo direito fundamental autonômo; na demonstração dos vários tipos de dados existentes e seus riscos; e na apresentação dos regimes jurídicos de obtenção de dados admitidos, os quais tendem a ser uniformizados.

Palavras-chave: Privacidade; Proteção de dados; Dados; Regime jurídico; Obtenção de dados.

ABSTRACT

Technological advances have brought great prosperity to humanity, while also enshrining a number of new responsibilities. This reality would not be different with the Internet and the advent of computing devices, which enable interconnection at a global level and the dissemination of information in record time.In this sense, there is an increase in the generation of data and information, which can be used for the most varied purposes. In view of this, questions arise on how to make the use of this data viable without harming the fundamental rights of the holders. Following this line of research, for this study, it focuses on the data generated by the legal systems of delimitation of these data generated by the legal systems. The general objective of the study can be defined: to understand the legal regimes for obtaining data in the light of the current brazilian legal reality around the rights to privacy and data protection. As for the specific objectives, they revolve around the following aspects: differentiating the rights to digital privacy and data protection; analyze user-generated data and how it connects to the individual within the data protection microsystem; understand what are the legal regimes allowed to obtain this data and the possibility of unification. The methodological path, on the other hand, passes through the deductive theoretical research method, with the theoretical-normative approach, considering that the study is based on the ideas present in previously formulated research, to then build the specific arguments relevant to the topics covered. Added to this is the use of the bibliographic research technique, since the research focuses on the reading and analysis of theoretical works on privacy in the digital environment and data protection today. It should be noted that the main hypothesis that the research hopes to test is that legal regimes for obtaining data subsist in the Brazilian legal system, which tend to be unified in light of recent changes around privacy and data protection, given given the great importance that data assume today. Finally, the study results in the observation of marked differences between privacy and data protection, which justifies the recognition of a new autonomous fundamental right; in demonstrating the various types of existing data and their risks; and in the presentation of the legal regimes for obtaining admitted data, which tend to be standardized.

Keywords: Privacy; Data protection; Data; Legal regime; Data acquisition.

SUMÁRIO

1 INTRODUÇÃO

Os avanços tecnológicos revolucionaram a forma do ser humano se relacionar com o mundo ao seu redor e com o próprio ser humano. Entre as inovações marcantes, nota-se o advento da Internet e dos dispositivos informáticos que possibilitam a comunicação quase que instantânea e sem conhecer limites geográficos.

Percebe-se, nesse contexto, a potencialidade de alguns aspectos que já marcavam a trajetória da humanidade, mas que agora foram alçados ao epicentro das sociedades. Talvez o aspecto mais marcante dessa nova realidade seja a informação, a qual é utilizada como definidora dos relacionamentos atuais no que se definiu denominar de Sociedade da Informação. Nessa nova sociedade, a informação ganha elevada importância devido aos usos que ela pode assumir dentro da malha social.

Levando em consideração isso, os grandes atores privados começaram a captar essas informações e utilizá-las segundo seus interesses. No ambiente virtual, elas são difundidas, muitas vezes, na forma de dados e metadados. Ao se relacionar na rede, o ser humano deixa "rastros digitais", os quais, por mais que aparentemente inofensivos, revelam muito a respeito dos indivíduos, desde hábitos a concepções filosóficas e políticas.

Com o reagrupamentos desses dados, segundo interesses econômicos bem definidos, nota-se o surgimentos de uma nova forma de economia de mercado, qual seja o capitalismo de vigilância. Essa vigilância se aperfeiçoa pelas ferramentas já utilizadas na rede, como o Big Data. Nesse sentido, o cruzamento da grande gama de informações presentes no ambiente virtual atrelado a uma prática parasitária de exploração dos resultados obtidos com o tratamento, inegavelmente, pode ser prejudicial a alguns pilares da sociedade atual, como a privacidade, a autodeterminação informacional e a proteção de dados.

Dentre os mecanismos de regulação da Internet, percebe-se que o sistema jurídico tem o papel central na tarefa de conter esse cenário, tendo em vista que apresenta a prerrogativa de criar obrigações gerais e abstratas para as plataformas, os usuários e os provedores que utilizam esses recursos tecnológicos, sobretudo, para compatibilizar as práticas virtuais com o ordenamento jurídico de determinado país.

Para tanto, nota-se a necessidade tanto da adaptação do regime jurídico existente, como no caso da privacidade, a qual deve ser pensada em uma perspectiva plural, como o surgimento de novos direitos que devem fazer frente às mudanças fáticas e sociais experimentadas, a exemplo do direito à proteção de dados.

Esse novo direito à proteção de dados ganhou notoriedade recentemente com a elevação explícita à categoria de direito fundamental por meio de Emenda à Constituição. Uma mudança dessa magnitude apresenta o condão de repercutir em todo o ordenamento jurídico, de tal forma que interpretações devem ser revistas, leis devem ser compatibilizadas e entendimentos jurisprudenciais devem ser superados.

Depreende-se que a junção desses elementos eleva a complexidade do estudo, de modo que se faz necessário que pesquisas acadêmicas sejam realizadas para entender as mudanças que são geradas no ordenamento jurídico brasileiro. Desse modo, vislumbra-se que, mais do que atual e relevante, o tema em estudo é urgente, pois não se pode ignorar essa nova realidade social e jurídica.

Entre os pontos que merecem reflexões críticas, encontra-se o assunto da obtenção de dados. Por muito tempo, o ordenamento jurídico brasileiro separou a proteção do conteúdo das comunicações em um patamar e a proteção dos dados armazenados em outro (mais aquém). Não por outro motivo que se encontram em várias legislações esparsas a possibilidade de requisição de dados administrativamente, sem reserva jurisdicional.

Nesse sentido, emprega-se, neste estudo, o termo obtenção de dados como as maneiras pelas quais podem ser obtidos dados dos titulares, principalmente, na Internet, mas não se restringindo a ela. Quanto aos regimes, de um lado se aborda as interceptações do fluxo informacional e, do outro, a coleta de dados armazenados, seja por meio da requisição de dados, seja por meio do acesso direto ao dispositivo informático.

Partindo disso, para fins de delimitação da pesquisa, pode-se fazer o seguinte recorte do problema: os regimes jurídicos de obtenção de dados admitidos no Brasil podem ser unificados diante das recentes mudanças na temática da privacidade e da proteção de dados?

Esse questionamento ainda permite algumas outras problemáticas subjacentes: o direito à proteção de dados pode ser entendido como um direito fundamental autônomo em relação à privacidade? Quais os principais tipos de dados vinculados ao indivíduo que podem ser admitidos no microssistema de proteção de dados? Quais os principais regimes jurídicos para obtenção de dados existentes no sistema jurídico brasileiro? Eles podem ser unificados?

Todos esses problemas podem ser transpostos para objetivos de pesquisa. Inicialmente, pode-se pensar o objetivo central de pesquisa fixado em torno de compreender a existência da possibilidade de unificação dos regimes jurídicos de obtenção de dados e metadados à luz das mudanças vivenciadas com os direitos fundamentais à privacidade e à proteção de dados.

Por sua vez, os objetivos específicos podem ser delimitados nos seguintes termos: diferenciar o direito à privacidade do direito à proteção de dados, levando em consideração que a proteção de dados pode ser entendida como um direito fundamental autônomo; analisar os vários tipos de dados e metadados que compõem o microssistema de proteção de dados e como eles se vinculam ao indivíduo; compreender quais são os principais regimes jurídicos admitidos para obtenção de dados e se existe possibilidade deles serem unificados.

Já o caminho metodológico escolhido para instrumentalizar o estudo perpassa pelo método de pesquisa teórico dedutivo, com o enfoque teórico-normativo, tendo em vista que o estudo se sustenta nas ideias de alguns pesquisadores que se debruçaram sobre a privacidade e a proteção de dados na atualidade, de maneira sistemática e analítica. A partir desses marcos teóricos, desenvolveu-se a fundamentação específica em relação aos tópicos que são abordados pela dissertação.

Entre as premissas centrais que a pesquisa se apropria, encontram-se a ideia de Sociedade da Informação (CASTELLS, 2003); privacidade plural (LEONARDI, 2012); privacidade contextual (BIONI, 2021); perigo em torno do uso dos dados (MELGARÉ, 2021); (MAGRANI, 2019); (ZUBOFF, 2020); proteção de dados enquanto direito fundamental autônomo (SARLET, 2018); (SARLET, 2021); microssistema de proteção de dados e os vários tipos de dados com níveis diferentes de proteção (DONEDA, 2020); (ABREU; ANTONIALLI, 2017); a coexistência de regimes jurídicos de obtenção de dados (MOURA; BARBOSA, 2020a); dentre outras que complementam o enfoque.

Soma-se a isso o emprego da técnica de pesquisa bibliográfica, uma vez que a pesquisa se debruça sobre a leitura e análise de obras teóricas disponibilizadas, preferencialmente, de forma digital, tendo em vista a pandemia global, e no formato de livros ou de artigos científicos, já que são materiais mais atualizados. Especificamente, neste estudo, foram utilizados, majoritariamente, os livros e artigos em torno da matéria encontrados, sobretudo, até meados de agosto de 2022, principalmente, no Google Acadêmico e na plataforma Minha Biblioteca disponibilizada pela instituição.

Aqui é preciso esclarecer que a pesquisa, como em muitas outras, desenvolveu-se em etapas. Primeiro, foram lidos os capítulos de livro pertinentes encontrados na plataforma Minha Biblioteca. Ao término da leitura de cada capítulo, eram destacadas as referências citadas no texto que poderiam ser úteis a este estudo. Após, eram realizadas as leituras dessas obras destacadas por meio do Google Acadêmico, em que se buscava o texto na sua

plataforma original de divulgação, a exemplo do site de um periódico acadêmico. Em seguida, repetia-se o processo. Desse modo, o referencial teórico foi coletado de maneira orgânica.

Sobre esse recorte metodológico escolhido, depreende-se que ele é de grande valia para esta pesquisa devido à grande quantidade de material teórico produzido tanto na temática da privacidade como da proteção de dados. Diante disso, faz-se necessária a formulação de um estudo teórico que possibilite tanto a organização do referencial teórico existente como a exposição dos principais julgados sobre a matéria, os quais foram escolhidos pelo grau de relevância e pertinência com as bases teóricas utilizadas como fontes primárias.

Ademais, busca-se com essa pesquisa testar a hipótese de que subsistem no sistema jurídico brasileiro regimes jurídicos de obtenção de dados, os quais tendem a ser unificados à luz das recentes mudanças em torno da privacidade e da proteção de dados, haja vista a grande importância que os dados assumem na atualidade.

Para chegar a tais resultados, no primeiro capítulo, caracteriza-se o momento atual vivenciado na Sociedade da Informação e os desafios presenciados. Em seguida, aponta-se as várias acepções teorizadas para privacidade e aquela que melhor se adequa ao cenário atual. Por fim, distingue-se a privacidade da proteção de dados, de tal modo que a proteção de dados possa ser reconhecida como um direito fundamental autônomo.

Posteriormente, no segundo capítulo, aborda-se alguns pontos pertinentes sobre o microssistema de proteção de dados e os vários tipos de dados existentes, os quais podem ser classificados levando em consideração o vínculo com o titular dos dados. Nesse sentido, discute-se os riscos existentes com a disponibilização desses dados, os quais permitem, por exemplo, a identificação dos usuários da rede, de forma que o titular dos dados possa, em casos legítimos, exercer algumas prerrogativas.

Finalmente, no último capítulo, analisa-se os intermediários que auxiliam na coleta e armazenamento de dados, bem como os regimes jurídicos que vigoram no sistema jurídico brasileiro para a obtenção desses dados. Para realizar essa análise, abordam-se os possíveis requisitos e o procedimento para que isso ocorra, de tal modo que seja viável contemplar, em breve, um único regime de obtenção de dados.

Logo, percebe-se que o objeto de estudo é muito atual e apresenta o potencial de contribuir com os vários substratos dos atores que atuam com o tema da proteção de dados e da privacidade. Espera-se que a pesquisa possa servir como propulsor de novas pesquisas, haja vista que ela não esgota o assunto abordado.

2 PRIVACIDADE E PROTEÇÃO DE DADOS: DESAFIOS DA ATUALIDADE

A sociedade atual se revela mais hiperconectada do que nunca, o que possibilita a propagação de informações em tempo recorde. Diante disso, muitas vezes, o indivíduo perde o controle sobre as suas informações que acabam divulgadas incansavelmente, até mesmo em nível global. Isso transforma a maneira de entender os fenômenos sociais atuais e a forma de lidar com os desafios inerentes a essa nova realidade.

Nesse contexto, o Direito, enquanto uma ciência social, não pode se furtar da missão de analisar essa nova realidade em busca da melhor maneira possível de regular as relações sociais emergentes de uma sociedade cada dia mais complexa e imprevisível[1]. Tal análise perpassa pela releitura de alguns direitos já admitidos pela ordem jurídica, bem como pelo reconhecimento de novos direitos relacionados a essas mudanças presenciadas.

No primeiro caso, percebe-se que um exemplo de direito adaptável à nova realidade é o direito fundamental à privacidade, o qual ganhou vários sentidos ao longo da história e não seria diferente no momento atual. Já no caso de novos direitos, observa-se o surgimento do direito fundamental à proteção de dados, que protege o indivíduo das novas práticas que atentam contra sua dignidade, sejam oriundas do Estado, sejam oriundas de atores privados.

Levando em consideração tais aspectos, passa-se a analisar, por intermédio de uma revisão teórica bibliográfica[2], neste capítulo e nos subtópicos seguintes, os direitos à privacidade digital e à proteção de dados a partir dos desafios atuais decorrentes das tecnologias digitais[3], sobretudo da Internet.

2.1 AS TECNOLOGIAS DIGITAIS E A SOCIEDADE DA INFORMAÇÃO

---

[1] De fato, a inovação tecnológica é mais veloz do que as alterações legislativas, o que não quer dizer que ela deva ser ignorada pela normatividade jurídica (MELGARÉ, 2021).

[2] Utiliza-se de tal abordagem metodológica para situar o leitor nas discussões teóricas contemporâneas, tendo em vista que a temática da proteção de dados ganhou uma maior atenção na atualidade. Isso se deve, dentre outras coisas, ao fato de que os dados, potencializados pelas tecnologias digitais, proporcionam uma maior amplitude, escala e velocidade no fluxo de informações. Consequentemente, também se observa que maiores são os riscos em torno da violação desses dados. Após a realização dessas considerações teóricas, sustenta-se uma visão crítica dos resultados alcançados.

[3] Essas tecnologias, que se sobressaem na Revolução Informacional, representam o conjunto integrado de recursos que podem ser aplicados nos mais variados tipos de tarefas, como na geração de riqueza e na propagação de informações. Dentre essas novas tecnologias, ganham relevo a Internet e os computadores, enquanto ferramentas essenciais para a conexão entre os usuários da rede (CASTELLS, 2002).

As tecnologias digitais trouxeram implicações sociais, culturais e jurídicas que despertam o interesse acadêmico daqueles que buscam entender essa nova realidade[4]. No que se refere ao Direito, percebe-se o surgimento de várias dúvidas, como a maneira de regulamentação ideal do ambiente virtual, o qual reflete uma nova estrutura social.

Essas tecnologias, resultantes do desenvolvimento de pesquisas científicas, apresentam efeitos que vão além das projeções humanas. Nesse sentido, levando em consideração a sua imprevisibilidade intrínseca, nota-se que "[...] sua ação costuma se dar em um universo amplo e complexo a ponto de tornar análises de impacto, projeções e testes, em alguns casos, meras aproximações" (DONEDA, 2020, p. 46).

Para entender esses efeitos, deve-se considerar a tecnologia através de um perfil dinâmico e não apenas estático, haja vista a própria interação do ser humano com esses novos saberes, de tal modo que a tecnologia se revela em um constante processo de mutação a partir da retroalimentação que recebe da sociedade[5].

Partindo disso, surge a Galáxia da Internet, um novo ambiente comunicacional, o qual transforma a própria interação social e possibilita a criação de uma sociedade de rede. Essa sociedade conectada acarreta várias consequências e desafios para a vida das pessoas, a depender da história, cultura e instituições de cada povo (CASTELLS, 2003).

Desse modo, novos padrões de interação social são criados na Internet. De um lado, as pessoas passaram a interagir a partir de comunidades virtuais desvinculadas de localidades determinadas por meio de novos padrões seletivos de relações sociais[6]. Por outro lado, há quem defenda que a Internet conduziu ao isolamento social, haja vista que os sujeitos estão abandonando as interações em ambientes reais em função de uma sociabilidade aleatória com indivíduos sem face[7] (CASTELLS, 2003).

Diante disso, Lévy (1999) percebeu o surgimento de uma cibercultura que representa um novo universal construído a partir dos avanços tecnológicos das telecomunicações, principalmente, com o surgimento da Internet. Em síntese, a cibercultura compreende as

---

[4] Um exemplo de mudança que impactou todas essas esferas é o advento da Internet das Coisas (IoT). Essa nova tecnologia abrange o conjunto de dispositivos interconectados que apresentam a capacidade de transmitir dados coletados dos mais variados ambientes. Nesse sentido, vislumbra-se uma mudança da própria maneira do ser humano se relacionar com a máquina e com os demais seres humanos (MAGRANI, 2019).

[5] A retroalimentação contínua ocorre entre inovação e uso, ou seja, os conhecimentos e as informações são utilizados para criar novos conhecimentos e informações dentro do processo comunicacional, o que não ocorre de maneira centralizada (CASTELLS, 2002).

[6] Pela primeira vez, as pessoas conseguem se comunicar em escala global com o advento da Internet (CASTELLS, 2003).

[7] A bem da verdade, a Internet não cria o individualismo em rede, mas seu desenvolvimento propicia os recursos necessários para sua difusão como um padrão hegemônico de sociabilidade (CASTELLS, 2003).

técnicas, práticas, atitudes, valores, dentre outras coisas, que se desenvolvem em conjunto com o ciberespaço.

Ora, os sistemas tecnológicos são produzidos pela sociedade, a qual é estruturada culturalmente e a Internet não seria exceção. Inclusive, as novas tecnologias possibilitaram a ampliação dos agentes envolvidos na criação da cultura[8] no ambiente digital, haja vista as várias possibilidades de interação nesse ambiente, seja como consumidores, seja como produtores (profissionais ou amadores) (LESSIG, 2006).

Nesse sentido, a cultura não representa ideologias ou representações individuais, mas é uma construção coletiva que vai além de preferências individuais, de modo que ela influencia as práticas das pessoas que interagem em seu meio, notadamente dos usuários que são produtores na Internet[9] (CASTELLS, 2003).

Isso demonstra uma transposição dos aspectos ligados ao ambiente físico para o ambiente digital, levando em consideração as mais variadas possibilidades de interações sociais virtuais com a utilização de avatares digitais. Com tais avatares[10], as pessoas conseguem criar um círculo de convivência e revelar suas concepções pessoais, como gostos, crenças, relacionamentos, entre outros.

Desse modo, percebe-se que, sem adentrar em questões filosóficas mais específicas, "[...] vive-se, atualmente, em dois mundos: o mundo concreto e o mundo digital. Nos dois mundos, o indivíduo nasce, se constrói e estabelece relacionamentos. No mundo digital, no entanto, não se morre" (REIS; NAVES, 2020, p. 147).

Como se pode depreender dessa afirmação, a projeção do indivíduo persiste no ambiente digital mesmo com sua morte. Algo intangível, mas que representa a sua personalidade, seu modo de ser, seus relacionamentos, continua na rede. Esse "legado" digital se refere, dentre outras coisas, aos dados digitais, os quais podem ser extraídos, por exemplo, das redes sociais das quais o sujeito fazia parte. Após a extração, esses dados podem ser tratados e revelar os mais variados tipos de informações sobre o usuário.

---

[8] Entende-se por cultura o conjunto de valores e crenças comportamentais, ao passo que a repetição padronizada dos comportamentos exterioriza os costumes seguidos por instituições e organizações sociais informais (CASTELLS, 2003).

[9] A cultura material se transformou com o advento das novas tecnologias, tendo em vista que vivemos em um mundo que se tornou digital mediante a grande capacidade de gerar, armazenar, recuperar, processar e transmitir informações (CASTELLS, 2002).

[10] Insere-se nesse contexto o metaverso, recente inovação anunciada pelo Facebook, em que se possibilita ao indivíduo uma experiência de imersão virtual. Ou seja, as dimensões física e virtual podem ser vistas, de certa forma, em um mesmo plano, o que pode ser muito útil, por exemplo, para o aprimoramento de jogos virtuais ou até mesmo para a expansão de empresas nesse novo cenário digital (MALAR, 2021).

Essa é uma das peculiaridades que tornam a dimensão virtual do ser humano tão complexa e desafiadora, haja vista que a difusão quase instantânea dessas informações pode gerar repercussões em grande escala e dificultar a proteção de direitos fundamentais (SARLET, 2018).

Atrelado a isso, percebe-se que a informação se transformou em ponto central nas últimas décadas, tendo em vista a maior facilidade de coleta, tratamento e manipulação, o que pode ocorrer de várias formas e possibilitar que ela também seja usada de várias maneiras[11] (DONEDA, 2011).

Essa que pode ser apontada como uma característica marcante da Sociedade da Informação, em que existe uma rede de informações armazenadas, analisadas e usadas de diversas formas que impactam a sociedade. Mesmo que as pessoas não tenham noção do que ocorre, as suas vidas acabam moldadas por esses usos da informação[12] (CASTELLS, 2003).

Informação essa que é formada pelo processamento e organização de dados brutos, os quais são a matéria prima para o surgimento do conhecimento inteligível. Nesse sentido, cresce o interesse pela análise dos dados digitais e como eles podem ser utilizados e relacionados com seus titulares[13], tendo em vista que quanto maior for a captação de dados, maior será a possibilidade de descoberta de informações.

Portanto, depreende-se que as novas tecnologias, sobretudo aquelas voltadas para a informação e comunicação, com destaque para a Internet, moldaram a Sociedade da Informação. Nesse novo arranjo social, a informação e, por decorrência lógica, os dados digitais são utilizados de maneira central tanto nas relações humanas como na atividade econômica, não necessariamente em uma perspectiva positiva, como será analisado a seguir.

2.2 USOS CONTROVERSOS DA INFORMAÇÃO: POTENCIAL LESIVO DOS DADOS DIGITAIS

A Internet surgiu com a proposta de criar uma nova Era, na qual os governos pouco controlam as comunicações que ocorrem em nível global. Isso ocorre devido à dificuldade de

---

[11] Dentre tais maneiras, nota-se que as empresas a utilizam para realizar negócios; as instituições financeiras para conceder créditos; os empregadores para contratar; os agentes públicos para investigação; e os criminosos para cometer fraudes (SOLOVE, 2004).

[12] A Sociedade da Informação gera um contexto instável, em que os institutos jurídicos tentam se amoldar para tutelar essa nova realidade de constantes transformações e mutações (RUARO; RODRIGUEZ, 2010).

[13] Além disso, depreende-se que nem toda informação é pessoal, já que esse tipo de dado demonstra um vínculo objetivo com a pessoa, o qual revela ações ou características do indivíduo, como o nome, domicílio, dados de consumo, opiniões pessoais, dentre outras coisas, como será analisado em momento oportuno (DONEDA, 2011).

verificação das criações introduzidas na Internet. Tais criações difundem a liberdade de expressão sem mídias tradicionais de massa e possibilitam o compartilhamento da propriedade intelectual (músicas, produções, ideais etc.) de forma quase que ilimitada[14] (CASTELLS, 2003).

Nesse sentido, não existe um poder jurídico central que regulamenta os usos que o ambiente digital propícia. Ou seja, notam-se ilhas de poder formadas em torno de interesses locais, mas sem que nenhuma consiga se sobrepor de modo global. A bem da verdade, o mais próximo de um poder global de regulamentação é o exercido pelas próprias empresas que monopolizam as tecnologias digitais. Isso ocorre, muitas vezes, pela autorregulamentação imposta à revelia dos sistemas jurídicos. A consequência mais notável disso é que a Internet se desenvolve sem a obrigatoriedade de que os direitos dos usuários sejam respeitados.

Levando em consideração esse contexto, percebe-se que o poder se fortalece em torno das incertezas e a política se mostra insuficiente para lidar com os problemas e temores da vida das pessoas. Frente a essa lacuna, observa-se que o poder de vigilância, seja governamental, seja privado, cresce cada vez mais no mundo digital (BAUMAN, 2013).

Esse poder de vigilância, segundo o entendimento de Zuboff (2020), manifesta-se de maneira gradual sem que o usuário consiga entender de maneira plena os seus mecanismos, de tal modo que as informações dos sujeitos podem ser captadas e utilizadas para agregar conhecimentos sobre os indivíduos. Em posse desse conhecimento, torna-se possível, dentre outras coisas, moldar comportamentos.

Tal poder foi primeiramente notado pelo próprio Estado, o qual se colocou na posição de usuário das informações gerados no ambiente digital através da justificativa de que elas seriam relevantes para se tornar mais eficiente. Essa justificativa era utilizada em muitos casos de realização de pesquisas e censos, os quais, em tese, possibilitariam um conhecimento mais refinado da população (DONEDA, 2020).

Ademais, no início, nota-se que essa atividade de tratamento de dados não era interessante para a iniciativa privada devido aos altos custos. Com o desenvolvimento das tecnologias da informação nas últimas décadas, percebe-se que os organismos privados também foram inseridos nesse contexto de utilização das informações presentes na rede, muito devido aos baixos custos e às várias possibilidades que surgiram. Assim, "[...] a

[14] A Internet se revela como uma rede de computadores que independe de controle centralizado hierarquizado. Diante disso, o controle do fluxo de dados se torna muito custoso, já que a comunicação pode ocorrer de várias maneiras (DONEDA, 2020).

importância da informação aumenta à medida que a tecnologia passa a fornecer meios para, a um custo razoável, torná-la útil"[15] (DONEDA, 2020, p. 34).

O sucesso do progresso quantitativo e qualitativo da gestão da informação resulta no aglomerado de informações geradas e difundidas em determinado ambiente[16]. Tais informações, quando analisadas em conjunto, permitem deduzir padrões e projeções que antes seriam praticamente impossíveis. Um fenômeno que exemplifica bem como isso ocorre é o do Big Data, o qual possibilita que um volume "[...] descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades"[17] (BIONI, 2021, p. 34).

Nesse sentido, percebe-se que o Big Data é um termo ainda em evolução utilizado para descrever a exploração volumosa e célere de grandes quantidades de dados, sejam estruturados (presentes em bancos de dados), sejam semiestruturados, sejam não estruturados (não codificados), para a obtenção de informações. Tais informações são oriundas do cruzamento relacional de dados (MAGRANI, 2019).

Partindo disso, saliente-se que o principal diferencial do Big Data não seria a grande quantidade de dados em si, mas sim a capacidade notável de quantificar os fenômenos inseridos no mundo digital e manipular esses dados[18]. Com essa manipulação, pode-se descobrir informações que passariam despercebidas a olhares mais superficiais. Em casos mais sofisticados, mostra-se viável até mesmo prever eventos que ainda não ocorreram.

Um caso interessante, que exemplifica o mencionado, ocorreu quando determinada empresa americana, a partir de dados relacionados a hábitos de compras de futuras mães, detectou padrões de compras relativos às várias fases da gestação e desenvolveu um sistema de predição. Usando esse sistema, a empresa entrou em contato com uma adolescente oferecendo seus produtos, mas o pai da adolescente ficou inconformado com a sugestão de que a filha estaria grávida. Após o gerente entrar em contato com esse pai para se desculpar, o

---

[15] Essa utilidade mencionada é percebida mais pelas empresas privadas que utilizam as informações coletadas do que pelos próprios usuários, haja vista que, muitas vezes, as funcionalidades ofertadas aos indivíduos são realizadas por meio de uma troca pelas informações dos sujeitos. Desse modo, pode-se notar uma falsa ilusão de que as tecnologias digitais podem resolver vários problemas, sem que se questione o custo por trás disso (MOROZOV, 2018).

[16] Nota-se, inclusive, que os dados podem ser coletados até mesmo do mundo *off-line*, como o monitoramento de câmeras que rastreiam os movimentos humanos, a exemplo de uma câmera de monitoramento em uma empresa varejista que registra para onde os clientes estão olhando (REIS; NAVES, 2020).

[17] Percebe-se que os bancos de dados são, fundamentalmente, agrupamentos de informações organizadas "[...] de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações" (DONEDA, 2011, p. 92).

[18] Isto é, o sujeito é "[...] (re)conhecido a partir de uma série desordenada e aleatória de dados. Algoritmos os analisam por meio de *standarts* lógicos, e os inventariam e classificam, constituindo, assim, personas, avatares, perfis, representações virtuais de si mesmo" (MELGARÉ, 2021, p. 506).

homem informou que conversou com a filha e descobriu que ela, de fato, estava grávida. Ou seja, o sistema sabia mais da filha do homem do que ele mesmo (REIS; NAVES, 2020).

Desse modo, algumas indagações em torno do Big Data precisam ser realizadas, tendo em vista a relevância que os dados assumem na atualidade, de tal modo que não se pode deixar de mencionar a imprescindibilidade de análises que esclareçam a maneira como esse fenômeno ocorre, bem como por que, por quem e para quem esses dados são usados.

Isso se mostra urgente pela utilização crescente de algoritmos[19] autônomos que fazem uso de inteligência artificial[20] para aumentar sua capacidade de aprendizado, de tal modo que o tratamento dos dados pode ocorrer até mesmo sem interferência humana, o que pode acarretar casos indesejados, a exemplo de práticas discriminatórias[21]. Diante disso, há quem defenda[22] que se torna fundamental a existência de uma ética dos dados, isto é, ramo que aborde a coleta e a análise de dados[23] (REIS; NAVES, 2020).

Dentre os mecanismos que auxiliam esse processo, destacam-se aqueles relacionados à Internet das Coisas (IoT), a qual abrange o conjunto de dispositivos, dos mais variados tipos, que são interconectados digitalmente e apresentam a capacidade de reunir e transmitir dados de acordo com a política de dados definida pelo fabricante segundo seus interesses (MAGRANI, 2019).

Com a popularização desses dispositivos, a exemplo da Alexa, nota-se um contexto que potencializa o constante e intenso armazenamento, tratamento e compartilhamento de dados. Nesse cenário, o usuário acaba alienado dos riscos existentes pelos usos dos seus dados, tendo em vista que informações como essa nem sempre são passadas de maneira clara e precisa para o adquirente do produto "inteligente".

---

[19] Neste estudo, seguindo a definição proposta por Magrani (2019, p. 19), emprega-se o termo algoritmo como "[...] uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa, ou seja, uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa".

[20] Adota-se o termo inteligência artificial para se referir a sistemas computacionais que sejam capazes de emular a inteligência humana quando realiza certas tarefas. Isto é, consiga realizar algo que, em tese, apenas seria possível de ser executado pela inteligência de seres humanos (MAGRANI, 2019).

[21] Aliás, percebe-se que preconceitos estruturais podem ser ampliados com o uso da inteligência artificial atrelada à coleta de dados, o que ocorre com a utilização de decisões automatizadas que interferem na vida das pessoas. Assim, "[...] a abusiva e descontrolada coleta de dados, a obscuridade de tratamento e a análise que eles recebem – distante de qualquer controle e até conhecimento –, permitem práticas discriminatórias" (MELGARÉ, 2021, p. 508).

[22] Dentre os autores que defendem esse ponto de vista, pode-se citar Magrani (2019), o qual entende que a discussão em torno dessa vertente de ética deve ser realizada de maneira ampla e com a participação de diferentes atores (empresas, governos e sociedade civil). Caso essa reflexão ética não seja desenvolvida adequadamente, a tutela da privacidade e da proteção dos dados pessoais pode se tornar perigosa para a coletividade ou até mesmo inócua.

[23] É importante ter em mente que "[...] uma ética dos dados engloba a ética dos dados propriamente dita, mas também a ética dos algoritmos e a ética prática, o que a torna um estudo transdisciplinar" (REIS; NAVES, 2020, p. 157).

Nesse sentido, não são raras as situações em que são utilizadas cláusulas de uso padrão para legitimar a divulgação de informações sobre o indivíduo. Essa configuração geral é interpretada geralmente como recomendações implícitas e são aceitas de maneira conveniente pelas pessoas, o que, a depender das cláusulas estipuladas, pode dificultar a tutela dos dados envolvidos (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

Nessa perspectiva, a existência, muitas vezes, de contratos de adesão reduz a complexidade do tema em torno da noção de que é suficiente o conhecimento dos contratos, dos termos de uso, entre outras coisas, para que seja garantido o consentimento do titular sobre a coleta dos seus dados (MELGARÉ, 2021).

Desse modo, no mundo digital, também se percebe uma grande dificuldade de estabelecer o consentimento do titular dos dados diante das tecnologias da informação, como redes sociais e aplicativos, tendo em vista as limitações existentes à autonomia privada existentes em contratos de adesão (SARLET, 2021).

A bem da verdade, troca-se o acesso a *websites* por dados de navegação, os quais podem ser utilizados para a descoberta de informações, inclusive, pessoais. Ou seja, renuncia-se a direitos para que se consiga usar a Internet, de modo que os dados são repassados para aqueles que atuam na rede, inclusive, com aparência de legitimidade[24] (CASTELLS, 2003).

A junção desses pontos mencionados demonstram que, atualmente, os usuários se encontram em uma posição vulnerável em relação aos atores que captam, armazenam e tratam os dados presentes no ambiente virtual. Em posse desses dados, torna-se possível tanto a extração das informações que porventura interessem ao agente que realiza o tratamento, como o seu posterior uso para fins que podem ser questionados. Vários casos demonstram o potencial lesivo dessa prática.

Um caso ilustrativo que se relaciona à Internet diz respeito à publicação de mais de vinte milhões de registros de pesquisas de 657 mil usuários realizadas no provedor norte-americano de serviços de *Internet America Online*. Isso resultou na descoberta de uma usuária por dois repórteres do jornal *The New York Times* em poucos dias e sem maiores esforços (LEONARDI, 2012).

Também é possível elencar o exemplo da boneca “My Friend Cayla”, a qual era conectada por *bluetooth* e permitia o “diálogo” do usuário com a boneca por seu microfone embutido. Como se pode imaginar, essa tecnologia recebeu muitas críticas por possibilitar que sujeitos mal-intencionados invadissem o sistema da boneca e começassem a conversar com as

[24] Essa conjuntura ainda pode ser vista quando os serviços criam uma verdadeira obrigação (fática) de utilização, que esvazia a autonomia individual (SARLET, 2021).

crianças. A boneca foi banida da Alemanha, onde foi declarada como “brinquedo proibido” (MAGRANI, 2019).

Nesses termos, discutir os impactados dessa vigilância na sociedade se torna vital, uma vez que a tecnologia trouxe para a vida humana uma necessidade de conexão quase que irresistível, de modo que aquele que não adere ao uso dessas novas tecnologias corre o risco de ficar marginalizado no processo socioeconômico[25] (MELGARÉ, 2021).

Atrelado a isso, é preciso que se tenha em mente que a confluência dos fenômenos já mencionados, como o Big Data e a Sociedade da Informação, apresenta o potencial de conduzir a “dataficação” do próprio ser humano no ambiente digital. Quando isso ocorre, ignora-se o fato de o titular dos dados ser sujeito de direitos e de ele ser colocado no patamar de uma mera fonte de dados.

Isto é, a pessoa, através do conjunto de opiniões, emoções, gostos etc. é capturada “[...] por algoritmos e transformada em dados, torna-se um elemento decisivo para uma operação econômica. O sujeito transforma-se em um objeto, indiferente e contemplativo, sem controle sobre as relações intersubjetivas” (MELGARÉ, 2021, p. 505).

Seguindo essa linha de pensamento, percebe-se um reducionismo do ser humano a dados triviais, seja por atores privados, seja por atores público, o que compromete a dignidade humana dos indivíduos. Essa atitude ocorre, dentre outros motivos, devido à exploração econômica dos dados.

Essa exploração econômica se tornou muito rentável com as mudanças que ocorreram nas bases materiais da economia, na sociedade e na cultura graças, dentre outras coisas, à revolução tecnológica comunicacional e informacional presenciada, a exemplo do que ocorreu com a revolução industrial do século XVIII (CASTELLS, 2002).

Aliás, vislumbra-se uma mudança de paradigma, haja vista que, no modelo industrial antecessor, a produtividade se baseava nas novas fontes de energia e na capacidade de uso e circulação dessas fontes no processo produtivo. Já no novo modelo, a fonte produtiva se concentra na tecnologia voltada para a captação e criação de conhecimentos, processamento de informações e difusão da comunicação[26] (CASTELLS, 2002).

Isso se deve, dentre outras coisas, ao fato dos limites que existiam sobre as maneiras de captar, armazenar e utilizar as informações antigamente. Não é segredo que a

---

[25] Na modernidade líquida, nota-se que as mídias sociais são produto da fragmentação social e vice-versa. Nesse sentido, as redes de vínculos sociais também dependem das interações que ocorrem no ambiente digital (BAUMAN, 2013).

[26] Mais do que isso, a sociedade pós-industrial se baseia em serviços e retira sua principal fonte de poder da informação (BELL, 1973).

documentação dos atos da vida ficava a cargo de poucos que dominavam a escrita e a leitura, de tal modo que existia uma seletividade sobre o que deveria ser registrado. Atualmente, as coisas mais cotidianas podem ser gravadas em forma de dados e posteriormente utilizados para a criação de conhecimento.

Nesse sentido, quanto à sociedade pré-industrial, percebia-se que a informação não era uma preocupação central, uma vez que "[...] a documentação acerca das relações pessoais era restrita a uma pequena parte da vida das pessoas, e isso ocorria dentro de uma elite reinante. A rotina diária das pessoas comuns não era documentada de forma escrita" (RUARO; RODRIGUEZ, 2010, p. 182).

Progressivamente, com o aumento da complexidade social, em que as pessoas não podiam mais confiar apenas nas palavras das outras, surgiu a necessidade de documentar várias situações da vida das pessoas que antes não eram levadas a registro. Essa transformação elevou a informação para uma posição vital dentro da estrutura social moderna, haja vista que a documentação, o armazenamento e o uso das informações se tornam imprescindíveis para que a sociedade moderna surgisse e se desenvolvesse[27].

Para o sucesso desse novo modelo, moldou-se um poder que seduz de uma forma inteligente e não que constrange, já que "[...] ao invés de inibir, conter, atuar prescritivamente, faz com que o sujeito voluntariamente estabeleça liames com a dominação. Ao invés de subjugar, torna a pessoa dependente" (MELGARÉ, 2021, p. 514).

Nessa realidade, em que o Leviatã não é apenas o Estado[28], mas também as corporações privadas, busca-se instrumentalizar o viver humano através de práticas que predizem, modificam e modulam a conduta dos sujeitos para possibilitar a monetização (MELGARÉ, 2021).

Destaca-se, nesse cenário, uma forma de capitalismo que monitora o comportamento dos indivíduos e utiliza as informações pessoais desses sujeitos como matéria-prima para a criação de riqueza[29]. Seguindo essa linha, nota-se que existe uma rede complexa de vários atores "[...] que transaciona as informações pessoais dos consumidores, agindo

---

[27] Por exemplo, nessa sociedade moderna, dominada pelas transações eletrônicas, os modelos de negócios precisaram se adequar às novas tecnologias baseadas na Internet, em que a economia é interconectada através do relacionamento entre compradores e fornecedores (CASTELLS, 2003).

[28] Vislumbra-se que muitas informações pessoais do sujeito acabam sendo compartilhadas indevidamente na Internet pelo próprio governo, informações que dizem respeito a várias peculiaridades da vida do indivíduo, como endereço, situação financeira, problemas médicos, transgressões legais, filiação, bens, dentre outras (SOLOVE, 2004).

[29] Isso se mostra preocupante, já que os dados que originam as informações pessoais, na sociedade atual, representam um dos mais importantes pilares do contrato social. Nesse sentido, esses dados exteriorizam como a pessoa é vista no mundo, além de permitir o exercício de direitos e da cidadania, de modo que a proteção desses dados pessoais é imperiosa para permitir o desenvolvimento, a inovação e a liberdade (BIONI, 2021).

cooperativamente para agregar mais e mais dados e, em última análise, tornar a mensagem publicitária ainda mais eficiente" (BIONI, 2021, p. 42).

Percebe-se o surgimento de um verdadeiro "capitalismo de vigilância"[30], o qual lucra por meio da exploração estratégica da grande quantidade de dados captados, armazenados e processados, legitimamente ou não, no ambiente virtual. Como os dados assumem o viés de matéria-prima, observa-se que o atores que tratam os dados conseguem, por exemplo, vender ou trocar dados com outros atores como se fossem proprietários das informações decorrentes da análise desses dados[31].

Nessa perspectiva, Zuboff (2020) entende que o capitalismo de vigilância define uma nova ordem econômica pautada no uso das experiências humanas como matéria-prima gratuita das práticas comerciais de extração, previsão e vendas, as quais operam por uma lógica dissimulada e parasitária que sustenta uma economia de vigilância prejudicial para a própria natureza humana.

Desse modo, o capitalismo de vigilância não é focado nos consumidores, mas na antecipação dos comportamentos dos sujeitos. Ou seja, os consumidores, na verdade, adquirem produtos ou serviços que são meramente hospedeiros de práticas parasitárias do capitalismo de vigilância, como no caso das bonecas que espionam ou máquinas que se dizem inteligentes (ZUBOFF, 2020).

Essas práticas do capitalismo de vigilância podem se estender para a esfera pública e afetar sistemas políticos, como no caso da Cambridge Analytica[32]. O espaço democrático acaba comprometido por processos automatizados dominados pelo capitalismo de vigilância que interferem na opinião pública e, por conseguinte, na decisão livre dos cidadãos, pressuposto fundamental para a democracia[33] (MELGARÉ, 2021).

---

[30] São exemplos de ferramentas de vigilância: a utilização de *cookies* por *websites* para as mais variadas finalidades e o registro automático de informações referentes ao número de IP, data e hora de acesso pelos *websites* (os quais podem ser utilizados, posteriormente, para identificar o sujeito) (LEONARDI, 2019).

[31] Diante disso, a estrutura digital é moldada em função "[...] dos interesses do capital e das grandes corporações que atuam – ou melhor seria dizer, controlam? – no/o mercado da tecnologia" (MELGARÉ, 2021, p. 507).

[32] Essa firma de consultoria do Reino Unido ganhou destaque com sua atuação polêmica em campanhas políticas, a exemplo da estadunidense que elegeu Donald Trump e do *Brexit* em 2016. Nesses casos, foi utilizada a coleta massiva de informações comportamentais dos indivíduos para auxiliar no direcionamento que as campanhas tomariam. Vislumbra-se que esses casos demonstram na prática como os mecanismos próprios do capitalismo de vigilância são aplicados na esfera política, dentre os quais ganham relevo: a capacidade de vigilância; a combinação de informações brutas; a utilização de inteligência de máquina; a geração de resultados que predizem ações futuras, dentre outras coisas (ZUBOFF, 2020).

[33] Essa tática de utilização de dados para os mais diversos fins não é nova. Já nas eleições de 2000 nos EUA, foi utilizado o banco de dados Aristotle com dados que revelam os perfis políticos de pelo menos 150 milhões de cidadãos para fins de campanha política (CASTELLS, 2003).

Com o sucesso dessa estratégia, os sistemas democráticos acabam capturados por interesses externos ao da nação, de tal modo que a democracia não consegue auxiliar no desenvolvimento daquele determinado povo, mas apenas legitimar a exploração segundo os desejos dos grandes atores que manipulam essa nova vertente de capitalismo. Quanto maior for a influência sobre os usos dos dados, mais desprotegido o usuário estará.

Diante disso, a sociedade democraticamente organizada está se transformando em virtude das dimensões digitais da vida humana, o que perpassa pelo correto entendimento do que significa a divulgação de informações na atualidade. Essa compreensão possibilita uma proteção mais adequada diante das distorções e manipulações que podem ocorrer, tendo em vista que "[...] os dados dos cidadãos permanecem desprotegidos de espionagem, mau-uso, manipulação e freqüentes equívocos" (RUARO; RODRIGUEZ, 2010, p. 184).

Nesse sentido, a exploração dos dados oriundos da experiência humana, os quais são utilizados como matéria-prima gratuita para as mais diversas práticas comerciais ocultas, cria esse modelo de negócio parasitário da própria vida humana, o qual é utilizada para conferir lucro às corporações[34].

Isso é materializado pelos dossiês digitais que são formados pelo fluxo de informação que interliga negócios, organizações e entidades governamentais. Esse fluxo pode se dividir em três caminhos: os que partem das grandes bases de dados do setor privado; os que fluem dos registros públicos para o setor privado; e os fluxos que saem do setor privado para o público (SOLOVE, 2004).

Nesse contexto, "[...] a pessoa se posta – e é posta – de modo transparente, sem qualquer coerção ou prescrição normativa, disponibilizando na rede todo o tipo de dado, processado sabe-se lá como, por quem, quando, de que maneira e com quais finalidades" (MELGARÉ, 2021, p. 513).

Ou seja, a vigilância sutil se espalha de forma nunca vista, captando fragmentos de dados que podem ser utilizados para diversos fins. Nesse sentido, a vigilância interage e reproduz a liquidez moderna se moldando a uma vigilância líquida (BAUMAN, 2013).

Diante disso, a distopia em torno da vigilância constante[35] parece se realizar atualmente com os indivíduos alienados e focados nas suas necessidades pessoais, sem questionar os mecanismos de controle refinados. Com isso, seus comportamentos são

---

[34] Pode-se dizer que o modelo de negócio é pautado na falta de transparência, a qual se sustenta no desconhecimento da invasão da privacidade e na modulação de comportamentos (MELGARÉ, 2021).

[35] A metáfora que ganhou destaque quanto à vigilância foi a figura do Grande Irmão de George Orwell, o qual surge quando a administração governamental se concentra em uma figura que utiliza os recursos administrativos como forma de controle total (BAUMAN, 2013).

facilmente manipulados em função dos usos controversos que são dados para as informações colhidas, as quais são extraídas, não raras vezes, de dados "inofensivos".

Nesse sentido, como sustenta Melgaré (2021), o Direito deve combater essa realidade, que precisa se adequar aos preceitos constitucionais que garantem, dentre outras coisas, a liberdade individual, a privacidade e o desenvolvimento da personalidade de maneira livre. É necessário que se reconheçam as desigualdades entre os atores que atuam na Internet, sobretudo do titular do dado, o qual não compreende, em muitos casos, a complexidade negocial por trás dos algoritmos utilizados[36].

Todavia, Zuboff (2020) adverte que esse novo modelo de negócios não encontra precedentes na história, o que, de certa forma, dificulta a criação de novas leis específicas que protejam os indivíduos daquilo que não se sabe dimensionar ao certo. Diante disso, deve-se fomentar o debate e a contestação desse sistema por instituições democráticas saudáveis, para que se construam bases legislativas e jurisprudências mais sólidas.

Desse modo, o ser humano se encontra no meio de um processo de objetificação através do uso desmedido dos seus dados pessoais que são coletados de maneira quase que imperceptível pelo sistema de vigilância moderno. Em posse desses dados, tanto o Estado como atores privados conseguem lucrar com a comercialização de informações pessoais, principal produto da Sociedade da Informação e matéria-prima do capitalismo de vigilância. Frente a esse contexto, é imperativo que o Direito defenda a dignidade humana e o sistema democrático em detrimento das práticas parasitárias do capitalismo de vigilância.

Portanto, deve-se buscar novos caminhos para os problemas oriundos das tecnologias digitais, que perpassam pelo uso controverso e desenfreado da informação através de um sistema de vigilância e de captação que muitas vezes ignora o potencial lesivo que o uso indevido dos dados pode representar para os usuários. Com isso, direitos fundamentais podem ser feridos, a exemplo da privacidade, como será esmiuçado a seguir.

2.3 PRIVACIDADE VIRTUAL: UMA RELEITURA A PARTIR DAS SUAS POSSÍVEIS CONCEPÇÕES

É importante reconhecer que, por mais que as novas descobertas tenham trazido avanços em vários campos, também originaram novos problemas, que demandam novas

[36] Caso não seja possível realizar a adequação desse modelo negocial aos preceitos constitucionais, ele deve ser afastado como outras atividades que também não se compatibilizaram com os direitos e garantias fundamentais (a escravidão, por exemplo), tendo em vista que o ser humano não é passível de se tornar objeto de negócios (MELGARÉ, 2021).

soluções jurídicas. Entre tais problemas, ganha relevo o perigo em torno da violação da privacidade do indivíduo por intermédio da facilidade de divulgação de informações na rede mundial de computadores. Assim, a privacidade precisa ser ressignificada perante essa nova realidade social que decorre do ambiente virtual.

Há quem fale, inclusive, em "morte da privacidade", justamente, porque os dados pessoais são matéria-prima da atual economia, a qual é gradativamente mais dependente do livre fluxo informativo, além do que é um importante mecanismo estratégico de várias estruturas de negócios e formulação de políticas públicas[37] (BIONI, 2021).

Nesse sentido, os indivíduos experimentam a incerteza de entender como a sua privacidade pode ser violada na atualidade. Nota-se que, quando a privacidade física é invadida, a exemplo da invasão domiciliar, a resposta é rápida e natural. Todavia, quando a invasão ocorre no âmbito das informações pessoais virtuais, os sujeitos hesitam em tomar providências por não ter certeza sobre quando a privacidade realmente está comprometida (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

Vislumbra-se que essa erosão da privacidade pode ameaçar a autonomia do indivíduo, seja como consumidor, seja como cidadão, haja vista que o aumento do compartilhamento de dados não implica necessariamente em progresso, eficiência ou igualdade. Ora, evidencia-se que "[...] o potencial de abuso de dados pessoais - para discriminação econômica e social, influência oculta e manipulação, coerção ou censura – é alarmante" (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015, p. 509).

Ocorre, ainda, a tentativa de neutralização dos impactos trazidos pelas novas tecnologias por intermédio da perspectiva de que a erosão da privacidade seria uma consequência natural dos avanços obtidos, de modo que a relativização da privacidade é algo natural ou o preço a ser pago pelos avanços experimentados pela sociedade de consumo (DONEDA, 2020).

Essa linha de pensamento acaba ganhando muitos adeptos devido à valorização que é dada aos serviços presentes na rede. Por exemplo, as redes sociais satisfazem necessidades ligadas à socialização e ao reconhecimento social, o que leva muitos usuários a sequer questionar suas políticas de uso, uma vez que eles ponderam que a necessidade de continuar utilizando a ferramenta é maior do que os potenciais riscos que isso poderia representar.

---

[37] Por exemplo, percebe-se que a grande quantidade de dados coletados pelos dispositivos da IoT coloca em risco o direito fundamental à privacidade, uma vez que os dados captados dizem respeito a vários aspectos da vida dos usuários (MAGRANI, 2019).

O fato é que essas informações pessoais armazenadas através dos dados pessoais se mostram ligadas à privacidade pela lógica de que quanto menor for a difusão dessas informações, mais se garante a privacidade do sujeito. Nesse sentido, não é possível ignorar que esses problemas apresentados são também desdobramentos da tutela do direito à privacidade (DONEDA, 2011).

Por sua vez, é complexo definir um conceito para direitos da personalidade, a exemplo da privacidade, o que a legislação brasileira não fez. Diante disso, algumas visões teóricas se destacam nessa tarefa, como a que defende esses direitos como extensão da própria pessoa humana, e a que entende esses direitos ligados à esfera relacional do indivíduo, tendo em vista que o ser humano é um ser social por excelência (BIONI, 2021).

Quanto à definição de privacidade, tanto a doutrina brasileira como a estrangeira se valem de uma gama de termos para se referir a tal direito fundamental. Não raras vezes, pode-se encontrar a privacidade relacionada a expressões como intimidade, segredo, sigilo e vida privada[38] (LEONARDI, 2012).

No Brasil, não há uma definição uníssona do que venha a ser privacidade, intimidade, vida privada ou termos correlatos, o que gera uma lacuna aparente no sistema jurídico pátrio. Inclusive, a própria Constituição Federal de 1988 não utiliza, de maneira expressa, o termo privacidade ao longo do seu texto, mas assegura a proteção da intimidade, da vida privada, da honra e da imagem das pessoas (LEONARDI, 2012).

Em igual sentido, o Código Civil de 2002 não utiliza, de maneira expressa, o termo privacidade, uma vez que se restringe a mencionar que a vida privada da pessoa natural é inviolável, de modo que o juiz, através do requerimento da parte interessada, tomará as medidas protetivas necessárias para impedir ou fazer cessar violação a esse direito (LEONARDI, 2012).

Depreende-se, desse modo, que a proteção conferida à privacidade decorre, ainda que implicitamente, das normas presentes no texto constitucional e se irradia por todo o ordenamento jurídico pátrio. Pode-se citar como exemplos de normas infraconstitucionais que garantem a proteção a esse direito fundamental, além do Código Civil, as normas presentes no Código de Defesa do Consumidor (CDC), bem como no Marco Civil da Internet (MCI), o que fazem de forma mais específica[39] (MAGRANI, 2019).

---

[38] Observa-se que a privacidade se revela como um conceito jurídico indeterminado, a exemplo da dignidade da pessoa humana. Seguindo essa linha, muitas vezes, a definição fica a cargo dos juristas, o que pode gerar certa insegurança jurídica (LUZ, 2019).

[39] Essa lista ainda pode ser atualizada com a Lei Geral de Proteção de Dados (LGPD), a qual também aborda a temática da privacidade a partir da proteção dos dados dos usuários.

Isso muito se deve ao fato de que o direito à privacidade ingressa nos ordenamentos jurídicos com uma perspectiva nitidamente patrimonialista, que era exercida por aqueles pertencentes a determinados extratos sociais mais elevados. Essa característica individualista e patrimonialista dominou esse direito fundamental por muito tempo[40] (DONEDA, 2020).

Nesse sentido, a definição e delimitação da privacidade reflete os valores e projeções do homem em cada sociedade, de modo que apresenta um forte conteúdo social e ideológico, para além do dogmático. Diante disso, pode-se notar a existência de extremos, isto é, aqueles que defendem fervorosamente esse direito fundamental e aqueles que renegam sua autonomia.

A bem da verdade, a definição precisa do que é privacidade é uma tarefa difícil, já que ela é considerada uma palavra "guarda-chuva", que revela seu conteúdo, muitas vezes, quando se está diante de casos concretos, como aqueles envolvendo domicílio, correspondência e comunicação. Pensar dessa forma ajuda a entender que a definição desse direito fundamental vai além de contornos conceituais e adentra nas vivencias sociais.

Partindo disso, a privacidade é delimitada segundo a precisão de capturar situações que melhor se enquadram nos contornos do que se entende por privacidade e excluir aquelas situações que, usualmente, não são abarcadas no seu âmbito de abrangência. Todavia, "[...] o principal problema desse método de conceituação é que ele acaba por produzir conceitos ora excessivamente restritivos, ora excessivamente abrangentes" (LEONARDI, 2012, p. 51).

Algumas categorias que se destacaram na tentativa de explicar o direito à privacidade foram as unitárias, as quais podem ser separadas em quatro grupos: "[...] a) o direito a ser deixado só (*the right to be let alone*); b) o resguardo contra interferências alheias; c) segredo ou sigilo; d) controle sobre informações e dados pessoais" (LEONARDI, 2012, p. 51).

No primeiro caso, o direito a ser deixado só (*the right to be let alone*), nota-se que a privacidade decorreria da própria inviolabilidade dos direitos de personalidade do indivíduo, de modo que se busca superar o vínculo existente entre esse direito e a propriedade privada. Tal vínculo ocorria pela primazia que o patrimônio tinha em relação a muitos dos direitos que o sujeito era titular.

O direito de ser deixado só, o qual foi influenciado pela obra "The Right to Privacy" (o direito à privacidade), dos autores Samuel Warren e Louis Brandeis, ainda em 1890, sustenta uma visão de privacidade ligada à inviolabilidade da personalidade, de modo que

---

[40] A privacidade se estabeleceu em consonância com a típica individualidade burguesa e não como uma continuidade anterior, tendo em vista o surgimento da noção desse direito atrelado à possibilidade material de assegurá-lo (DONEDA, 2020).

esse direito fundamental foi ressignificado para não abarcar apenas à propriedade privada (WARREN; BRANDEIS, 1890).

Diante disso, o valor da privacidade se encontra na tranquilidade ou na paz de espírito de impedir a violação à privacidade com publicizações indevidas e não na indenização posterior pelo ato. Isto é, "[...] o respeito à vida privada se traduz, essencialmente, em um dever de abstenção, representado pela máxima 'deixe-me tranquilo'" (LEONARDI, 2012, p. 54).

Na segunda hipótese, resguardo contra interferências alheias, observa-se que determinados atos seriam divulgados e outros seriam reservados. Com isso, o indivíduo conseguiria viver sua vida com um grau mínimo de interferências, dado que não seria viável viver em sociedade sem que nenhuma de suas informações fossem reveladas[41].

Essa definição ganhou muitos simpatizantes devido, em grande parte, à teoria das esferas de matriz alemã, a qual estipula que existiriam três esferas distintas e com intensidades de proteção diferentes. A primeira seria a de foro íntimo (inviolável); a segunda a esfera privada; e a terceira a esfera social, que compreende o que não for englobado nas outras delimitações[42] (LEONARDI, 2012).

Em terceiro lugar, também se pode pensar a privacidade em torno da ideia de segredo, ou sigilo, de certas informações do sujeito. Nesse sentido, parte-se da dicotomia entre informações públicas e privadas[43]. Talvez o maior problema dessa vertente seja, dentre outras coisas, entender o sigilo das informações como essência da privacidade e não como um dos meios de proteção possíveis[44].

Além disso, observa-se que, em certos casos, o próprio indivíduo pode optar em compartilhar suas informações com determinado grupo de pessoas e ocultá-las de outros sujeitos. Assim, depreende-se que essa noção de privacidade equipara a o segredo a um sigilo absoluto, "[...] *erga omnes*, e não relativo e seletivo, ignorando que, ao compartilhar certas informações privadas, nem sempre o indivíduo almeja mantê-las em segredo, mas apenas deseja confidencialidade" (LEONARDI, 2012, p. 65).

---

[41] Vislumbra-se que o indivíduo elege quais fatos são resguardados e quais podem ser públicos. Inclusive, parte da doutrina entende que essa perspectiva da privacidade seria justamente o direito à intimidade (LUZ, 2019).

[42] Percebe-se que esse conceito é passível de críticas na medida que não estipula de forma clara quais seriam as interferências razoáveis ou não, ou seja, qual seria o limite que o sujeito deveria ser tolerante em relação à invasão da sua privacidade (LEONARDI, 2012).

[43] Essa divisão entre esfera pública e privada é realizada de tal modo que a violação da privacidade ocorreria quando uma informação da esfera privada (secreta ou sigilosa) torna-se pública (LUZ, 2019).

[44] A proteção ao sigilo não deixa de ser uma proteção contra a interferência alheia (LUZ, 2019).

Outrossim, percebe-se que não existe relação direta entre a noção de segredo e privacidade, haja vista que existem informações secretas que não seriam necessariamente privadas, como a relação de débitos de alguém. Diante disso, nota-se que "[...] a privacidade engloba mais do que o impedimento da revelação de informações secretas" (LEONARDI, 2012, p. 66).

Além do mais, essa forma de pensar a privacidade foi prejudicada pela atual estrutura social informacional, como já mencionado, em que as informações são captadas constantemente de acordo com "rastros" deixados pelos indivíduos[45]. Desse modo, reduzir a privacidade a dicotomia entre público e privado prejudicaria a correta compreensão desse direito fundamental.

Para resolver esse impasse, a privacidade também foi delimitada como o controle sobre informações e dados pessoais[46]. Essa corrente ganha relevância na atualidade devido à grande quantidade de atos humanos praticados por intermédio de mídias digitais, o que gera, consequentemente, o crescimento vertiginoso de informações e dados no ambiente virtual.

Nessa perspectiva, estipula-se como atributo básico da privacidade a capacidade de o titular das informações gerenciar o fluxo de informações que sejam relacionadas a ele. Com isso, observa-se que "[...] a privacidade é a reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que extensão informações a seu respeito são comunicadas a terceiros" (LEONARDI, 2012, p. 67).

Nesses termos, depreende-se que esse controle engloba tanto o consentimento do titular do dado, como a utilização do fluxo informacional de acordo com as legítimas expectativas do sujeito, em conformidade com o livre desenvolvimento da sua personalidade[47] (BIONI, 2021).

Partindo disso, pode-se pensar até em controle misto, isto é, o sujeito controlaria sua privacidade dentro da sua esfera privada, ao passo que seria protegido em âmbito público. Desse modo, todos que buscam monitorar, coletar, utilizar e armazenar dados pessoais necessitam de motivos plausíveis para a vigilância (BERNAL, 2014).

---

[45] Aliás, esses rastros são captados como uma invasão relativamente pequena e inócua da privacidade, tendo em vista que as pessoas não sofrem danos diretos quando os seus dados são manipulados pelas empresas que atuam em cadeia, o que prejudica o reconhecimento da violação (SOLOVE, 2004).

[46] Diante dessa vertente, a própria pessoa determinaria sua esfera particular, o que vai além do simples controle isolado, haja vista a disparidade de poderes entre os atores que atuam na rede (RODOTÀ, 2008).

[47] Para Rodotà (2008), por exemplo, a privacidade passaria da ideia de isolamento para a possibilidade de cada sujeito controlar as suas informações pessoais, de modo que ganha relevo o tipo de conhecimento manifestado, o qual deve ser adequado e livre.

Por mais plausível que seja conceituar a privacidade em função da capacidade de controle do indivíduo, essa noção também não delimita perfeitamente a noção de privacidade, uma vez que acaba se tornando insuficiente diante da implementação de novas tecnologias. Essa implementação não necessariamente leva em conta a livre manifestação de vontade dos usuários, de tal modo que não seria possível um controle efetivo.

Por exemplo, observa-se que a privacidade pode ser protegida ou violada dependendo dos mecanismos tecnológicos pré-estabelecidos pela própria arquitetura da rede. Nesses casos, cabe ao usuário apenas escolher entre opções pré-estabelecidas, isso quando existe alguma faculdade de escolha (LEONARDI, 2019).

Além disso, no modelo social atual, a obscuridade em torno da ideia de esfera privada faz com que se interprete e se negocie sobre a privacidade de maneira situacional. Ou seja, age-se de acordo com a situação com base em preceitos culturais, motivacionais e contextuais (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

A maneira como as informações são repassadas também afetam as decisões relacionadas à privacidade. Segundo pesquisa especializada, a tendência das pessoas é comprar de vendedores que apresentem os menores preços, independentemente da política de proteção da privacidade[48] (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

Contudo, quando os buscadores oferecem informações relevantes e de fácil acesso aos participantes sobre as diferenças no grau de proteção da privacidade dos comerciantes, percebe-se que as pessoas escolhem comprar com comerciantes que protegem a privacidade, inclusive, pagando a mais[49]. Ora, não é costumeiro o compartilhamento de dados de cartão de crédito, por exemplo, com vendedores sabidamente desprotegidos (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

Desse modo, não basta apenas informar ou empoderar o sujeito sobre os riscos atuais em torno da privacidade colocados pelas novas tecnologias de informação. Mais do que isso, é imprescindível que haja transparência para que se proteja satisfatoriamente a privacidade por meio de políticas suficientemente flexíveis para evoluir e se adaptar às complexidades emergentes que são imprevisíveis.

---

[48] Interessante notar esse aparente paradoxo que se forma em torno de contextos como o da pesquisa: pessoas dizem se importar com a privacidade, mas dependendo dos custos e benefícios atrelados a uma situação específica, podem buscar ou não proteger a privacidade (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

[49] Depreende-se que a grande maioria dos usuários da Internet não lê as políticas de privacidade. No entanto, mesmo se o fizesse, talvez não entendessem, já que quase metade das políticas de privacidade on-line verificadas era escrita em linguagem de difícil compreensão para grande parte dos internautas (ACQUISTI; BRANDIMARTE; LOEWENSTEIN, 2015).

Nesses termos, observa-se que a privacidade, que antes era garantida pela própria lógica da rede[50], a qual era pautada no anonimato da comunicação e na dificuldade de identificação das origens da transmissão, agora corre perigo devido aos usos das novas tecnologias como ferramentas aptas a violar esse direito fundamental (CASTELLS, 2003).

Diante disso, depreende-se que os conceitos unitários apresentados ainda são inconclusivos ao tratar da privacidade, seja por serem muito abrangentes, seja por serem muito restritos. O fato é que o denominador comum buscado é de difícil especificação. Contudo, talvez o maior aprendizado que essas teorias repassem é que uma definição aceitável de privacidade não será atingida a partir de uma visão individualista, em que os encargos ficam a conta do sujeito.

Isso fica evidente porque a privacidade abandona seus sentidos tradicionais e assume, cada vez mais, um caráter relacional, tendo em vista que o sujeito determina sua esfera privada (sua individualidade) por meio do nível de interação com o mundo exterior e com as outras pessoas. Isto é, ele estabelece o nível de exposição e de inserção que deseja (DONEDA, 2020).

Partindo disso, nota-se que é mais interessante conceber a privacidade segundo uma visão plural, já que existem semelhanças entre os casos concretos, mas nenhum é idêntico ao outro, apenas se relacionam[51]. Ou seja, é preciso compreender o direito à privacidade, no Brasil, "[...] em um sentido genérico e amplo, como destacado anteriormente, necessário para sua tutela em face das novas modalidades de violação proporcionadas pelo uso de computadores e da Internet" (LEONARDI, 2012, p. 89).

Todavia, adverte-se que essa delimitação mais aberta de privacidade não resolve todos os problemas decorrentes da atualidade. A bem da verdade, mostra-se mais prudente que essa concepção seja agregada a novos regimes protetivos mais voltados para a compreensão aprofundada dos desafios atuais trazidos pelas novas tecnologias, de tal modo que se torne possível o apontamento de soluções mais duradouras.

Levando em consideração essa conclusão, mostra-se inevitável que sejam criadas novas fronteiras adequadas ao cenário digital, tendo em vista que o direito à privacidade não se revela mais suficiente para tutelar um cenário em que ocorre o armazenamento quase que

---

[50] Redes irrestritas de computadores ligadas através de protocolos aversos à censura moldaram a "natureza" da Internet em função da liberdade e da dificuldade de controle (CASTELLS, 2003).

[51] Essa visão plural de privacidade abarca várias possibilidades conforme as peculiaridades do caso concreto, de modo que esse direito fundamental complexo assuma mais de uma feição protetiva (LUZ, 2019).

ilimitado de dados das mais variadas naturezas, os quais são usados sem um controle rigoroso tanto pelo Estado como por particulares[52] (RUARO; RODRIGUEZ, 2010).

Logo, mais do que a definição conceitual de privacidade, é necessário que novos caminhos protetivos sejam traçados, em consonância com essa lógica de privacidade plural citada. Dentre esses novos rumos, encontra-se o direito à proteção de dados, o qual se vincula diretamente com o contexto apresentado, como será visto a seguir.

2.4 DIREITO AUTÔNOMO À PROTEÇÃO DE DADOS NO BRASIL: UM NOVO DIREITO FUNDAMENTAL

Percebe-se que o processamento automatizado de dados passou a representar um risco para o indivíduo, haja vista que a atividade de tratamento de dados impacta progressivamente a vida das pessoas, principalmente, no que diz respeito às decisões automatizadas que definem o futuro do indivíduo. Para fazer frente a esse cenário, mostra-se imperioso o desenvolvimento de um novo direito à proteção de dados.

Esse novo direito já surge com uma tarefa árdua, uma vez que ele vai lidar com situações "[...] que dizem respeito à proteção da pessoa, mas também à higidez do Estado democrático, à liberdade de informação e expressão, à segurança jurídica para os mercados, entre tantas outras" (DONEDA, 2021, p.23).

Os marcos regulatórios da temática são, em grande parte, de matriz europeia, o que não exclui o caráter global do assunto, tendo em vista, por exemplo, a origem de alguns institutos nos Estados Unidos. Diante disso, o núcleo central é formado pela influência mútua e dinâmica de vários sistemas jurídicos, com destaque para o europeu e o estadunidense (DONEDA, 2021).

Em tais países, o desenvolvimento econômico e o tecnológico, dentre outros fatores, aceleraram o reconhecimento de problemas ligados à privacidade e à proteção de dados pessoais. Diante disso, é natural que eles sejam tidos como exemplos de vanguarda quanto ao estabelecimento de instrumentos regulatórios e jurídicos de tutela aos direitos individuais afetados pelas mudanças experimentadas.

Já no Brasil, a regulamentação da temática não se encontra tão desenvolvida muito devido à manutenção da proteção de dados vinculada à privacidade por muito tempo. Não se

[52] Ou seja, não é possível admitir a atuação privada livre de direitos fundamentais no ambiente virtual, haja vista o perigo de atores fortes se sobressaírem. Nessa linha, as restrições a direitos fundamentais, nesses casos, devem ocorrer com um controle rigoroso, inclusive preventivo, por parte dos órgãos estatais (SARLET, 2021).

nega que, em certos casos, a proteção de dados pode ser vista como uma evolução do direito à privacidade. Todavia, desde já se esclareça que não se pretende nesta pesquisa tratar a privacidade e a proteção de dados como direitos sobrepostos.

Depreende-se que a privacidade indica uma visão negativa e estática. Por outro lado, a proteção de dados se refere a uma visão positiva e dinâmica, ou seja, o poder conferido ao titular do dado pessoal de controlar a coleta e o processamento dos seus dados[53]. O bem jurídico tutelado na privacidade se relaciona mais ao sigilo e à informação, ao passo que a proteção de dados seria mais abrangente e abarcaria, além do sigilo, a informação, a circulação e o controle[54] (SARLET, 2021).

Seguindo essa vertente de pensamento, o direito à proteção dos dados pessoais pode ser analisado tanto sob o prisma do sigilo dos dados como do controle sobre eles, o que não necessariamente ocorre com o direito à privacidade, puro e simples. Ou seja, a proteção de dados garante, pelo menos, duas dimensões de proteção, de tal forma que seja garantido o desenvolvimento livre da personalidade contra intervenções indevidas em ambos os casos.

Na perspectiva do sigilo dos dados, observa-se que esse direito se mostra como uma garantia, haja vista que preserva direitos como à privacidade e à liberdade (decidir se os dados serão revelados ou não). Já do ponto de vista do controle, percebe-se um direito subjetivo (informação prévia e completa do procedimento a ser realizado[55]).

Diante disso, essa dupla dimensão tutela os direitos dos indivíduos tanto em uma dimensão negativa (abstenção de interferências indevidas) como em uma positiva (proteção contra essas interferências de terceiros)[56]. Seguindo essa linha, tanto o setor público como o privado precisam observar o sigilo e a segurança dos dados[57] (MELGARÉ, 2021).

Nessa perspectiva, por mais que usado para dar respostas efetivas aos problemas das novas tecnologias, nota-se que o direito à privacidade esbarra em seu caráter individualista e

---

[53] Em tais casos, "[...] o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade" (BIONI, 2021, p. 96).

[54] Importante destacar que existe posicionamento doutrinário contrário à divisão entre privacidade, proteção de dados e outros direitos da personalidade correlatos, tendo em vista que bastaria a utilização dos instrumentos jurídicos já existentes para realizar a proteção devida. Isso muito se deve a lógica de que a automatização da informação pessoal possibilitou a revelação de informações do indivíduo através do cruzamento de dados, independentemente se os dados utilizados são íntimos ou não (RUARO; RODRIGUEZ, 2010).

[55] Isso inclui, além do discernimento, a consciência das vantagens e dos riscos envolvidos (REIS; NAVES, 2020).

[56] Essas dimensões são alocadas levando em consideração a separação ainda existente em relação a direitos de primeira e segunda geração. Nesse sentido, a privacidade ficaria mais próxima de um direito fundamental de primeira geração (deveres de abstenção), ao passo que a proteção de dados agregaria aspectos tanto de primeira como de segunda geração (deveres prestativos).

[57] Isto é, aqueles que manipulam dados pessoais têm deveres negativos (não difusão indevida dos dados) e deveres positivos (ações de segurança para o tratamento dos dados e divulgação de informações aos usuários sobre o uso dos dados coletados) (MELGARÉ, 2021).

subjetivo. Ou seja, o direito à privacidade dialoga mais no plano axiológico com a proteção de dados do que no plano da dinâmica e do desenvolvimento[58] (DONEDA, 2021).

Ademais, a bem da verdade, destaque-se que a privacidade, dentro da sua perspectiva plural já abordada, é acionada quando a proteção de dados não se mostra suficiente no caso concreto. Por exemplo, quanto ao sujeito ativo do direito fundamental à proteção de dados, entende-se que, à priori, estariam abrangidos apenas as pessoas naturais, identificadas e identificáveis. Partindo desse pressuposto, os dados das pessoas jurídicas poderiam ser devassados?

Aqui há uma divergência teórica sobre qual direito aplicar às pessoas jurídicas[59], mas o fato é que esses entes jurídicos não podem ficar desamparados. Desse modo, atribui-se às pessoas jurídicas o direito à privacidade, o qual seria exteriorizado pelo caráter instrumental da proteção de dados, ainda que a LGPD só se aplique a pessoas naturais, de modo que os dados das pessoas jurídicas ficam resguardados em função da efetividade do direito à privacidade (SARLET, 2021).

Desse modo, os novos problemas oriundos da captação massiva de dados pessoais demandam a formulação de novas soluções jurídicas que vão além das existentes. Partindo disso, nota-se que, enquanto a tutela da privacidade é negativa, a proteção de dados requer tanto comportamentos negativos como positivos. Nesse sentido, mostra-se relevante que se reconheça a existência de um direito autônomo à proteção de dados.

Internacionalmente, o direito à proteção de dados pessoais ganhou autonomia com a Carta de Direitos Fundamentais da União Europeia (doravante CDFUE), limitado aos integrantes da União Europeia. Por sua vez, esse direito foi previsto expressamente na Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (1981), também conhecida como Convenção de Estrasburgo. Todavia, já era possível deduzir essa proteção do art. XII[60] da Declaração Universal dos Direitos Humanos (1948) e do art. 8º[61] da Convenção Europeia dos Direitos do Homem (1950) (SARLET, 2021).

Contudo, essa gama de dispositivos internacionais não garante que esse direito seja incorporado formalmente aos ordenamentos jurídicos nacionais. Há Estados que não reconhecem o direito à proteção de dados de maneira expressa nas suas Constituições, como

---

[58] Por exemplo, depreende-se que a proteção de dados não está ligada à diferença entre público e privado, como o direito à privacidade pode fazê-lo. Tal distinção é irrelevante para a tutela dos dados (MELGARÉ, 2021).

[59] Divergência menor existe em relação ao direito à autodeterminação informativa, o qual é atribuído, em algumas ordens jurídicas, como a alemã, tanto as pessoas naturais como jurídicas (SARLET, 2021).

[60] O dispositivo assegura a inviolabilidade da privacidade e garante a proteção legal em caso de interferências ou de ataques.

[61] Depreende-se que essa norma afiança o respeito à vida privada do indivíduo.

ocorre, por exemplo, na Alemanha. No entanto, esse direito pode ser reconhecido, em muitos casos, como positivado implicitamente e ligado ao direito à autodeterminação informativa.

A relação entre ordem jurídica nacional e internacional é particularmente complexa e dinâmica em relação à proteção de dados, tendo em vista que ela se conecta com várias áreas do saber, a exemplo dos direitos humanos e sociais. Desse modo, agregam-se em torno da temática elementos econômicos, financeiros, comerciais, políticos, sociais, entre outros (SARLET, 2021).

Nesse sentido, para a solução de problemas concretos envolvendo a temática, mostra-se oportuno que sejam adotados parâmetros substancialmente comuns (respeitadas as peculiaridades), tanto normativos como dogmáticos. Aqui ganha relevância a ideia de proteção de dados multinível, uma vez que são tratados problemas e desafios comuns, "[...] como é o caso da proteção da privacidade, dos direitos do consumidor, da responsabilização por violações dos dados pessoais, entre outros [...]" (SARLET, 2021, p. 44).

No Brasil, depreende-se que a Constituição de 1988 não previu de imediato o direito à proteção de dados pessoais, mesmo que tenha previsto a ação de *habeas data* (art. 5º, LXXII); os direitos à vida privada e intimidade (art. 5º, X); bem como o segredo das comunicações telefônicas, telegráficas e de dados (art. 5º, XII) (DONEDA, 2021).

Pela interpretação em conjunto dessas normas, observa-se que já era possível extrair, ainda que implicitamente, a proteção de dados do sistema jurídico brasileiro. Em relação ao *habeas data*, percebe-se que ele já se relacionava com a tutela dos dados dos indivíduos, de tal modo que pode ser apontado como um ponto de partida, pelo viés constitucional, para o reconhecimento da importância da proteção de dados no Brasil.

Isso muito se deve ao fato desse remédio constitucional proteger o direito do cidadão de acessar e retificar os dados pessoais que se encontram em bancos de dados, sejam públicos, sejam de caráter público. Todavia, essa ação não é dotada de instrumentos ágeis e eficazes capazes de tutelar o direito fundamental à proteção de dados, haja vista os requisitos exigidos para o seu manejo, dentre os quais a presença de advogado e a necessidade de demonstração da recusa administrativa de cumprir o que foi postulado (DONEDA, 2011).

Em sentido contrário, há quem defenda que a proteção presente no texto constitucional se limitou à comunicação das informações pessoais, consoante uma das formas de interpretar o art. 5º, inciso XII, da Constituição Federal de 1988. Ou seja, protege-se apenas o fluxo informacional e não as informações em si.

Inclusive, seguindo esse entendimento, o STF já reconheceu, em tempos passados, que não existiria a inviolabilidade dos dados armazenados em computadores, haja vista que esses dados não estariam inseridos no contexto de uma "comunicação". Esse tipo de posicionamento demonstra a "[...] dificuldade em tratar do tema da informação pessoal de forma diversa daquela binária – sigilo/abertura, público/privado – de forma que reflita a complexidade da matéria da informação" (DONEDA, 2011, p. 105-106).

A presença dessa linha de pensamento mais conservadora ainda na realidade brasileira deve-se, em grande medida, ao fato de que a pessoa foi negligenciada em detrimento do patrimônio por muito tempo no sistema jurídico brasileiro, até meados da metade do século XX. Nesse sentido, o direito privado passou por um movimento de humanização, o qual culminou com a previsão expressa de direitos da personalidade no Código Civil de 2002, dentre os quais o direito ao nome, à imagem, à liberdade, à honra, e à integridade física[62] (BIONI, 2021).

Estruturar e pensar o direito pátrio dessa forma confirma a busca por um direito privado focado na proteção da pessoa humana, ou seja, um direito civil despatrimonializado e repersonalizado. Esse novo direito civil coloca o ser humano em posição de destaque, o que reflete na interpretação das normas jurídicas, as quais devem ser lidas privilegiando o regime protetivo mais benéfico e não apenas apegado a dogmas do passado.

Nesse sentido, é imperiosa a superação desse antigo paradigma, tendo em vista a elevação da dignidade da pessoa humana como um fundamento da República na Constituição de 1988. Ademais, o texto constitucional estipulou um sistema de direitos e garantias que abrangiam, além das normas presentes no texto constitucional, as normas internacionais que versavam sobre direitos e garantias fundamentais[63] (LEONARDI, 2012).

Partindo disso, nota-se que os direitos de personalidade, na atualidade, integram um sistema geral de tutela à pessoa humana, o qual dispõe de certa elasticidade. Ora, esses direitos fundamentais não se limitam àqueles previstos no Código Civil[64], de modo que não

---

[62] Diante disso, não é por acaso que a personalidade é tratada entre um dos capítulos inaugurais do atual Código Civil, bem como a dignidade da pessoa humana, fundamento da República, abre o texto constitucional com a sua previsão expressa no art. 1º, inciso III (BIONI, 2021).

[63] Em relação a temas correlatos à privacidade, isso se mostra relevante, uma vez que ela "[...] é reconhecida como um direito fundamental em praticamente todos os tratados e convenções internacionais de direitos humanos ratificados pelo Brasil" (LEONARDI, 2012, p. 95).

[64] Destaque-se que várias leis já versam sobre temas ligados à proteção de dados, entre as quais merecem realce "[...] a Lei de Acesso à Informação (Lei 12.527/2011) e o assim chamado Marco Civil da Internet (Lei 12.965/2014) e o respectivo Decreto que o regulamentou (Decreto 8.771/2016), mas especialmente a Lei Geral de Proteção de Dados (Lei 13.709/2018)" (SARLET, 2021, p. 57).

existe óbice para o reconhecimento da proteção de dados como um novo direito da personalidade[65] (BIONI, 2021).

Desse modo, necessita-se de uma visão sistêmica do diálogo entre a proteção de dados e as demais normas que tangenciam a temática para a compreensão, interpretação e aplicação constitucionalmente adequadas desse novo direito. Inclusive, isso pode auxiliar na demarcação de limites direitos e indiretos dentro do seu âmbito de aplicação.

Nesses termos, não existiria óbice para um dado adjetivado como pessoal ser inserido no rol dos direitos da personalidade, uma vez que caracteriza uma projeção, extensão ou dimensão do titular. Essa capitulação jurídica é relevante para proteger a identidade das pessoas na atualidade, em que a sociedade e a economia, como já mencionado, orientam-se por esses dados identificadores. Assim, também é preciso que sejam criadas formas de defesa contra essa realidade[66].

Deve-se superar, pois, a dicotomia entre público e privado e entender a proteção de dados como uma projeção da esfera relacional do sujeito e um novo direito da personalidade. Com isso, supre-se a necessidade dogmática de criar coerência normativa as faculdades jurídicas inerentes a esse direito (direito de acesso, correção, revisão de decisões automatizadas, dentre outros), o que também permite uma melhor interpretação e aplicação dos seus conceitos basilares (BIONI, 2021).

Diante disso, o que prevalece não é que esse direito à proteção de dados pessoais decorreria tão somente do direito à privacidade. Percebe-se que o direito fundamental à privacidade se relaciona mais ao controle das informações íntimas ou privadas do sujeito. Todavia, nem todas as informações estão compreendidas nessa esfera privada, há casos em que a informação se encontra na esfera pública e se discute, por exemplo, apenas a exatidão desses dados, o que decorre da identidade do indivíduo e não propriamente da privacidade[67].

Nessa perspectiva, a esfera privada não estaria posta à espera de violação, mas ela seria construída dinamicamente com o controle das informações pessoais. Ou seja, a mudança seria de ordem qualitativa "[...] representada pela transposição do eixo antes focado no

---

[65] A personalidade é marcada por aquelas características que distinguem uma pessoa da outra, sejam através de caracteres corpóreos, sejam através de caracteres incorpóreos, as quais conformam a projeção da pessoa humana. Por essa concepção, podem servir como exemplos de prolongamentos da personalidade o nome, a honra e a integridade física ou psíquica (BIONI, 2021).

[66] Essa forma de pensar, de certa forma, justifica dogmaticamente a inclusão dos dados pessoais na categoria dos direitos da personalidade, tendo em vista que é aceitável que uma pessoa pleitei a correção dos seus dados pessoais quando não representam precisamente a projeção da sua personalidade (BIONI, 2021).

[67] Para entender o direito à proteção de dados pessoais como uma "evolução" do direito à privacidade, mostra-se necessário que o direito à privacidade seja entendido como uma proteção dinâmica e uma liberdade positiva do controle sobre as informações pessoais (BIONI, 2021).

trinômio ‘pessoa-informação-sigilo’ ao eixo agora composto por quatro elementos – ‘pessoa-informação-circulação-controle’[68]” (BIONI, 2021, p. 93).

Isso corrobora a ideia de que o direito à proteção dos dados pessoais deve ser compreendido como uma nova espécie de direito da personalidade, haja vista a necessidade de maior elasticidade para a cláusula geral de proteção da pessoa humana. Em sentido contrário, esse direito pode continuar vinculado à perspectiva conceitual e à "[...] dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana” (BIONI, 2021, p. 96).

Ora, a Sociedade da Informação cria uma nova realidade social e novos desafios para tutela da proteção humana, como com a monetização dos dados pessoais. Estes dados se revelam como prolongamento da pessoa e interferem na esfera relacional do sujeito, de modo se mostra necessária uma normatização autônoma e específica.

Ademais, é válido destacar a decisão da Corte Constitucional alemã sobre a Lei do Censo de 1983 como marco inicial da percepção da proteção de dados pessoais como um direito de personalidade autônomo, além da compreensão da autodeterminação informacional para além do consentimento do indivíduo.

Nessa oportunidade, entendeu o Tribunal Constitucional alemão que a autodeterminação informacional está interligada com o direito geral de personalidade, na medida que é garantido ao indivíduo a proteção contra a manipulação irrestrita de seus dados pessoais, de modo que a autodeterminação informacional apenas pode ser afastada em casos excepcionais[69] (MARTINS, 2005).

No Brasil, cabe destacar a decisão liminar de relatoria da Ministra Rosa Weber, em 24 de abril de 2020, a qual suspendeu a eficácia da Medida Provisória (MP) de número 954/2020. Essa MP possibilitava ao Instituto Brasileiro de Geografia e Estatística (IBGE) o acesso aos dados dos clientes de operadores de telecomunicações em determinados casos[70].

Nota-se que os argumentos suscitados pelos legitimados do controle direto de constitucionalidade giravam em torno da falta dos requisitos constitucionais formais exigidos

---

[68] Ou seja, é necessário que a visão tradicional de privacidade conviva com essa nova dimensão, de modo que “[...] deveria haver um intercâmbio entre as tutelas estática e dinâmica do direito à privacidade, o que, no entanto, não significa que o direito à proteção dos dados pessoais deveria ser reduzido a uma mera evolução do direito à privacidade” (BIONI, 2021, p. 93).

[69] Vislumbra-se que a fundamentação não partiu da premissa de que a proteção dos dados pessoais é uma evolução do direito à privacidade, mas o tratou como um direito de personalidade autônomo que reclama uma técnica de proteção própria (MARTINS, 2005).

[70] Nesse sentido, suspendeu-se a eficácia do artigo segundo, *caput*, da referida MP, o qual previa que as empresas de telecomunicações deveriam repassar ao IBGE dados relacionados ao nome, número de telefone e endereço de seus consumidores (BRASIL, 2020).

pela Constituição (art. 62, *caput*), bem como a violação a alguns direitos fundamentais, dentre os quais a dignidade da pessoa humana e a inviolabilidade da intimidade e da vida privada. Por fim, também se ventilou a violação à autodeterminação informativa e à proteção de dados (BRASIL, 2020).

Além disso, percebia-se que o comando normativo era muito genérico e vago, além do que era desproporcional a requisição da totalidade de dados pessoais dos clientes das operadoras, haja vista que a pesquisa era realizada por amostragem (posição sustentada pelo STF). Soma-se a isso a ausência de regulação de mecanismos de proteção desses dados em casos de vazamentos ou usos indevidos (BRASIL, 2020).

Desse modo, a interpretação constitucional dada, aparentemente, foi de que merecem proteção constitucional todos os dados que podem levar à identificação do indivíduo, os quais interessam ao mercado e ao Estado. Diante disso, não existiria restrição protetiva apenas a esfera privada do sujeito, mas também a outros casos que envolvam a coleta, o processamento ou a transmissão de dados pessoais (MENDES; RODRIGUES JÚNIOR, 2021).

Aliás, várias passagens do julgamento denotam a ampliação da proteção aos dados pessoais para além daqueles tidos como sensíveis ou íntimos. Por exemplo, a Ministra Cármen Lúcia entendeu que dados como nome, endereço e número de telefone não seriam neutros e nem públicos, de modo que demandam proteção jurídica, ao passo que não existem dados insignificantes[71] (BRASIL, 2020).

Tal decisão foi importante por representar uma possível mudança na visão defendida pelo STF de considerar que a Constituição tutelaria apenas dados sigilosos e sua confidencialidade, conforme pontuado anteriormente. Pensar dessa forma é importante para afastar sobreposições entre a proteção de dados e o direito à privacidade[72].

Com a mudança de paradigma, a Constituição não protegeria apenas os dados sigilosos, como prevê o art. 5º, inciso XII, mas todos os dados que representem um atributo da personalidade humana. Diante dessa evolução, fica muito evidente que ocorreu a passagem, "[...] a partir da construção do conceito de autodeterminação informativa, do direito à

---

[71] Nesse mesmo tom, o Ministro Luiz Fux ressaltou o tema da proteção de dados como importante para a manutenção da democracia, uma vez que dados tidos como insignificantes podem ser utilizados para corromper processos eleitorais, como já mencionado (BRASIL, 2020).

[72] Para o Ministro Gilmar Mendes, a proteção de dados seria mais ampla do que o direito à privacidade por não se limitar a dados íntimos ou privados. Esse direito fundamental autônomo recairia sobre todos os dados que possam identificar o indivíduo (BRASIL, 2020).

privacidade, liberdade negativa, para um direito à proteção de dados, liberdade positiva e projeção da personalidade, a ser protegida e promovida pelo Estado"[73] (BIONI, 2021, p. 104).

Por mais que a liminar não tenha os mesmos efeitos de uma decisão de mérito[74], cabe frisar que essa decisão foi emblemática na temática da proteção de dados, haja vista que ficou reconhecida, de maneira expressa, a autonomia do direito fundamental à proteção de dados. Esse reconhecimento é relevante para os setores da economia, para os sujeitos e para o próprio Estado, uma vez que é preciso que exista segurança jurídica no tratamento de dados.

Desse modo, o direito à proteção de dados deve ser abordado como um direito com características próprias que podem ou não se relacionar com o direito à privacidade. Partindo disso, mostra-se relevante entender o que significa dizer que esse direito à proteção de dados se revela um verdadeiro direito fundamental.

Isso se revela vital diante do desenvolvimento de novas tecnologias de informação e comunicação que desafiam a efetividade dos direitos, principalmente, quando se aplicam os mecanismos tradicionais de efetivação (sanções, processo judicial, eficácia das decisões, dentre outras coisas) (SARLET, 2021).

Nesse contexto, coloca-se em risco vários pontos que tangenciam a dignidade da pessoa humana, a qual se relaciona cada vez mais com o direito fundamental à proteção dos dados pessoais. Entre esses pontos estão a autodeterminação e os direitos de personalidade, os quais se desdobram no direito de livre desenvolvimento da personalidade (natureza geral) e os direitos especiais à privacidade e à autodeterminação informativa (SARLET, 2021).

Desse modo, no Brasil, ganha relevo a PEC 17/2019 que previu a inserção do direito fundamental à proteção de dados pessoais no rol de direitos e garantias fundamentais contidos no art. 5° da Constituição Federal, especificamente no inciso LXXIX. Além disso, estipulou-se a competência exclusiva da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais (art. 21, inciso XXVI), bem como para legislar sobre a matéria (art. 22, inciso XXX) (BRASIL, 2021).

Depreende-se, segundo parecer de relatoria da Senadora Simone Tebet (BRASIL, 2021), que essas mudanças recepcionam, em âmbito constitucional, os princípios já dispostos

---

[73] Esse julgado também foi importante por delimitar, à luz dos contornos trazidos pela noção de proporcionalidade, alguns parâmetros para legitimar a interferência na esfera pessoal da vida de um indivíduo, como: "[...] a) a finalidade do tratamento deve ser clara e legítima; b) a quantidade de dados coletada é limitada ao estritamente necessário em relação às finalidades para as quais o tratamento é feito; c) medidas de segurança da informação são adotadas para evitar acessos indevidos por terceiros" (BIONI, 2021, p. 105).

[74] A Medida Cautelar deferida pela Ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade (ADIs) números 6.387, 6.388, 6.389, 6.390 e 6.393, foi referendada pelo voto favorável de 10 ministros no plenário da Suprema Corte (MENDES; RODRIGUES JÚNIOR, 2021).

na Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), como o respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem do indivíduo, os quais podem ser extraídos do art. 2º da LGPD.

Por sua vez, a atribuição das competências de organizar e fiscalizar o tratamento e a proteção dos dados a União possibilita o reconhecimento constitucional das funções exercidas pela Autoridade Nacional de Proteção de Dados (ANPD), prevista no art. 55-A da LGPD, "[...] a quem o legislador ordinário delegou poder normativo, fiscalizatório, sancionatório e mediador de conflitos [...]"[75] (BRASIL, 2021).

Diante disso, essa nova competência material exclusiva da União, exercida através da ANPD, "[...] será decisiva para a harmonização regulatória e fiscalizatória da matéria, com ganhos de segurança jurídica não apenas ao titular dos dados pessoais, mas também aos agentes, públicos e privados, responsáveis pelo seu tratamento" (BRASIL, 2021).

Ademais, a PEC, ao reservar a competência legislativa apenas para a União sobre a temática de proteção e tratamento de dados pessoais, busca assegurar a coesão normativa sobre a matéria em nível nacional, o que já se infere do art. 1º da LGPD, o qual dispõe que suas normas devem ser observadas por todos os entes federados (BRASIL, 2021).

Ressalte-se que a PEC, a bem da verdade, apenas assegura expressamente o direito fundamental à proteção de dados no texto constitucional, tendo em vista que esse direito já era reconhecido pelo Supremo Tribunal Federal (STF), como se observa nas Ações Diretas de Inconstitucionalidade (ADIs) de números 6387, 6388, 6389, 6393 e 6390[76] (BRASIL, 2021).

Nessa perspectiva, a partir da promulgação da Emenda Constitucional 115, fruto da aprovação da já abordada PEC 17/2019, percebe-se que o direito à proteção de dados passa a ser, expressamente, previsto no texto constitucional. Ou seja, esse direito, agora, indiscutivelmente, assume a roupagem de um direito fundamental tanto no aspecto material como no aspecto formal.

Pelo aspecto material, depreende-se que esse direito apresenta grande relevância individual e social (tanto para a sociedade civil como para o Estado), haja vista que instrumentaliza direitos como a dignidade humana, o livre desenvolvimento da personalidade e o direito à privacidade (SARLET, 2021).

---

[75] Inclusive, vislumbra-se que a ANPD é incumbida de zelar, justamente, pela proteção dos dados pessoais, o que demonstra a necessidade de uma competência material organizacional centrada na figura da União (BRASIL, 2021).

[76] Destaque-se que não existe incoerência no fato de o STF reconhecer direitos que não estão expressos no texto constitucional, mas que são decorrência lógica dele. Ora, não existe menção expressa à palavra "privacidade" no texto constitucional, mas isso nunca impediu a Suprema Corte de aplicar esse direito fundamental, o que não poderia ser diferente.

Já pelo ponto de vista formal, observa-se que esse direito apresenta a mesma hierarquia normativa em relação aos demais direitos fundamentais, de modo que ele pode ser utilizado como "[...] parâmetro para o controle da legitimidade constitucional dos atos normativos infraconstitucionais e de atos (e omissões) do poder público em geral, ademais de sua projeção na esfera das relações privadas [...]" (SARLET, 2021, p. 47).

Aliás, a inserção expressa desse direito fundamental na Constituição acarreta uma série de consequências jurídicas. Entre elas, fica clara a condição de direito fundamental autônomo, com campo de aplicação próprio. Além disso, aplica-se a esse direito todo o regime jurídico-constitucional relativo aos direitos fundamentais em sentido material e formal reconhecidos pela Constituição, doutrina e jurisprudência[77].

Partindo disso, é importante frisar que esse direito fundamental apresenta como titular a pessoa a quem pertencem os dados e suporta os riscos do uso indevido e não os dados em si, exclusivamente. Deve-se ter em mente que esse direito fundamental foi reconhecido para proteger, dentre outras coisas, os direitos do titular dos dados (MENDES; RODRIGUES JÚNIOR, 2021).

Por sua vez, nota-se que os destinatários do direito, ou seja, aqueles que são vinculados pelo direito, são o Estado e os particulares, dado que não é lícito a nenhum dos dois devassar indevidamente, seja por ação, seja por omissão, os dados pessoais de alguém, o que fere os seus direitos de personalidade (SARLET, 2021).

Quanto aos efeitos desse direito, já levando em consideração a autodeterminação informativa, eles abrangem tanto uma dimensão subjetiva[78] (liberdade negativa diante dos destinatários), como uma dimensão objetiva (dever de atuação positiva dos destinatários para garantir o exercício do direito) (MENDES; RODRIGUES JÚNIOR, 2021)

Desse modo, pelo viés subjetivo, o titular dos dados apresenta uma série de prerrogativas e os destinatários uma gama de deveres. Por exemplo, o titular do direito pode ter acesso aos dados pessoais existentes em bancos de dados públicos ou privados, bem como identificar as pessoas responsáveis pela coleta, armazenamento e tratamento dos dados[79].

---

[77] Percebe-se que esse regime jurídico-constitucional garante: a supremacia material e formal desse direito no ordenamento jurídico; a inclusão dele entre os limites materiais à reforma constitucional (cláusulas pétreas); e a proteção de dados como um direito dotada de aplicabilidade imediata (direta) que vincula os atores públicos e os atores privados (no que couber) (SARLET, 2021).

[78] Nota-se que o reconhecimento do direito fundamental enquanto direito subjetivo abarca, fora a exigibilidade, "[...] uma relação trilateral entre o titular (ou sujeito ativo), o objeto e o destinatário (sujeito passivo) do direito – posição(ções) jurídica(s) – atribuída pelo direito objetivo" (SARLET, 2021, p. 66).

[79] Ainda existe a possibilidade do indivíduo proibir a utilização ou difusão dos seus dados pessoais pelo Estado ou por terceiros, o que abarca o direito de sigilo desses dados pessoais. Além disso, o titular dos dados também

Já do ponto de vista objetivo, percebe-se que o reconhecimento de um direito fundamental apresenta o condão de irradiar seus efeitos por todo o ordenamento jurídico[80]. Também é importante destacar que um direito fundamental cria para o Estado o dever geral de efetivação desse direito, haja vista que o ente estatal deve assegurar a proteção do direito fundamental, inclusive preventivamente, contra violações de particulares, de outros Estados e dos próprios poderes públicos (SARLET, 2021).

Para tanto, mostra-se necessária a criação e constituição tanto de instituições estatais voltadas para a proteção do direito fundamental, como de procedimentos próprios que englobem as especificidades em torno daquele direito. Em caso contrário, pode-se ter o reconhecimento do direito, mas sem a estrutura necessária para efetivá-lo.

Diante disso, o Estado pode efetivar seus deveres protetivos de várias formas, desde a responsabilização civil ou criminal, até a criação de mecanismos processuais (como o *habeas data*) e de órgãos designados para realizar a proteção de dados, a exemplo da Autoridade Nacional de Proteção de Dados (ANPD) no Brasil (SARLET, 2021).

Levando em consideração todos esses pontos colocados, ainda é importante ter em mente que a proteção de dados, bem como os demais direitos fundamentais, não é um direito absoluto. As informações pessoais obtidas pelo processamento ou exposição dos dados também repercutem na órbita social, ainda que de titularidade individual, de modo que podem sofrer limitações pela lei ou pela Constituição.

Todavia, a limitação desse direito fundamental deve ser baseada em alguns critérios, sob pena da ilegalidade da restrição[81]. Nesse sentido, no caso concreto, nota-se que a limitação deve ser: com fundamento jurídico seguro; clareza da finalidade; proporcionalidade, adequação e necessidade; mecanismos mínimos de segurança dos envolvidos e diminuição de riscos de violação aos direitos da personalidade[82] (MENDES; RODRIGUES JÚNIOR, 2021).

Depreende-se que quanto mais sensível for o dado pessoal, mais rigorosas devem ser as exigências de intervenções e mais intenso os mecanismos de controle, haja vista esses

---

dispõe da prerrogativa de ser informado da finalidade da coleta e da utilização dos seus dados, bem como do poder de ratificar ou excluir os dados pessoais armazenados nos bancos de dados (SARLET, 2021).

[80] Associado a esse efeito, vislumbra-se a constitucionalização do Direito, inclusive o privado, tendo em vista a aplicação dos direitos fundamentais nas relações privadas (eficácia horizontal ou em relação a terceiros) (SARLET, 2021).

[81] Essas relativizações não podem prejudicar a efetiva proteção jurídica da proteção de dados pessoais na Internet, o que perpassa pelo direito de navegar na Internet sem deixar rastros de modo geral; de ter ciência de quem é o responsável do monitoramento; de deletar ou retificar dados pessoais; e de proteger a sua identidade online (BERNAL, 2014).

[82] Fica claro que "[...] toda e qualquer captação (levantamento), armazenamento, utilização e transmissão de dados pessoais, em princípio, constitui uma intervenção no âmbito de proteção do direito, que, portanto, como já adiantado, não prescinde de adequada justificação" (SARLET, 2021, p. 72).

dados estarem ligados à dignidade do titular[83]. Ou seja, por ser um direito fundamental, a proteção de dados não admite intervenções infundadas ou pautadas em justificativas que não condizem com a relevância que esse direito assume na atualidade.

Portanto, reconhecer o direito à proteção de dados como um direito fundamental autônomo da privacidade é de suma importância para que se possa tutelar adequadamente os direitos dos titulares dos dados diante dos novos desafios colocados pelas várias formas de exploração dos dados na sociedade atual. Partindo disso, mostra-se prudente entender o contexto em que esse novo direito fundamental se insere e os tipos de dados que merecem proteção jurídica, haja vista que alguns diplomas legislativos infraconstitucionais já abordam a temática da proteção de dados, como será visto a seguir.

[83] Em síntese, "[...] quanto mais grave for essa restrição, mais contundentes devem ser as justificativas, os critérios e as precauções para tal fim, sob pena de se legitimar intervenções na vida privada em nome de fins genéricos ou necessidades coletivas abstratas" (MENDES; RODRIGUES JÚNIOR, 2021, p. 86).

3. MICROSSISTEMA DE PROTEÇÃO DE DADOS NO BRASIL: A IMPORTÂNCIA DOS DADOS E DOS METADADOS NA ATUALIDADE

A proteção de dados ganhou destaque nos últimos anos, não apenas no Brasil, mas no mundo de maneira geral. Isso se deve, dentre outras coisas, ao uso crescente dos dados digitais para as mais diversas finalidades (lícitas ou não), como abordado no primeiro capítulo. Todavia, percebe-se que o debate em torno da tutela dos dados pessoais remonta desde o século passado.

Ainda em meados de 1970, notabilizaram-se as primeiras leis que buscavam normatizar o uso dos dados, como a Lei do Land alemão de Hesse (1970); o Estatuto para bancos de dados da Suécia (1973); e o *Privacy Act* norte-americano (1974). Esses diplomas normativos ficaram conhecidos como leis de "primeira geração", dada a preocupação com os grandes centros de tratamento de dados que atuavam de maneira centralizada, em grande medida sob responsabilidade estatal (DONEDA, 2020).

A primeira geração de leis pecou pelos seus princípios muito abstratos e amplos, os quais eram, muitas vezes, focados apenas na atividade de processamento. Já a "segunda geração", inaugurada a partir da segunda metade da década de 70, baseava-se na noção de privacidade e proteção de dados pessoais como liberdades negativas exercidas pelo próprio cidadão. Vislumbra-se que a primeira lei a aderir essa percepção foi a lei francesa de proteção de dados pessoais de 1978 (*Informatique et Libertés*) (DONEDA, 2020).

Contudo, fugiu a essa segunda geração a compreensão de que os problemas em torno da proteção de dados pessoais não seriam resolvidos pura e simplesmente por um viés individualista. Ora, desde aquela época, observava-se que o fornecimento de dados pessoais pelos cidadãos, seja para entes estatais, seja para entes privados, tinha se tornado primordial para a vida social do indivíduo, tendo em vista que o rompimento do fluxo informacional poderia levar, não raras vezes, à exclusão social.

Partindo disso, surgem as leis da "terceira geração", as quais buscavam empoderar o cidadão sobre o efetivo controle dos seus dados, de modo que sua liberdade de escolha fosse livre de vícios. Por fim, as leis de "quarta geração", como as adotadas na atualidade em vários países, instrumentalizam a tutela do direito à proteção de dados por intermédio de mecanismos coletivos voltados para resultados concretos[84] (DONEDA, 2020).

---

[84] Ressalte-se que não será abordada cada geração com minúcia, haja vista essa não ser a finalidade deste estudo.

Observa-se que as leis atuais de proteção de dados carregam influências dessas gerações, as quais contribuíram para demonstrar os riscos em torno do tratamento de dados; a necessidade de conhecimento de quais agentes são responsáveis pelo tratamento; e o empoderamento efetivo do indivíduo sobre o controle dos seus dados, não só do ponto de vista normativa, mas acima de tudo instrumental.

Diante desse plano de fundo, cumpre destacar que a Europa se mostrou pioneira na temática da proteção de dados. A *General Data Protection Regulation* (GPDR), ou Regulamento Geral sobre a Proteção de Dados (RGPD), foi fruto de um longo debate que perdurou até a entrada em vigor do instrumento normativo em 18 de maio de 2018.

Tal regulamento serviu como parâmetro para várias leis sobre proteção de dados, entre as quais se destacam o *California Consumer Privacy Act*, de 2018, nos Estados Unidos e a *Ley General de Protección de Datos Personales* (LGPDP), de 2017, no México. Importante frisar que a presente pesquisa não se destina a realizar um estudo comparado, de modo que tais instrumentos normativos são citados a título de exemplos (RIHL, 2020).

Já no Brasil, diferentemente do processo europeu, mas influenciado por ele, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi aprovada, em agosto de 2018, com os debates legislativos concentrados em 3 (três) meses, apenas. Nesse sentido, não se estranha que a LGPD tenha passado por uma produção legislativa tempestuosa, no mínimo. Em síntese: promulga-se a lei; veta-se a lei; emenda-se a lei (Medida Provisória de número 869/2018); altera-se a lei (Lei nº 13.853/2019). Tudo isso ao longo de dez meses, sem sequer a lei estar em vigor ainda (RIHL, 2020).

O fato é que a LGPD inaugurou um regime geral de proteção de dados no Brasil, o qual atribuiu nova roupagem à lógica por trás da proteção dos dados pessoais no país. Isso se deve ao fato da tradição jurídica brasileira ser construída sobre a premissa de que apenas mereciam proteção os dados pessoais "privados" (íntimos ou não compartilhados). Essa proteção se dava por meio do sigilo (ABREU, 2021).

Por sua vez, a nova legislação de proteção de dados assegura que todo dado pode vir a ser protegido a depender de sua vinculação ao indivíduo. Nessa linha, toda operação de tratamento deve ser alicerçada em uma das hipóteses legais (arts. 7º e 11), indistintamente, se "públicos" ou "privados".

Esse novo regime de proteção de dados é complementado por normas setoriais, como a Lei de Acesso à Informação (Lei nº 12.527/2011), o Marco Civil da Internet (Lei nº

12.965/2014) e o Código de Defesa do Consumidor (Lei nº 8.078/1990)[85]. Por exemplo, bem antes da lei de proteção de dados, o Marco Civil da Internet (MCI) já enumerava os fundamentos da proteção de dados no país em seu art. 2º (DONEDA; MENDES, 2019).

Ademais, o MCI regulamentou, de maneira inicial, o tratamento de dados pessoais (coleta, uso, armazenamento, etc.) em vários dispositivos, o que foi complementado pelo Decreto nº 8.771/2016, que regulamenta a Lei nº 12.965, especialmente no que diz respeito à transparência, à guarda e à requisição de dados.

Válido mencionar que isso ocorreu muito devido ao contexto em que o MCI foi elaborado, o qual era marcado pelas invasões de privacidade cometidas pelos Estados Unidos. Essas invasões vieram à tona pelo relato do ex-analista da Agência Nacional de Segurança dos EUA Edward Snowden[86] (LIMA; RAMIRO, 2020).

Nesse sentido, devido à pluralidade normativa, percebe-se que é necessário que haja um diálogo entre todas essas fontes normativas. Esse diálogo ocorre para trazer unicidade interpretativa ao microssistema jurídico de proteção de dados (coerência-sistemática); complementar as normas entre si (complementariedade-subsidiariedade); e possibilitar que as leis se influenciem mutuamente (coordenação-adaptação sistêmica)[87] (BIONI, 2021).

A preocupação com a efetividade normativa, tanto das lei anteriores como da LGPD, justifica-se em função de fenômenos como o da "datificação". Esse fenômeno pode ser entendido como a transformação do comportamento humano em dados. Ou seja, as interações no ambiente digital deixam um verdadeiro rastro digital, o qual pode ser utilizado para os mais diversos fins (BOTELHO; CAMARGO, 2021).

Para fazer frente a esse cenário, vislumbra-se que a LGPD é organizada em torno de cinco eixos centrais: "[...] i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes" (DONEDA; MENDES, 2019, p. 312).

---

[85] Ainda podem ser citados como exemplos: a Lei do Cadastro Positivo (Lei nº 12.414/2011), a Lei do Habeas Data (Lei nº 9.507/1997), e o Código Civil (Lei nº 10.406/2002), dentre outras (LIMA; MEDEIROS NETO, 2022).

[86] Levando isso em consideração, o art. 7°, inciso I, do MCI, assegura a "[...] inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2014).

[87] Caso isso seja feito, vislumbra-se uma maior chance de efetivação dos valores centrais elegidos pela lei, como o respeito à privacidade (art. 2º, inciso I) e a autodeterminação informativa (art. 2º, inciso II) (FERNANDES; OLIVEIRA, 2020).

Essa organização é importante para tentar abarcar os possíveis conflitos que envolvem o uso indevido dos dados no ambiente virtual, tanto os presentes como os futuros. Neste estudo, não será realizada a investigação em torno de todos os eixos da LGPD, detalhadamente, mas os principais dispositivos serão utilizados como objeto de investigação científica.

Logo, depreende-se que as complexidades em torno da temática da proteção de dados requerem que o assunto seja tratado à luz de um microssistema de proteção de dados. Para entender melhor esse microssistema, faz-se necessário que se possua uma correta compreensão sobre os tipos de dados existentes e os seus regimes jurídicos de proteção, o que será feito a seguir.

3.1 DADOS MULTIFORMES: UM VERDADEIRO DEGRADÊ JURÍDICO

Como já abordado no primeiro capítulo, percebe-se que os dados podem ser utilizados para os mais diversos fins e são coletados de várias maneiras. Diante disso, nota-se o surgimento de uma variedade de dados, os quais são analisados, em sua grande maioria, a partir das informações que eles podem revelar sobre o titular do dado.

Alguns desses dados podem estar vinculados à esfera individual da pessoa, de tal modo que sejam enquadrados como dados pessoais, os quais merecem especial atenção, haja vista a necessidade da tutela da própria pessoa e de sua dignidade (LIMA; MEDEIROS NETO, 2022).

Os dados pessoais, no Brasil, são definidos no artigo 5º, inciso I, da LGPD. Tal norma consagra como dado pessoal toda informação relacionada à pessoa natural identificada ou identificável. Inclusive, a redação corresponde ao que já era previsto na Lei de Acesso à Informação (LAI), no seu artigo 4º, inciso IV, o que reforça a tese do diálogo das fontes normativas[88] (MACHADO; DONEDA, 2018).

Partindo do pressuposto de que apenas pessoas físicas podem ser titulares de dados pessoais, nota-se que a LGDP adota o conceito idêntico ao presente no art. 4º, do Regulamento Geral de Proteção de Dados (GDPR) europeu[89]. Todavia, o GDPR vai além e define o significado de pessoa "identificável". Nesse sentido, é identificável toda pessoa física

---

[88] O Decreto nº 8.771/2016, ao regulamentar a Lei nº 12.965/2014, também definiu dados pessoais, em seu art. 14, inciso I, por intermédio dessa mesma ideia (SILVA, 2019).

[89] Percebe-se que essa ideia de dado pessoal remonta a Convenção de Strasbourg (1981), a qual define a informação pessoal em função da sua vinculação à pessoa identificada ou identificável (SILVA, 2019).

que possa ser identificada direta ou indiretamente por algum identificador (nome, número de identificação, dados de localização, identificadores eletrônicos, entre outros) (LEONARDI, 2021).

Quanto aos identificadores diretos, vislumbra-se que eles enunciam aspectos intimamente ligados ao sujeito, como o nome. Já os identificadores indiretos complementam as informações relacionadas ao indivíduo, o que se mostra muito útil, por exemplo, em casos de homonímia. São exemplos de identificadores indiretos o número do CPF, a nacionalidade, a filiação, ou até mesmo características fenotípicas (MACHADO; DONEDA, 2018).

Por sua vez, o conceito de dado pessoal adotado é lido em sentido amplo, isto é, não apenas identificadores diretos e indiretos podem ser considerados dados pessoais, tendo em vista que dados que potencialmente conduzem à individuação da pessoa também podem representar informações pessoais. Isso ocorre com aqueles dados que, caso tratados em conjunto com técnicas específicas, podem levar à identificação do titular.

Partindo disso, há, na ordem jurídica brasileira, alguns tipos de dados pessoais, entre os quais aqueles que se referem a dados cadastrais, os quais revelam aspectos como a qualificação pessoal, a filiação e o endereço, conforme o art. 10, §3º, do Marco Civil da Internet[90]. Também há menção aos registros de conexão e de acesso a aplicações de Internet. Tais registros se encaixam no conceito de dado pessoal, caso estejam atrelados a uma pessoa natural (MOURA; BARBOSA, 2020a).

No caso do registro de conexão, percebe-se que ele pode ser compreendido como, consoante o estipulado no art. 5º, inciso VI, do MCI, "[...] o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (BRASIL, 2014).

Já os registros de acesso a aplicações de Internet são definidos, no art. 5º, inciso VIII, do Marco Civil da Internet, como "[...] o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (BRASIL, 2014).

Diante disso, nota-se que os dados cadastrais dizem respeito às informações pessoais, a exemplo do nome, do endereço, dos números de documentos pessoais ou empresariais,

---

[90] Inclusive, o Decreto no 8.771/2016, em seu art. 11, dispõe sobre o acesso aos dados cadastrais, os quais dizem respeito, conforme o §2º, aos dados sobre "[...] filiação, endereço e qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário" (BRASIL, 2016).

fornecidas pelo usuário para o provedor a fim de gozar das funcionalidades oferecidas por ele, desde a instalação, o funcionamento e a cobrança dos serviços. De outra banda, os registros se relacionam aos dados de conexão que se referem às informações técnicas capazes de identificar o usuário durante o uso da rede (endereço IP, datas e horários de *login* e *logout*, nome de usuário utilizado, dentre outras.

Nessa perspectiva, percebe-se que tais dados de conexão representam metadados, os quais também são muito utilizados no ambiente virtual para os mais diversos fins. Esses metadados podem ser entendidos como a informação que, de alguma forma, influencia outra fonte de informação.

Ou seja, os metadados são os dados e registros oriundos de uma comunicação que não constituem o conteúdo propriamente dito da comunicação, dentre os quais se destacam: "[...] data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI), etc." (ABREU; ANTONIALLI, 2017, p. 17).

Desse modo, nota-se que esses dados são muito úteis para traçar perfis de consumo dos usuários com a utilização dos chamados *Cookies*. A bem da verdade, a análise estatística do comportamento virtual das pessoas permite influenciar os próprios hábitos dos indivíduos, tendo em vista o acesso a informações que dizem respeito ao horário de acesso, às páginas mais acessadas, aos serviços utilizados, entre outras (MACHADO, 2018).

Fica clara, ainda, a relevância dos metadados quando se analisa o contexto de uma comunicação, como a que ocorre por carta. A mensagem veiculada na carta seria a informação principal e todas as informações acessórias (dados do remetente e destinatário, a data e o local de postagem, etc.) seriam metadados. Interessante notar que os metadados não são novidades da nova era digital, uma vez que eles já eram utilizados em algumas atividades, a exemplo das fichas catalográficas dos livros em uma biblioteca (MENEZES NETO; MORAIS; BEZERRA, 2017).

Esses tipos de dados, como os demais de maneira geral, não podem ser ignorados na atualidade. Por mais que o "dado", isoladamente, represente um estado primitivo e fragmentado da informação, ele possui o potencial de se tornar uma informação mais complexa quando explorado em conjunto[91]. Ou seja, ele seria uma espécie de "pré-informação", uma informação em potencial. Já a informação propriamente dita advém, justamente, do processo de interpretação desses dados (DONEDA, 2020).

[91] Nesse sentido, dados que, à priori, parecem inofensivos podem ser transferidos, cruzados ou organizados, de tal modo que sejam descobertas informações muito específicas de determinada pessoa (VIOLA; TEFFÉ, 2021).

Ou seja, o cruzamento desses dados e registros pode revelar informações íntimas sobre o indivíduo, por exemplo, as pessoas com quem ele se comunica. Tais dados se revelam, nesses casos, dados pessoais, os quais precisam de um regime jurídico diferenciado, haja vista que decorrem das garantias constitucionais da liberdade, da dignidade humana, bem como da intimidade e da vida privada (FRANCISCO; VENTURINI, 2019).

Todavia, essa informação também pode se referir a pessoas indeterminadas. Nesse caso, surge a figura do dado anônimo, o qual provém de uma coletividade ou de um corte específico de indivíduos que não podem ser nomeados, pelo menos não dentro de um esforço razoável de tratamento de dados.

Isto é, pode-se dizer que dado anonimizado é todo aquele que não se refere à pessoa identificada ou identificável, levando em consideração o esforço razoável na utilização de técnicas de tratamento de dados para tanto, nos termos do art. 5º, inciso III, da LGPD (MACHADO; DONEDA, 2018).

Tendo isso em mente, o conceito de dado pessoal deve ser lido em conjunto com esse conceito de dado anonimizado. Este não recebe a proteção da LGPD, haja vista o pressuposto de que esses dados anonimizados não podem revelar a identidade do seu titular (BARRIOS; SANTOS, 2021).

Ainda sobre os dados pessoais, nota-se que esses dados também podem ser enquadrados na categoria de dados sensíveis. Tal categoria de dados pessoais recebe uma proteção qualificada[92], haja vista que a circulação desregrada desses dados poderiam representar um elevado risco discriminatório para seus titulares (DONEDA, 2020).

Nessa perspectiva, a LGPD, consoante o art. 5º, inciso II, já define alguns dados que são considerados sensíveis, entre os quais se destacam aqueles que versam sobre origem racial ou étnica; convicção religiosa; opinião política; e filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além dos dados ligados à saúde, à vida sexual, a informações genéticas ou biométricas[93] (VIOLA; TEFFÉ, 2021).

---

[92] Entre os mecanismos de proteção diferenciados, nota-se a necessidade de incremento da segurança tanto dos locais físicos de produção, armazenamento, ou tratamento, como dos sistemas de informação que lidam com esses dados sensíveis (GONÇALVES; VARELLA, 2018).

[93] Percebe-se que a própria natureza das informações que podem ser extraídas desses dados justificam a proteção mais rígida, já que essas informações integram o "núcleo duro" da personalidade do indivíduo (VIOLA; TEFFÉ, 2021).

Interessante notar que a LGPD não se aplica apenas ao ambiente virtual, o que justifica essa gama variada de dados pessoais sensíveis[94]. Um exemplo interessante diz respeito aos condomínios e o controle de pessoas. Observa-se que geralmente alguns dados pessoais, até mesmo sensíveis, são requisitados pelas portarias para que se possa ingressar no ambiente interno do condomínio (DIEFENTHÄLER; MALUF, 2021).

Comumente, para o reconhecimento de visitas, são requeridos o nome, documento de identificação (RG ou CPF), contato (e-mail ou telefone), além de ser feito o registro fotográfico[95]. No documento de identificação, nota-se que também existem outros dados pessoais (DIEFENTHÄLER; MALUF, 2021).

Já para o reconhecimento dos usuários, empregados, ou moradores, as opções também abarcam a identificação por cartões magnéticos e o uso de dados biométricos[96]. Esta última hipótese inclui o reconhecimento facial e a impressão digital, os quais representam dados pessoais sensíveis e necessitam de um tratamento diferenciado (DIEFENTHÄLER; MALUF, 2021).

Outro exemplo de captação de dados fora da Internet é o da utilização de informações de chamadas e de localização de celulares, os quais não necessariamente funcionam baseados no endereço IP. Nesse contexto, mostra-se oportuno que se reconheçam esses dados telemáticos como dados pessoais, haja vista a necessidade de se garantir que cada etapa da coleta, uso, compartilhamento e processamento ocorra seguindo as normas de proteção de dados[97] (SHANAPINDA, 2019).

Tendo isso em vista, observa-se que a LGPD estabeleceu como regra geral (no art. 1º) a necessidade do tratamento dos dados pessoais ser realizado com alguma base legal que o fundamente, o que se aplica indistintamente a qualquer pessoa que trate dados, natural ou jurídica, pública ou privada.

---

[94] Destaque-se que a coleta constante de dados ocorre em outros "[...] ambientes do convívio rotineiro do indivíduo, como em condomínios (o que se tornou muito comum em tempos recentes), escolas, clubes de recreação, academias etc." (FALEIROS JÚNIOR, 2019, p. 223).

[95] Destaque-se que a imagem de alguém, por si só, configura um dado pessoal. Além disso, pela lógica da privacidade contextual, esse dado também pode se apresentar como um dado sensível. Um exemplo é a fotografia de determinado indivíduo em uma reunião partidária, o que revela sua opinião política (DIEFENTHÄLER; MALUF, 2021).

[96] Os dados biométricos estudam tanto as características físicas como as comportamentais de determinado indivíduo. No primeiro caso, insere-se o reconhecimento facial, muito utilizado para controle de acesso. Ademais, observa-se que, em geral, o sistema biométrico se revela uma forma segura de identificação, haja vista a captação das características únicas de determinado sujeito por meio de algum mecanismo de scanner que capta as imagens que posteriormente são processados com o auxílio de algum software biométrico (DIEFENTHÄLER; MALUF, 2021).

[97] Isso se mostra vital na atualidade, já que os termos de uso das operadoras telefônicas, em muitos casos, não informam os direitos dos titulares dos dados, o que impacta no fornecimento do consentimento livre, expresso e informado sobre o uso, processamento e compartilhamento dos seus dados (SHANAPINDA, 2019).

Pontue-se que essa base legal se encontra disposta no art. 7º, em relação aos dados pessoais ordinários, e no art. 11, ao se referir a dados pessoais sensíveis. Inclusive, nota-se que as bases legais do tratamento de dados pessoais ordinários e sensíveis são diferentes justamente pelo caráter mais crítico dos dados sensíveis (BUENO, 2020).

Ademais, mencione-se que essa separação entre dados pessoais e dados pessoais sensíveis não é imune a críticas. Entre as que mais se destacam, percebe-se a dificuldade de definir, à priori, quais informações seriam sensíveis ou não, uma vez que essa qualidade, na maioria dos casos, apenas se revela após o tratamento dos dados (DONEDA, 2020).

Aliás, os dados pessoais não sensíveis, a depender do tipo de tratamento realizado, podem acarretar a discriminação do titular do dado, a exemplo do que ocorre com os dados sensíveis, de modo que também precisam de um regime protetivo robusto (GUNTHER; COMAR; RODRIGUES, 2020).

Isso revela que o contexto em que os dados sensíveis são guardados e utilizados é de suma relevância, haja vista que o plano de fundo do tratamento do dado pode se revelar mais importante do que o próprio dado em si. Pode-se citar como exemplo o caso de uma lista de nomes e endereços, a qual não seria formada, à priori, por dados sensíveis, mas apenas dados pessoais. Todavia, essa lista poderia ser considerada sensível caso se referisse a pessoas proeminentes e caísse na mão de terroristas (FALEIROS JÚNIOR, 2019).

Diante disso, percebe-se que é necessário analisar o contexto informacional para definir se houve violação ou não a proteção de dados do sujeito. Essa análise pode ser feita tanto no viés interno como externo. No primeiro caso, deve-se perquirir quais informações podem ser trocadas entre emissário e receptor. Já no aspecto externo, observa-se quais são os terceiros que podem acessar o fluxo informacional[98] (BIONI, 2021).

Além disso, essa divisão realizada entre dados está cada vez mais desacreditada pelos avanços tecnológicos, haja vista que fenômenos como a datificação e o Big Data, dentre outros já mencionados nesta pesquisa, fortalecem a ideia de que até mesmo metadados, quando tratados em conjunto por técnicas específicas, podem revelar informações de foro íntimo do indivíduo.

Um caso que ilustra bem isso foi a pesquisa realizada no projeto MetaPhone, o qual monitorou os metadados das ligações telefônicas de alguns participantes, sem o acesso ao conteúdo das ligações. Ao realizar esse procedimento, os pesquisadores perceberam que

[98] Ou seja, "[...] o paciente não espera que seu médico vá trocar informações com o seu empregador (fluxo externo) e, nesse sentido, que ele deva informar seus rendimentos e atribuições profissionais para fins de atendimento médico (fluxo interno)" (BIONI, 2021, p. 206).

determinado sujeito tinha ligado para diversos neurologistas locais e para um laboratório farmacêutico especializado em esclerose múltipla. Outro indivíduo tinha realizado uma longa ligação para a irmã e dois dias depois para uma clínica de aborto (MENEZES NETO; MORAIS; BEZERRA, 2017).

Ora, apenas com os metadados das ligações se mostra possível deduzir algumas informações extremamente pessoais sobre as vidas particulares dos participantes. Agora, imagine-se o que não seria possível descobrir com a captação dos metadados dos emails trocados, das mensagens instantâneas e até mesmo das buscas realizadas por determinado usuário no Google, por exemplo[99].

O fato é que a capacidade de avanço tecnológico altera constantemente o que pode ser entendido ou não por dado pessoal, principalmente, levando em consideração que as condições e os graus de identificabilidade mudam rapidamente diante das novas formas de armazenamento, de tratamento e de reidentificação dos dados (RUARO; SARLET, 2021).

Todavia, a revelia disso, "[...] a legislação infraconstitucional e a jurisprudência dos tribunais conferem diferentes níveis de proteção a essas diferentes categorias de informações, quais sejam, as informações cadastrais, os metadados e conteúdo das comunicações em si" (ABREU; ANTONIALLI, 2017, p. 17).

Isto é, o grau de proteção aos dados varia de acordo com o tipo de informação que se pretende acessar. Informações cadastrais, em regra, podem ser requisitadas por alguma autoridade autorizada por lei, sem ordem judicial. Já para a requisição de dados, nota-se que é necessário, em geral, ordem judicial fundamentada. Por fim, para que ocorra o acesso ao conteúdo das comunicações em fluxo, ou seja, a interceptação, requer-se, além da ordem judicial fundamentada, a existência de alguma situação permitida na Constituição e seguindo o procedimento da lei de regência[100] (ABREU; ANTONIALLI, 2017).

Portanto, observa-se que os dados são multiformes e podem mudar de categoria jurídica (metadados, dados, dados pessoais, dados pessoais sensíveis, dados anônimos, entre outros) muito rapidamente a depender do contexto e das técnicas de tratamento realizadas. Nesse sentido, a noção de proteção em níveis (degradê), por mais que válida, delega ao intérprete a tarefa de perquirir no caso concreto o correto regime protetivo a ser aplicado, o que nem sempre é uma tarefa fácil, como se verá a seguir.

---

[99] Pode-se dizer que, com a abordagem de tratamento adequada, algumas informações podem ser extraídas dos metadados, como remetente, destinatário, assunto, horário de envio e endereço IP, as quais "[...] podem ser tão ou mais valiosas que o conteúdo dos e-mails. Assim, os dados não são, como quer a lei, 'essencialmente' pessoais, sensíveis ou anônimos" (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 194).

[100] Essa variedade de regimes jurídicos será aprofundada no último capítulo deste estudo.

3.2 FORMAS DE DISPONIBILIZAÇÃO DE DADOS

É crescente a disponibilização de dados na Internet. Isso ocorre de diferentes formas, desde deliberadamente pelas entidades públicas e privadas; até mesmo pelos próprios titulares dos dados (propositadamente ou não). Ocorre que, como visto, os dados não são tão "inofensivos", haja vista que o cruzamento de informações e bancos de dados podem revelar aspectos sensíveis do indivíduo. Levando isso em consideração, a disponibilização desses dados não pode cair no arbítrio dos detentores dos dados.

Pensar dessa forma possibilita a tutela da identidade do usuário em pelo menos duas vertentes. A primeira que protege a identidade digital[101] propriamente dita e possibilita o livre desenvolvimento da personalidade (honra, reputação, imagem, entre outras). Já a segunda que aborda a proteção do indivíduo em face das técnicas de identificação do sujeito, ou seja, protege o usuário dos mecanismos indevidos de tratamento de dados pessoais (RUARO; SARLET, 2021).

Na atualidade, constata-se que o usuário constrói uma projeção da sua identidade física no ambiente virtual. Não se pode esquecer a crescente necessidade de interação do ser humano com a máquina e vice-versa. Diante disso, mostra-se complexo facultar a entidades, públicas ou privadas, a decisão sobre a exposição ou não desses dados.

Isso pode ser visto em casos que envolvem bases de dados públicas, as quais permitem o cruzamento de informações diversificadas, como as de natureza socioeconômica; mercado de trabalho; programas sociais; características demográficas; entre outras (GONÇALVES; VARELLA, 2018).

Desse modo, a disponibilização desses dados sensíveis em posse da Administração Pública se torna complexa, principalmente, considerando que as entidades governamentais são inclinadas a implementar uma política de dados abertos com a publicidade plena. Para tanto, precisa-se de conceitos mais assertivos que viabilizem a correta interpretação dos institutos envolvidos tanto pelas autoridades governamentais como pela sociedade civil (GONÇALVES; VARELLA, 2018).

Aqui, torna-se também importante diferenciar os dados de acesso público daqueles manifestamente públicos. Os primeiros seriam os dados divulgados para atender o dever de transparência imposto ao Poder Público, a exemplo da lista de beneficiários do auxílio emergencial disponibilizada pelo governo. Como a finalidade não é mercadológica, não seria

---

[101] A identidade digital compreende os *passwords*, os dados sobre reconhecimento da face, da voz, da íris, das impressões digitais, entre outros (RUARO; SARLET, 2021, p. 197).

permitido o tratamento desses dados para esse fim, por exemplo (FONSECA; MURAYAMA; ALMGREN; NEVES; MARTINS, 2021).

Por outro lado, também existem os dados manifestamente públicos, os quais são disponibilizados pelos próprios titulares, como ocorre no LinkedIn (rede social profissional). Nas contas da rede social é possível encontrar referências ao nome, à ocupação profissional, à formação, entre outras. Levando em consideração o caráter desses dados, à luz da LGPD, percebe-se que seria possível o tratamento por outra empresa, o que pode ocorrer, por exemplo, para ofertar propostas de emprego (BIONI, 2021).

Essa possibilidade é aberta devido à finalidade pela qual os dados foram tornados públicos. Ou seja, considera-se o contexto em que tal informação foi disponibilizada. Todavia, consoante o disposto na LGPD, mesmo os dados manifestamente públicos devem ser utilizados de tal modo que se respeitem os direitos do titular e os princípios da lei. Ora, a LGPD não autoriza o uso indiscriminado desses dados, muito pelo contrário. Assim, não seria possível a utilização, por exemplo, nesse caso do LinkedIn, dos dados para fins de *marketing.*

Soma-se a esse cenário a disponibilização de dados pelos atores privados, seja propositalmente, seja por vazamento. Na primeira situação, o setor privado divulga os dados por acreditar que eles não apresentam potencial lesivo aos usuários. Um desses casos que ganhou notoriedade foi a divulgação realizada pelo Netflix, em 2006, de um banco de dados parcial, contendo 100.408.507 avaliações criadas por 490.189 usuários. Registre-se que apenas ficou disponível a nota atribuída pelo usuário e a data em que a avaliação foi feita (MENEZES NETO; MORAIS; BEZERRA, 2017).

Ocorre que pesquisadores, utilizando esses dados em conjunto com outra base de dados de acesso público, conseguiram identificar alguns usuários da base de dados do Netflix, a qual teoricamente seria anônima. Isto é, com a utilização das técnicas corretas e com o acesso a informações complementares, pode-se chegar a uma gama de informações sobre os usuários na rede.

Outro caso interessante foi o uso do GPS de alguns acessórios para exercícios, como o bracelete Fitbit, para localização de bases militares secretas, inclusive com um mapa interativo divulgado na rede. Isso foi possível graças ao uso dos soldados de geolocalizadores presentes nos braceletes ao realizar atividades físicas, o que demonstra o risco no uso e na disponibilização sem cautela dos dados (ALONSO, 2018).

Já na ocasião de vazamentos de dados, percebem-se incidentes de segurança que comprometem grandes quantidades de dados. No Brasil, recentemente, verificou-se que 220

(duzentos e vinte) milhões de pessoas tiveram seus dados pessoais divulgados indevidamente na Internet, o que inclui até mesmo pessoas falecidas. Posteriormente, a empresa de cibersegurança PSafe, que identificou o vazamento, informou que aproximadamente 100 milhões de contas de celular foram vazadas na *Deep Web*[102] (SANTOS; SILVA; PADRÃO, 2021).

Ou seja, os dados dos indivíduos devem ser guardados com cautela pelos agentes que atuam no tratamento dos dados. Não é porque eles são acessíveis a terceiros que não merecem proteção jurídica. Ademais, como visto ao longo deste capítulo, deve-se superar a visão de que alguns dados são "inofensivos".

Logo, é preciso que o acesso aos dados gerados por determinado indivíduo seja realizado com as devidas cautelas legais, tanto no âmbito da Administração Pública como da iniciativa privada, tendo em vista a importância que esses dados assumem na atualidade. Caso isso não ocorra, é possível que os titulares dos dados se oponham às violações de seus direitos, como será abordado a seguir.

3.3 PRERROGATIVAS DOS TITULARES DOS DADOS COMO BARREIRA LEGÍTIMA

Frente a esse contexto apresentando, em que a proteção de dados acontece em níveis, observa-se que um dos eixos da LGPD é informado pelos princípios e direitos do titular dos dados. Tal proteção legal busca possibilitar ao titular que tenha controle efetivo sobre o uso de seus dados e possa se opor contra o tratamento de dados indevido.

Inicialmente, levando em consideração que a matéria ainda é nova no país, a LGPD estabelece uma série de diretrizes principiológicas que são utilizadas para sustentar o regime de proteção de dados brasileiro. Ganham destaque o princípio da finalidade, o qual prega que o tratamento de dados só pode ocorrer atrelado à finalidade que justificou a coleta[103]; e o princípio da não discriminação, o qual reconhece o potencial discriminatório do uso de dados ou de mecanismos de decisão automatizada (DONEDA; MENDES, 2019).

---

[102] Dentre os dados vazados, notam-se informações sensíveis: "[...] como tempo de duração das ligações realizadas, número de telefone, plano contratado, valor da conta, volume de minuto gastos por dia, data de nascimento e CPF" (SANTOS; SILVA; PADRÃO, 2021, p. 3).

[103] Partindo disso, a LGPD alterou o art. 16, inciso II, do Marco Civil da Internet (Lei nº 12.965/14), para assegurar que os provedores de aplicações de Internet, onerosos ou gratuitos, não guardem dados pessoais em dissonância com a finalidade pela qual anuiu o titular do dado, salvo nos casos previstos em lei (FLUMIGNAN; FLUMIGNAN, 2020).

Além desses princípios, também chama atenção os cuidados que a nova lei de proteção de dados teve com o postulado da segurança. Essa diretriz aponta para a necessidade dos dados serem mantidos em ambientes seguros contra vazamentos indevidos. A título de exemplo, a transferência de dados entre entidades públicas só deve ocorrer se o órgão receptor apresentar a capacidade técnica para manter os dados seguros (BIASE; AGUILERA, 2021).

Ademais, todos os princípios enunciados na LGPD devem ser lidos em conjunto com o princípio da boa fé objetiva, o qual se encontra previsto tanto no *caput* do art. 6.º do referido diploma legal, como no art. 4.º, inciso III, do Código de Defesa do Consumidor. Desse modo, surgem deveres conexos que devem ser respeitados sob pena de violar as normas de proteção de dados (MENKE; GOULART, 2021).

Cumpre destacar, ainda, que a boa-fé é concebida no ordenamento jurídico brasileiro em duas vertentes. A primeira ligada ao estado de consciência sobre o caráter ilícito de determinada conduta em relação a terceiros, o que pode ser sintetizado na ideia de boa intenção. Já a segunda assume o viés objetivo, baseado no comportamento leal, correto probo (FLUMIGNAN; FLUMIGNAN, 2020).

Desse modo, espera-se que exista transparência no tratamento de dados por parte dos respectivos agentes, de tal modo que os titulares dos dados tenham a garantia de que são municiados com informações claras, precisas e acessíveis acerca do uso dos seus dados. Tal garantia enuncia justamente o princípio da transparência, o qual está previsto no inciso VI do art. 6º, da LGPD, e é aplicado em conjunto com o livre convencimento. Em igual sentido, destaca-se o art. 7° do Marco Civil da Internet (Lei nº 12.965/14) (FLUMIGNAN; FLUMIGNAN, 2020).

Por sua vez, os princípios previstos no art. 6.º da LGPD, voltados para a proteção do indivíduo, devem ser interpretados sistematicamente com os outros princípios já existentes no ordenamento jurídico brasileiro. Um exemplo dessa leitura conjunta ocorre com o tratamento de dados realizado pela Administração Pública, a qual já se encontra submetida aos princípios presentes no texto constitucional, na legislação ordinária, e na doutrina (WIMMER, 2021).

Partindo do pressuposto de que os princípios da LGPD são plenamente aplicáveis ao tratamento de dados realizado por entes públicos, vislumbra-se que alguns princípios conversam entre si, enquanto outros precisam ser compatibilizados. No primeiro grupo, percebem-se os princípios da legalidade e da impessoalidade, os quais se alinham com a lógica da LGPD da não discriminação ilícita ou abusiva. Já no grupo aparentemente dissidente, ganham destaque a publicidade e a privacidade.

Ora, espera-se do Estado um nível elevado de publicidade das suas atividades públicas, ao passo que também há a expectativa de que os dados pessoais dos cidadãos sejam preservados, dentro do possível, já que se referem à intimidade, à vida privada, à honra e à imagem. Mais do que principiológica, pode-se dizer que a discussão gira em torno do diálogo das fontes entre a Lei de Acesso à Informação (LAI) e a LGPD[104]. Esta última que se afasta da ideia pura de sigilo, ainda presente na primeira (GONÇALVES; VARELLA, 2018).

Nesse sentido, mesmo que por meio de caminhos diversos, vislumbra-se que ambos os diplomas legais se tocam quanto à lógica de transparência e à lógica de proteção. A LAI faz menção ao consentimento para a divulgação de informações pessoais (também presente na LGPD). Já a LGPD condiciona o tratamento de dados pessoais de acesso público, dentre outras coisas, ao interesse público. A preocupação com a segurança das informações é comum às leis (WIMMER, 2021).

Diante disso, no que diz respeito à proteção de dados, nota-se uma mudança de paradigma em relação à supremacia do interesse público sobre o privado, principalmente, quando ele está em aparente conflito com um direito fundamental. Mencione-se que a compreensão da privacidade enquanto direito individual a coloca em situação ingrata frente ao interesse público. Ou seja, deve-se entender a privacidade de maneira mais ampla, como já visto no primeiro capítulo.

Já no que diz respeito aos direitos, percebe-se que a norma brasileira de proteção de dados específica esse catálogo no seu Capítulo III, entre os arts. 17 a 22, em grande maioria[105]. O rol de direitos engloba o tradicional "ARCO" (acesso, retificação, cancelamento e oposição) e vai além ao prever, dentre outras, as prerrogativas dos titulares dos dados de: confirmar o tratamento; anonimizar, bloquear ou eliminar dados desnecessários ou excessivos; eliminar os dados pessoais (quando tratados com consentimento); ser informado sobre a possibilidade de não fornecer consentimento e suas consequências; revogar o consentimento; bem como revisar as decisões automatizadas[106] (CRAVO, 2021).

---

[104] Não há uma prevalência, à priori, de algum regime jurídico sobre o outro. A bem da verdade, eles devem ser compreendidos em conjunto com o fim do Estado de fortalecer a democracia e concretizar direitos fundamentais (WIMMER, 2021).

[105] Ressalte-se que não há dúvidas que o rol de direitos elencados na lei de proteção de dados é aberto, haja vista o que se encontra disposto no artigo 64 da LGPD. Este artigo é categórico ao afirmar que os direitos e princípios previstos expressamente na lei não excluem outros que sejam reconhecidos, inclusive, por intermédio de tratados internacionais (CRAVO, 2021).

[106] Outrossim, importante ter em mente que tais direitos, sobretudo os concentrados no art. 18 da LGPD, são exercidos perante o controlador, que é o agente responsável por fornecer as informações e por proceder às correções devidas. Isto é, a informação de quem é o controlador também é vital para o exercício das prerrogativas do titular dos dados (BRASIL, 2022).

Entre todos esses direitos, percebe-se que o consentimento informado ganha muito relevo. Seguindo essa linha, a LGPD garante que será nulo o consentimento quando manifestado de maneira genérica (art. 8º, §4º), haja vista que, a partir de uma análise sistêmica da lei, o consentimento se vincula aos princípios da finalidade, adequação e necessidade (art. 6º, incisos I, II e III) (LIMA; RAMIRO, 2020).

Por sua vez, a defesa desses direitos é facilitada pela LGPD com a previsão de instrumentos processuais tanto individuais como coletivos, nos termos do art. 22. Aliás, pode-se mencionar que esse artigo decorre do próprio princípio da indeclinabilidade da jurisdição previsto no art. 5º, inciso XXXV, da Constituição Federal, já que nenhuma lesão ou ameaça a direito se furta da apreciação do Poder Judiciário.

Como mecanismo individual de tutela, importante destacar a inversão do ônus da prova, a qual se encontra presente no §2º, do art. 42, da LGPD. Para tanto, percebe-se que basta a verossimilhança da alegação e a hipossuficiência para fins de produção de prova ou a onerosidade excessiva na produção dela (BESSA; NUNES, 2021).

Do ponto de vista coletivo, nota-se que os direitos dos usuários da Internet são classificados como direitos coletivos, conforme o art. 81, inciso II, do CDC. Isso se deve ao fato desses direitos ostentarem a qualidade de transindividuais, de tal modo que os usuários se encontram ligados com a parte contrária por intermédio de alguma relação jurídica base, como no caso dos termos de uso de algum aplicativo (SILVA, 2019).

Diante disso, se alguma cláusula destes termos de uso violar algum direito dos indivíduos, por exemplo, mostra-se plenamente possível que ocorra a declaração de nulidade dessa cláusula no bojo de algum processo coletivo, dado o vínculo dos usuários com o aplicativo por meio de uma relação jurídica básica.

Inclusive, percebe-se que tal ação coletiva pode ser intentada até mesmo pelo Ministério Público Federal (MPF), haja vista a competência institucional do órgão de zelar tanto pela proteção dos direitos do consumidor, como dos usuários de provedores e aplicativos da Internet. Deduz-se essa prerrogativa do disposto no art. 6º, inciso VII, letras "c" e "d", da Lei Complementar nº 75/1993, o qual autoriza o manejo das medidas judiciais e extrajudiciais cabíveis (SILVA, 2019).

Outrossim, a atuação do MPF não retira a capacidade de agir de outros órgãos que atuam na proteção de dados. Na verdade, observa-se a necessidade de uma atuação articulada com as instituições que dispõem de competência sancionatória, a exemplo do Senacon, em nível federal, e os Procons, em nível estadual. Também se revela válida a intervenção de

organismos privados de proteção, como o Instituto Brasileiro de Defesa do Consumidor (Idec), que também pode defender os direitos dos consumidores (SILVA, 2019).

Portanto, o titular dos dados pessoais, em conjunto com os demais órgãos competentes, pode exercer os seus direitos e criar uma barreira contra os abusos que porventura estejam ocorrendo no tratamento dos seus dados. Não obstante, essa barreira só pode ser erguida se for dentro do que se compreende como legítimo, de modo que os dados podem ser utilizados em determinas situações, como será abordado a seguir especificamente quanto ao anonimato na rede.

3.4 ANONIMATO NA REDE: UM MITO EM DESCONSTRUÇÃO

A ideia de anonimato em ambientes virtuais se mostra muito útil em determinados contextos. Entre esses contextos, pode-se citar a liberdade de comunicação dentro de certos ambientes sem o temor de sofrer pressões sociais e políticas ou até mesmo preconceito. Nesses casos, tutela-se o livre desenvolvimento da personalidade por intermédio da salvaguarda das liberdades de associação, expressão e relacionamento.

Tendo isso em vista, nota-se, no Brasil, uma grande adesão ao espaço virtual, sobretudo, com a utilização de “personagens virtuais”, os quais empoderam o indivíduo com a sensação de liberdade plena. Todavia, diante de um computador, de um teclado, e de algum mecanismo de disseminação de informação, o usuário externa as mais variadas formas de expressão, tanto o que há de melhor, como o que há de pior (BITTAR, 2012).

Do ponto de vista normativo, há orientações em aparente conflito sobre a temática. Em um lado, aqueles que defendem que o texto constitucional veda o anonimato no âmbito da manifestação do pensamento (art. 5º, inciso IV). Do outro, aqueles que advogam a favor da inviolabilidade do sigilo de dados (os quais podem individualizar o usuário), de modo que se preserve a proteção em relação à intimidade (art. 5º, incisos X e XII da Constituição)[107] (MELO, 2018).

Para aqueles que sustentam o anonimato, percebe-se que isso corre, dentre outras coisas, levando em consideração que o usuário nem sequer é chamado a se manifestar no caso de quebra do sigilo, já que, justamente, o que se discute é a sua identidade, ou seja, qualidade de "anônimo", a qual seria violada em caso de citação. Desse modo, coloca-se em discussão

[107] Indo além, discute-se a imposição de limites à monitoração das atividades onlines, uma vez que a vedação absoluta do anonimato poderia levar à quebra do sigilo dos dados em qualquer caso, o que esvaziaria a garantia constitucional do sigilo (MELO, 2018).

as garantias do devido processo legal, da ampla defesa e do contraditório nesses casos em que o véu de proteção dos dados é levantado[108] (MELO, 2018).

Já para os que relativizam o anonimato, observa-se que eles partem da premissa de que os indivíduos não podem utilizar personagens para praticar a mais variada gama de condutas antijurídicas com a expectativa de que possam sair impunes por meio do anonimato. Diante disso, o regime de proteção do sujeito deve levar em consideração que o reconhecimento de direitos não se presta a conferir um regime jurídico em que vigora a mais plena irresponsabilidade (LEONARDI, 2012).

Ou seja, faz-se necessário o combate à ideia de anonimato pleno que alimenta a sensação de impunidade na rede. Tal combate demanda a criação de mecanismos eficientes que sejam capazes de identificar o autor das transgressões, de forma que seja desestimulado a prática desenfreada de abusos por meio do ajuizamento de ações que possam resultar em punições para o usuário.

Dentre tais mecanismos, evidencia-se a necessidade da retenção dos dados cadastrais e de conexão dos usuários no âmbito da Internet. Isso se mostra possível graças à capacidade dos provedores que operam na Internet de armazenar dados, como os registros de endereço IP de terminais que acessaram seu sítio eletrônico, de forma que esses dados possam, posteriormente, ser usados para identificação dos usuários (MACHADO; DONEDA, 2018).

Para entender melhor como isso ocorre, em síntese, é necessário compreender o que são logs de dados; endereços IP (*Internet Protocol*), e endereço do computador ou MAC (*Media Access Control*) *address.* Nesse sentido, observa-se que os logs são registros de eventos relevantes no sistema computacional, o qual é utilizado para restabelecer um estado anterior ou para registro do comportamento do sistema (SIMÕES; SIMÕES, 2019).

Por sua vez, o IP é um identificador de dispositivos de rede (computador, impressora, etc.), o qual é único e serve para as máquinas se comunicarem na Internet. Por fim, o MAC *address* é o endereço físico do dispositivo, ou seja, sua identificação que é gravada em *hardware.* Isso garante que não existam duas máquinas com o mesmo endereço, haja vista que ele está vinculado à interface de comunicação, que conecta um dispositivo à rede (SIMÕES; SIMÕES, 2019).

---

[108] A árdua tarefa está posta: investigar meios de defesa do sigilo "[...] (i) antes do cumprimento da ordem de fornecimento de dados; e (ii) sem que o titular desse direito seja forçado a se identificar no processo" (MELO, 2018).

Ressalte-se que o endereço IP é usado para rastrear a conexão que se formou em determinado momento vinculada a um *Uniform Resource Locator* (URL), o qual é atribuído por um provedor de conexão ao aparelho conectado à rede. Esse endereço IP é dinâmico, isto é, só perdura enquanto o usuário estiver conectado, de modo que, após o sujeito cessar a conexão, esse IP é atribuído a outro indivíduo. Daí a importância dos logs, os quais são fornecidos pelos provedores de conexão contendo o momento exato de acesso. Com isso, chega-se ao MAC, o que possibilita a individualização (SIMÕES; SIMÕES, 2019).

Mencione-se que é necessária a cooperação também dos provedores de aplicação nessa tarefa, tendo em vista que, nos termos do art. 14 do MCI, os provedores de conexão só estão autorizados (obrigados) a reter os logs de conexão. Não que esses provedores não dispusessem de capacidade técnica para tanto, mas o legislador optou por preservar os usuários temendo uma vigilância completa de toda a navegação do indivíduo pelos provedores de conexão[109] (BIONI, 2021).

De outra banda, percebe-se que um procedimento comum utilizado para garantir, em tese, a não identificação dos usuários é o de anonimização[110]. Essa técnica consiste na utilização de artimanhas razoáveis disponíveis no momento do tratamento para que o dado perca a possibilidade de associação, seja direta, seja indireta, a um indivíduo, segundo o art. 5º, inciso III da LGPD[111] (VIOLA; TEFFÉ, 2021).

Entre essas artimanhas, destacam-se a supressão, a generalização, a randomização e a pseudoanonimização. Tais artifícios possibilitam a ruptura do vínculo existente entre a pessoa e o dado. Quando não for viável a ruptura, busca-se tornar o vínculo, dentro possível, mediato, inexato e impreciso (RUARO; SARLET, 2021).

Nesse sentido, dificulta-se a identificação do titular do dado. Entre as técnicas citadas para tanto, a título de exemplo, mostra-se válido ressaltar a técnica da pseudonimização, a qual mitiga os riscos do tratamento.

Essa técnica consiste na substituição de um atributo (geralmente único) em um pseudônimo. Isto é, ocorre um disfarce da identidade, o que é muito útil diante de

---

[109] Seguindo essa linha, qualquer estipulação em contrário, que permita a coleta combinada de dados (logs de acesso e aplicação), será tida como tendente a fraudar norma imperativa prevista no MCI, de tal modo que deverá ser declarada sua nulidade (BIONI, 2021).

[110] O assunto da anonimização pode ser encontrado ao longo da LGPD, nos seguintes termos legais: "[...] conceituada no artigo 5º, III e XI, e definida como direito do titular de dados nos artigos 11, II, b, 16, II e IV, e 18, IV, mas essencialmente peculiar por afastar a incidência da LGPD em razão de expressa disposição contida no artigo 12, §§1° a 3º" (FALEIROS JÚNIOR; MARTINS, 2021, p. 378).

[111] Rememore-se que, consoante o art. 12 da LGPD, o dado anonimizado não seria um dado pessoal, de tal modo que a privacidade do titular, em tese, estaria mais protegida (VIOLA; TEFFÉ, 2021).

identificadores diretos. Pelo colocado, nota-se que a identidade do usuário se encontra preservada, desde que as informações suplementares relacionadas ao atributo original sejam mantidas separadas da base de dados que originária (MACHADO; DONEDA, 2018).

Mencione-se que a pseudoanonimização não necessariamente conduz a anonimização dos dados tratados, de tal modo que há quem sustente que ocorre apenas uma redução da "[...] possibilidade de composição de conjuntos de dados para a reindentificação mas não a elimina e, portanto, é considerada apenas como uma medida de segurança suplementar, mas não um método de anonimização de dados pessoais" (RUIZ, 2020, p. 114).

Nesse cenário, a pseudoanonimização possibilita a reversão do processo de anonimização, tendo em vista a utilização de uma técnica de anonimização superficial. Por exemplo, os dados do indivíduo podem ser acessados pela própria organização que empregou a técnica, o que revela que um procedimento passível de quebra.

Desse modo, em alguns casos, sustenta-se a utilização de uma noção de "anonimização robusta", a qual poderia ser realizada com a formação de bancos de dados compostos por dados anonimizados. Isso, em tese, tornaria a reidentificação impossível. Todavia, como já apresentado em vários momentos, a ideia vigente é utilizar os dados para os mais variados fins e realizar o tratamento apenas com dados anonimizados reduziria em muito a gama de informações que poderiam ser extraídas (RUIZ, 2020).

Registre-se que os dados anonimizados, por mais que não identifiquem diretamente o usuário, também apresentam grande utilidade. Pode-se citar o exemplo da apuração de intenção de votos em uma eleição com a coleta informações referentes ao sexo, à escolaridade, à região geográfica e à classe social dos entrevistas. Depreende-se que, embora as informações sejam cruzadas entre si, será quase impossível chegar a pessoa específica que respondeu à pesquisa (VIOLA; TEFFÉ, 2021).

Não por outro motivo a própria LGPD aborda os dados anonimizados sob a premissa de que a reversão seria possível, ou seja, que não seria utilizada essa concepção de "anonimização robusta". A bem da verdade, o referido instrumento normativo analisa os dados anonimizados por intermédio da composição de uma matriz de risco de reversibilidade[112] (BIONI, 2020).

Seguindo essa linha, é importante ter em mente que, da mesma forma que existem maneiras de anonimizar os dados, também há mecanismos para identificá-los novamente. Ora,

---

[112] Depreende-se que a LGPD adota a anonimização (art. 18, inciso IV) como um importante pilar para o sistema protetivo dos dados pessoais, o qual deve ser lido em conjunto com o consentimento informado (art. 7º, inciso I da LGPD) (LIMA; RAMIRO, 2020).

os dados são coletadas em praticamente todas as atividades realizadas diariamente, seja no ambiente físico (câmeras de vigilância), seja no ambiente virtual (redes sociais).

Nessa perspectiva, "pegadas" são deixadas ao longo das atividades que são realizadas, o que possibilita a reidentificação do usuário[113]. Partindo disso, a anonimização e a desanonimização podem ser caracterizadas como um jogo de adversários, em que o adversário é a pessoa ou modelo computacional voltado para a desanonimização. O objetivo do adversário, na maioria das vezes, é conseguir novas informações do indivíduo ou grupo de indivíduos pela combinação do conhecimento próprio ou adquirido dos dados anonimizados ou da técnica empregada para tanto (RUIZ, 2020).

Verdadeiramente, com os avanços tecnológicos; a grande quantidade de dados coletados; o implemento da capacidade de processamento e análise de algoritmos de mineração de dados; e o aprimoramento do aprendizado de máquina, a reidentificação dos indivíduos, mesmo diante de dados anonimizados, revelou-se uma realidade que não pode ser ignorada[114] (MACHADO; DONEDA, 2018).

Diante disso, tornou-se um mito em desconstrução pensar que o usuário poderia utilizar a rede de maneira totalmente anônima. Isto é, por mais que a proteção de dados avance, observa-se que as técnicas de desanonimização de bases de dados acompanham esse avanço[115] (RUARO; SARLET, 2021).

Portanto, não se sustenta o mito de que seria possível interagir na Internet de maneira totalmente anônima. Ora, nem os dados anonimizados preservam em todos os casos a característica do anonimato. Depreende-se que, ao usar a rede, são coletados os mais variados tipos de dados que podem servir para identificar o usuário, a exemplo dos dados de conexão e cadastrais. Diante disso, mostra-se vital que seja desenvolvido um regime de obtenção de dados que leve em consideração todos esses pontos e traga maior proteção para os titulares de dados, como será abordado a seguir.

---

[113] Em síntese: "[...] a agregação de diversos 'pedaços' de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico" (BIONI, 2020, p. 191).

[114] Percebe-se que atributos únicos podem identificar o sujeito sem maiores esforços algoritmos para tanto. Por sua vez, por meio do cruzamento de informações e bases de dados, qualquer atributo pode se tornar um identificador (FALEIROS JÚNIOR; MARTINS, 2021).

[115] De certa forma, mostra-se razoável que não ocorra o total anonimato na rede, haja vista que a Internet não deve ser usada com uma máscara que encobre os mais variados tipos de abusos e violações de direito (BITTAR, 2012).

4. REGIMES JURÍDICOS DE OBTENÇÃO DE DADOS NO DIREITO BRASILEIRO

Desde a promulgação da Constituição Federal de 1988, nota-se que o debate em torno do regime jurídico a ser aplicado no caso da obtenção de dados ganha notoriedade no cenário jurídico brasileiro. Percebe-se que a maior controvérsia travada gira em torno das proteções conferidas ao fluxo informacional, isto é, a comunicação dos dados e os dados já armazenados em determinado dispositivo informático.

Não por outro motivo esse debate já foi introduzido no imaginário jurídico nacional, ainda no início da década de 90, por Ferraz Júnior (1993), o qual defendia que a proteção presente no art. 5º, inciso XII, da Constituição Federal, seria aplicável apenas no caso da comunicação dos dados, e não dos dados considerados em si mesmos.

Mencione-se que esse entendimento se encontra presente até os dias atuais, tendo em vista sua adesão, à época, em alguns julgados do Supremo Tribunal Federal (STF)[116]. Ocorre que a tecnologia avança muito rapidamente e muda o substrato fático das normas jurídicas com muita dinamicidade. Diante disso, não se nega a coerência da linha argumentativa que sustentava a proteção mais qualificada apenas para a comunicação dos dados, todavia os dados, como visto no capítulo anterior, ganharam uma nova dimensão de importância na sociedade atual, a qual é cada vez mais dependente dos dados dos dispositivos informáticos.

Seguindo essa linha, subsiste no ordenamento jurídico brasileiro duas maneiras bem definidas da obtenção de informações decorrentes da interpretação de dados. De um lado, a interceptação do fluxo informacional e, de outro a requisição de dados, que em determinados casos, pode acontecer até administrativamente.

Partindo disso, analisa-se, a seguir, como ocorre a obtenção de dados e como as atuais mudanças fáticas (evolução tecnológica), jurídicas (novas normas) e sociais (novos modos de se relacionar com a tecnologia) experimentadas no país podem ou não afetar nesse processo e no papel assumido pelos intermediários da Internet que prestam serviços relacionados com a coleta e guarda de dados dos usuários.

4.1 HEGEMONIA DOS ATORES PRIVADOS NO AMBIENTE DIGITAL E SUA ATUAÇÃO COMO INTERMEDIÁRIOS DA REDE

[116] Dentre esses julgados, podem ser citados o Mandado de Segurança nº 21.729/DF (em que se discutia um caso em torno do sigilo bancário), e o Recurso Extraordinário 418.416/SC (em que se debateu o sigilo dos dados armazenados em dispositivo informático obtido por intermédio de uma busca e apreensão). Em ambos os casos, a tese defendida por Ferraz Júnior se sagrou vitoriosa, de tal modo que não foi conferida a proteção presente no art. 5º, inciso XII, da Constituição Federal, haja vista não se tratarem de situações de comunicação de dados (QUEIROZ; PONCE, 2020).

Mostra-se crescente o poder (auto)atribuído[117] aos atores privados no ambiente privado, principalmente, levando em consideração a arquitetura da rede[118] e a omissão estatal. Nesse sentido, nota-se, por exemplo, que os provedores digitais estão assumindo funções de regulação e de poder de polícia, tipicamente de direito público. De fato, atuam como ciberreguladores privados e ciberpoliciais[119].

Tanto é verdade que já se pensa em uma modalidade de "Constitucionalismo Digital"[120], o qual primeiramente se vinculava a ideia de limitação dos poderes dos atores privados na Internet. Com o decorrer do tempo, essa ideia ganhou uma conotação de "guarda-chuva", haja vista que passou a abranger áreas jurídicas, políticas, estatais e não-estatais, direcionadas à garantia de direitos fundamentais na Internet, levando em consideração as dimensões horizontal e vertical dos direitos fundamentais (MENDES; FERNANDES, 2020).

Percebe-se que esses atores privados utilizam algumas ferramentas para garantir e perpetuar sua hegemonia. Um exemplo é a utilização de Termos de Serviço (ToS), que estipulam, unilateralmente, dentre outras coisas, a maneira de acesso aos conteúdos e o regime de coleta e utilização de dados. Frente uma realidade de adesão, "pegar ou lugar", o usuário não dispõe de poder de barganha e se depara com uma verdadeira "lei", a qual é estabelecida e modificada de forma exclusiva pelo provedor de aplicação[121] (BELLI; FRANCISCO; ZINGALES, 2019).

Essa realidade se revela problemática, uma vez que esses atores privados são movidos, muitas vezes, por interesses próprios que podem comprometer sua atuação imparcial. Nesse sentido, percebe-se um aparente conflito entre os interesses econômicos dos agentes

---

[117] Percebe-se que a regulação não é exercida apenas pelo Estado, mas também pode ser executada tanto por atores privados (autorregulação) como pela junção desses dois sistemas (corregulação). Mencione-se que esse cenário de autorregulação crescente pode ser explicado pela ausência de leis mais assertivas sobre a temática, o que não impede que esse contexto possa evoluir para um ambiente de corregulação e, por fim, de regulação (VALENTE, 2019).

[118] A arquitetura da rede diz respeito à maneira pela qual a Internet é estruturada, ou seja, ao conjunto de camadas que a compõem e as formas como elas interagem entre si. Nesse sentido, percebe-se que ela é organizada em torno de protocolos, os quais são multáveis. Por intermédio dessas modificações, mostra-se possível alterar as formas de utilização da rede. Por analogia, exemplifica-se essa ideia com a construção de lombadas, as quais representam uma modificação na arquitetura urbanística que repercute nas maneiras de utilização dos usuários (LESSIG, 2006).

[119] Diante da falta de autoridade pública internacional, os provedores de plataforma apresentam a capacidade de ditar "[...] unilateralmente a lei do (ciber) território, aplicá-la e utilizar suas regras autoestabelecidas para julgar conflitos entre os usuários da plataforma" (BELLI; FRANCISCO; ZINGALES, 2019, p. 450).

[120] Destaque-se que essa noção não se limita aos mecanismos tradicionais do constitucionalismo, ao passo que também inclui ferramentas para lidar com a transnacionalidade inererente ao ambiente digital globalizado (CELESTE; SANTARÉM, 2022).

[121] Ressalte-se que essa normatividade estabelecida é autoexecutória, haja vista que ela não precisa ser implementada por órgãos públicos, de tal modo que ela se adequa aos interesses dos seus criadores (BELLI; FRANCISCO; ZINGALES, 2019).

privados que atuam na rede e os direitos fundamentais dos usuários, tendo em vista a busca por lucro das grandes corporações.

A título de exemplo, pode-se citar o caso do YouTube, sem dúvida uma das mais notáveis plataformas digitais. Criado em 2005 e logo após adquirido pelo Google, a plataforma é de longe a maior plataforma online de *streaming* de vídeo do mundo, a qual influencia a própria maneira de consumir conteúdo online, atuando como um intermediário da indústria cultural (BELLI; FRANCISCO; ZINGALES, 2019).

Interessante notar que o YouTube implementa sua política de uso baseado na *US Digital Millennium Copyright Act* (DMCA), um regime legal estadunidense, mas que se aplica a todos os usuários da plataforma, independentemente de qual local ocorra o acesso. Nesse sentido, cria-se um regime híbrido público-privado, o qual, por sua vez, é implementado de forma privada (BELLI; FRANCISCO; ZINGALES, 2019).

Isso demonstra uma hibridização da governança na rede, tendo em vista a delegação crescente por parte dos atores públicos de atribuições regulatórias para os atores privados. Essa delegação ocorre, muitas vezes, pelo setor público acreditar na eficiência maior dos intermediários da rede em conseguir os fins almejados.

Dentre as normas estipuladas pela plataforma, chama atenção a política de violação de direitos autorais. Segundo o procedimento privado do YouTube, a conta do usuário é encerrada se um canal receber três *strikes* de direitos autorais. Ou seja, "[...] todos os seus vídeos serão removidos – note, mesmo aqueles que não infringem quaisquer direitos – e o usuário não poderá criar novas contas" (BELLI; FRANCISCO; ZINGALES, 2019, p. 463).

Nesses termos, percebe-se que esses intermediários gozam de certo poder normativo para estabelecer seus ToS, bem como apresentam, em certa medida, o poder de executá-los, o que é complementado pela prerrogativa de julgar as condutas dos usuários que violam ou não seus ToS. Todavia, nem sempre as decisões tomadas pelos atores privados são acertadas, principalmente, quando se deparam com conceitos indeterminados ou conflito de princípios jurídicos, o que pode levar a restrições indevidas.

Por sua vez, esses agentes privados também devem cumprir certas obrigações legais, dada essa posição privilegiada no ambiente digital, sobretudo, do ponto de vista técnico. Observa-se que essas obrigações variam de acordo com a função desempenhada pelo ator privado e o fim que ele almeja atingir.

Desse modo, inicialmente, é importante analisar os vários tipos de provedores que atuam na Internet para que se possa definir quais interessam para o presente estudo. Partindo

disso, pode-se esclarecer que ao se referir a "provedor de serviços de Internet" se está abordando a pessoa natural ou jurídica que fornece serviços por intermédio da Internet ou auxilia no funcionamento dela (LEONARDI, 2005).

Cabe frisar que esse é o gênero do qual decorrem as demais categorias de provedores, os quais são classificados em provedores de *backbone*, de acesso, de correio eletrônico, de hospedagem e de conteúdo[122]. Registre-se que existe certa confusão quanto à categorização dos principais provedores de serviços de Internet, tendo em vista que eles costumam aglutinar as funcionalidades de vários provedores, como provedores de informação, conteúdo, hospedagem, acesso e correio eletrônico (ROTH; NUNES, 2019).

Nesse sentido, quanto às espécies de provedores, percebe-se que eles são divididos levando em consideração o seu papel na rede. Desse modo, há os provedores de *backbone* (ou "espinha dorsal"), o qual representa a estrutura física (cabos de fibra óptica de alta velocidade) por meio do qual se realiza o tráfego de dados na Internet (LEONARDI, 2005).

Esses provedores não apresentam grande relevância na temática da guarda de dados, uma vez que apenas oferecem a infraestrutura necessária para que a conexão ocorra, de tal modo que não se espera que esses provedores armazenem dados dos usuários, dada a natureza do serviço prestado.

Por sua vez, ganha destaque na cadeia de transporte de dados eletrônicos os provedores de acesso (conexão)[123], os quais, a partir das suas funções realizadas na rede, podem auxiliar no rastreamento do ponto de origem de determinado usuário no ambiente digital, o que permite a adoção das medidas legais contra ele, se for o caso (YAMAGUCHI, 2021, p. 533).

Partindo disso, nota-se que o usuário consegue acessar a Internet, justamente, por intermédio de um provedor de acesso à Internet, o qual representa uma pessoa jurídica que, muitas vezes, vale-se de um servidor de *backbone*[124] para franquear o acesso do usuário ao ambiente digital. Essa forma de acesso pode ocorrer de várias maneiras, tanto por meio de um provedor comercial (instalado em empresas, livrarias e cafés), como da própria empresa,

---

[122] Destaque-se que essa classificação é doutrinária, tendo em vista que após o Marco Civil da Internet, passou-se a definir de maneira um pouco diferente os provedores que atuam na rede, como será abordado logo mais.

[123] Registre-se que esses provedores, teorizados no passado, hoje se encaixam bem na ideia de provedores de conexão à Internet, tendo em vista as funções exercidas e o regime de isenção de responsabilidade pelo conteúdo veiculado por intermédio dele (ROTH; NUNES, 2019).

[124] Válido mencionar que o internauta que se vale de um provedor de acesso não tem relação jurídica direta com o provedor de *backbone*, haja vista que, em regra, desconhece até a estrutura por trás desses provedores (LEONARDI, 2005).

instituição de ensino ou órgão público, desde que disponham de conexão direta a um provedor de *backbone*[125] (LEONARDI, 2005).

Já o provedor de hospedagem é a pessoa jurídica encarregada de fornecer o serviço de armazenamento de dados em servidores de acesso remoto, de tal modo que seja facultado o acesso a esses dados de acordo com a política de contratação do serviço. Ou seja, esse tipo de provedor fornece tanto o serviço de armazenagem de dados como o de acesso a esses dados armazenados (LEONARDI, 2005).

Percebe-se que tais provedores hospedam o conteúdo gerado pelos provedores de conteúdo, de tal modo que a relação jurídica existente ocorre entre o provedor de hospedagem e o provedor de conteúdo, consoante o modelo de contrato firmado. Seguindo essa definição, observa-se que são exemplos desse tipo de serviço as redes sociais (*twitter*, *facebook* e *instagram*) e os serviços de *streaming*. Ademais, também pode-se citar os blogs pessoais, em que um provedor de conteúdo se vale de um provedor de hospedagem para ofertar seu serviço (YAMAGUCHI, 2021).

Também é importante distinguir os provedores de informação dos provedores de conteúdo. Por mais que empregados como termos sinônimos em muitos casos, observa-se que a equivalência não é exata. O provedor de informação é a pessoa natural ou jurídica responsável pela criação das informações veiculadas na Internet. Já o provedor de conteúdo representa as pessoas naturais ou jurídicas encarregadas pela disponibilização na rede das informações criadas ou desenvolvidas pelos provedores de informação (LEONARDI, 2005).

Nessa perspectiva, as figuras dos provedores de informação e conteúdo podem ou não coincidir na mesma pessoa, levando em consideração se o provedor é autor ou não daquilo que disponibiliza. Mencione-se que, como visto, o serviço de oferta do conteúdo no ambiente digital pode ocorrer com o uso de um provedor de hospedagem ou com a oferta desse serviço pelo próprio provedor de conteúdo.

Importante destacar que essas várias espécies de provedores foram resumidas a dois gêneros tanto pelo MCI como pelo Superior Tribunal de Justiça (STJ), quais sejam os provedores de conexão e os provedores de aplicação. Seguindo essa linha, leva-se em consideração a atividade desempenhada pelo provedor para o enquadramento em alguma

---

[125] Levando em consideração o colocado, depreende-se que só é necessário que a empresa forneça o acesso à Internet para o indivíduo para ser considerado provedor de acesso, de forma que não é preciso que ocorra a oferta de nenhum outro produto (YAMAGUCHI, 2021).

dessas categorias, as quais não são estanques. Desse modo, o gênero provedor de aplicação pode ser decomposto em provedores de conteúdo, hospedagem etc. (ROTH; NUNES, 2019).

Desse modo, os provedores de aplicação, consoante o artigo 5º, VII, do MCI, englobam todas as funcionalidades que podem ser acessadas na Internet, como os serviços de "[...] correio eletrônico (Gmail, Hotmail, entre outros), hospedagem/armazenamento de dados (serviços de Cloud Computing, como a Amazon, Google, Dropbox etc.), disponibilização de imagens, inclusive, com a finalidade de compartilhamento (Youtube) [...]" (COLOMBO; FACCHINI NETO, 2017, p. 228).

Superadas essas explicações iniciais, nota-se que, no ambiente virtual, o intermediário dos serviços ofertados "[...] é, quase sempre, um provedor que oferece aos seus usuários diversos serviços, conforme a natureza de suas atividades: infraestrutura, acesso, correio eletrônico, hospedagem, conteúdo, busca, entre outros" (LEONARDI, 2012, p. 262).

Esses intermediários ganharam muito relevo no contexto de regulação da Internet, haja vista a tendência dos entes estatais em impor uma série de deveres e sanções a certos intermediários. Isso ocorre, por exemplo, para que determinada prática ilegal cometida no ambiente virtual não fique sem proteção jurídica.

Diante disso, a fixação de medidas de apoio em relação aos intermediários permite a regulação de condutas online e a tutela de direitos violados na Internet. Registre-se que o fato de a violação ser oriunda de outro país não obsta, por si só, a utilização dos agentes que atuam no ambiente virtual, uma vez que, mesmo nesses casos, pode-se fazer uso de intermediários locais (LEONARDI, 2012).

Ora, observa-se uma gama de agentes locais que atuam na Internet e que podem auxiliar na regulação da Internet. Dentre eles, podem ser citados o provedor de acesso que possibilita a conexão; a infraestrutura física de comunicações; os servidores de DNS; os provedores nacionais de hospedagem e de mecanismos de busca; as instituições financeiras que transacionam na rede[126], entre outros (LEONARDI, 2012).

Tendo isso em mente, mostra-se fundamental entender quais são essas medidas e quando podem ser utilizadas. Preliminarmente, o uso desses atores privados ocorre quando eles próprio não são os violadores de normas jurídicas e eles dispõem de capacidade técnica para implementar as medidas necessárias para efetivar o desejo pleiteado pela vítima e

[126] Ressalte-se que a utilização de intermediários financeiros para regulação do ambiente digital pode ser realizada tanto pelo Estado como pelos particulares, tendo em vista a possibilidade de implementação de arquiteturas de controle que apresentam a capacidade de checar a localização geográfica da conexão do usuário (LEONARDI, 2012).

determinado pela autoridade competente. Ademais, também é importante analisar contra quem será imposto o ônus colaborativo.

Diante disso, percebe-se que, se o intermediário for nacional, a medida pode ser imposta diretamente; caso seja estrangeiro, mas com representante nacional, a medida pode ser imposta contra o representante nacional; por fim, se o intermediário não for nacional nem possua representação nacional, a medida pode ser direcionada para os intermediários locais que oferecem formas de acesso às informações, como provedores de acesso, provedores de infraestrutura e mecanismos de busca (LEONARDI, 2012).

Por exemplo, vários tribunais brasileiros já confirmaram que a empresa Google Brasil Internet Ltda. e Google Inc. fazem parte do mesmo grupo econômico, de tal modo que a filial brasileira deve cumprir as decisões proferidas contra a matriz norte-americana. Entre essas decisões, notabilizaram-se aquelas sobre o fornecimento de dados cadastrais armazenados em servidores fora do Brasil (LEONARDI, 2012).

Já quanto ao comando colaborativo, nota-se que ele deve ser feito dentro dos ditames da razoabilidade e da proporcionalidade, uma vez que, via de regra, a "[...] imposição aos provedores do ônus de fiscalização de seus serviços, como meio de impedir atos ilícitos futuros de modo permanente, quase sempre ofenderá a regra da proporcionalidade" (LEONARDI, 2012, p.280).

Isso se deve ao fato das medidas impostas, na grande parte das vezes, serem adequadas (conseguem atingir o fim) e necessárias (medida mais eficaz). Contudo, não necessariamente são proporcionais em sentido estrito. Ora, sem uma boa especificação do comando colaborativo, os provedores acabam obrigados a realização de fiscalizações infinitas que podem até mesmo beirar a censura dos usuários.

A preocupação é legítima frente a grande quantidade de informações disponibilizadas na Internet, o que coloca os mecanismos de busca como intermediários centrais no que diz respeito ao acesso ao conteúdo presente no ambiente digital. Esses intermediários podem se valer de algumas medidas para coibir o cometimento de ilícitos na rede. Uma delas, talvez a mais conhecida, diz respeito à remoção ou à modificação de determinados resultados de busca.

Outra forma de atuação dos mecanismos de busca se refere à implementação de filtros de localização geográfica, sobretudo, quando o assunto litigioso pode ser ilícito em determinado país, mas lícito em outro. Pode-se citar como exemplo o caso LICRA v. Yahoo!, o qual teve início na França e término nos Estados Unidos. A problemática girava em torno da

veiculação de conteúdo nazista no website norte-americano www.yahoo.com, o qual podia ser acessado livremente por qualquer pessoa (LEONARDI, 2012).

Ocorre que a disponibilização desse tipo de material é tida como crime pela legislação francesa, de tal modo que a subsidiária Yahoo! France retirou as informações nazistas encontradas no website www.yahoo.fr. Contudo, os franceses conseguiam acessar e até mesmo comercializar o conteúdo por intermédio do website estadunidense. Nesse sentido, uma solução viável seria a implementação de um filtro tecnológico com base na localização geográfica dos internautas para barrar o acesso de endereços IP oriundos da França (LEONARDI, 2012).

Outro episódio emblemático ocorreu com os buscadores Google e Yahoo!. Caso utilizado o termo de busca "stormfront" (ligado à uma organização estadunidense supremacista branca), nas versões brasileira ou norte-americana, seria possível o acesso ao website da organização Stormfront.org. Por sua vez, isso não seria possível se utilizadas as versões alemã e francesa dos buscadores, tendo em vista a vedação desse tipo de material nesses países. Novamente, necessita-se do filtro geográfico (LEONARDI, 2012).

Nota-se que os atos ilícitos virtuais envolvem pelo menos três agentes, quais sejam: autor, vítima e intermediário. Ressalte-se que também é possível que o próprio intermediário pratique o ato ilícito ou se responsabilize por ele, levando em consideração o descumprimento de suas obrigações. Nesse sentido, importante destacar que os esforços iniciais contra o ato ilícito praticado podem recair sobre o autor de tal ato, que pode ser um intermediário ou não. Caso não seja o autor do ilícito, o intermediário, a priori, não será responsabilizado, uma vez que apenas fornece o serviço.

Por exemplo, depreende-se que o provedor de conexão à Internet não se responsabiliza pelos conteúdos postados pelos usuários, tendo em vista que ele não se relaciona com as informações divulgadas, mas apenas guarnece meios para que o internauta interaja com outros provedores, seguindo o disposto no art. 18 do MCI. Situação diversa pode ser vista com os provedores de aplicação, os quais também são intermediários, mas que podem vir a ser responsabilizados nos termos do art. 19 do MCI[127] (TEFFÉ; SOUZA, 2019).

Logo, depreende-se que os atores privados que atuam na Internet, na atualidade, apresentam muitas prerrogativas (delegadas ou autoatribuidas), o que os coloca como sujeitos

[127] Nesse sentido: "Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário" (BRASIL, 2014).

de grande interesse para o sistema jurídico. Na qualidade de intermediários, função exercida, geralmente, por algum tipo de provedor, percebe-se que eles podem auxiliar os entes estatais de várias maneiras, de tal modo que são estipuladas algumas obrigações legais para esses agentes privados. Dentre elas, o dever de guarda de dados, como se verá a seguir.

4.2 INTERMEDIÁRIOS DA INTERNET E DEVER DE GUARDA DE DADOS

Um dos temas mais polêmicos na atualidade se relaciona com a proteção dos dados dos usuários e a necessidade legal de retenção de dados pelos intermediários dos serviços. Em vários casos, tais intermediários se encontram compelidos a coletar e armazenar dados para não serem penalizados. Diante disso, é preciso entender em quais casos isso ocorre, para que o indivíduo não fique ainda mais exposto ao uso desmedido de seus dados.

Esse debate vem à tona quando a monitoração eletrônica de pessoas se torna cada vez mais comum, como por tornozeleira eletrônica, *softwares* e demais dispositivos. Para o funcionamento dessa tecnologia, nota-se a utilização de sinais de GPS e de telefonia móvel, os quais indicam localidades geográficas e possibilitam o monitoramento em "tempo real" da pessoa (PIMENTA; PIMENTA; DONEDA, 2019).

Nesse sentido, percebe-se que, para o correto funcionamento desse sistema de monitoramento eletrônico, é necessária a utilização do tratamento de dados pessoais, inclusive, dados pessoais sensíveis. Essa definição de sensível, segundo a base teórica presente no capítulo anterior, deve-se ao fato do tratamento propiciar, de forma detalhada, os deslocamentos físicos de uma pessoa, de tal modo que é possível inferir os hábitos, relacionamentos, preferências, entre outras coisas.

Desse modo, inicialmente, é importante destacar que a retenção desses dados não se confunde com a interceptação do conteúdo das comunicações. Depreende-se que o sigilo dos dados, em nível constitucional, segundo a visão mais tradicional[128], decorre do art. 5º, inciso X, da Constituição Federal, ao passo que o sigilo das interceptações decorre do art. 5º, inciso XII, do texto constitucional, conforme será aprofundado em momento oportuno.

Ademais, nota-se que as disposições legais para determinar o armazenamento de dados e metadados por empresas privadas durante um prazo pré-determinado foi introduzido no Brasil de maneira gradual, como em outros países. Isso demonstra o nível de importância

[128] Como defensor dessa corrente mais tradicional, pode-se apontar Ferraz Júnior (1993).

que é dado para essas informações, as quais são geradas de maneira passiva, pelo uso da tecnologia (FRANCISCO; VENTURINI, 2019).

Ressalte-se que os provedores de conexão e de conteúdo são os atores privados mais demandados na temática da colaboração probatória. Partindo disso, nota-se que a guarda de dados por esses atores já é debatida na realidade jurídica brasileira desde o Projeto de Lei nº 84/1999, mas que só se aperfeiçoou com o surgimento do Marco Civil da Internet (MCI) (SIMÕES; SIMÕES, 2019).

Observa-se que o Marco Civil da Internet (Lei 12.965/2014), em junho de 2014, trouxe a preocupação expressa do legislador com a proteção dos dados pessoais, inclusive, com a sua incorporação tanto entre os pilares do diploma legislativo como entre os princípios presentes na lei (art. 3º, inciso III). Seguindo essa linha, é garantido a inviolabilidade e o sigilo do fluxo de comunicações pela Internet, bem como das comunicações privadas armazenadas (art. 7º, incisos II e III)[129] (GAJARDONI; MARTINS, 2020).

Diante desse contexto, o art. 10 do Marco Civil da Internet fixa o regime de guarda dos dados digitais por parte dos provedores. Pela interpretação literal do *caput* do referido artigo, nota-se que "[...] a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, [...], devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas"[130] (BRASIL, 2014).

Registre-se que essas garantias são muito valiosas dentro da Lei mencionada, de modo que, em que pese não serem garantias absolutas, só podem ser devassadas, inclusive para fins penais, por ordem judicial, nos termos do §1º, do art. 10. Desse modo, o provedor somente deverá disponibilizar os citados dados digitais "[...] de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial [...]" (BRASIL, 2014).

Ainda, o art. 15 do referido diploma legal determina o dever de guarda para os provedores que exerçam sua atividade empresarialmente, ou seja, de forma organizada, profissional e com fins econômicos. Percebe-se que o destinatário não é todo e qualquer provedor, contudo provedores não comerciais podem ser obrigados a guardar dados, mediante

---

[129] Outrossim, o Marco Civil da Internet assegura dentre os direitos dos usuários previstos no art. 7°, no inciso I, a "[...] inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2014).

[130] Pelo colocado, vislumbra-se que os provedores podem compartilhar os dados pessoais captados em determinadas situações, contudo o compartilhamento, em qualquer caso, deve garantir a intimidade, a vida privada, a honra, e a imagem das partes envolvidas, seja diretamente, seja indiretamente (MOURA; BARBOSA, 2020a).

ordem judicial e condicionado à especificação de fatos e por tempo determinado, como assegura o §1, do art. 15 do MCI (BRASIL, 2014).

Ademais, restam claros os cuidados legais no que diz respeito à guarda dos referidos dados e ao seu respectivo período de custódia, uma vez que os provedores de acesso devem guardar esses dados pelo período de pelo menos 1 (um) ano, conforme o art.13 da Lei, ao passo que os provedores de aplicação devem preservar os dados pelo período de pelo menos 6 (seis) meses, de acordo com o art. 15 do Marco Civil (BRASIL, 2014).

Mencione-se que esses prazos fixados pelo legislador não são imunes a críticas, sobretudo, levando em consideração os prazos prescricionais presentes no ordenamento jurídico brasileiro. Por exemplo, na legislação civil, vislumbra-se que é de três anos o prazo prescricional para reparação civil (art. 206, inciso III, do Código Civil). Diante disso, a vítima pode se ver desamparada caso busque a reparação após o prazo de guarda dos dados pelos provedores, mesmo que dentro do prazo prescricional (LIMA, 2015).

Por outro lado, também é importante frisar que o armazenamento de dados durante longos períodos acarreta um custo operacional e de armazenamento elevado para as empresas que fornecem os dados. Não se pode negar que o armazenamento de informações pelos atores privados que atuam na Internet é uma atividade de significativa onerosidade, tendo em vista que a manutenção de bancos de dados necessita de uma infraestrutura de equipamentos comprados ou alugados, bem como os serviços de manutenção, fora os gastos com energia (YAMAGUCHI, 2021).

Não por outro motivo mostra-se inviável impor aos provedores que atuam na Internet o dever de verificar a autenticidade da identidade de todos os usuários que utilizam seus serviços, uma vez que uma atividade como essa acumula uma grande quantidade de informações. Diante disso, não se mostra desarrazoada a atitude do provedor que apenas retém os dados que é obrigado por determinação legal.

Nesse ponto, o maior impasse talvez seja em relação a requisição de dados pessoais, uma vez que os agentes privados não são obrigados a captar e nem armazenar esses dados fora das hipóteses legalmente previstas. Aliás, nota-se que a legislação, a bem da verdade, limita a coleta de dados e incentiva a exclusão deles, como depreende-se do art. 7º, incisos VIII, IX e X, do Marco Civil da Internet, bem como dos arts. 7º a 10, 15 e 16 da Lei Geral de Proteção de Dados Pessoais (LGPD) (MOURA; BARBOSA, 2020a).

Diante disso, não é razoável compelir o provedor a mudar a sua política de coleta e armazenamento de dados para além daquilo que já é previamente definido. Por exemplo, se

determinado serviço de troca de mensagens adota como sua política eliminar as mensagens logo após elas serem entregues, não seria possível impor que ele realizasse um *backup* dessas informações. Nessa mesma linha, não se deve requisitar dados que não são coletados ou já foram excluídos[131].

Ainda sobre os arts. 13 e 15 do MCI, importante frisar que cabe ao administrador do sistema do respectivo provedor manter os registros de conexão, sob sigilo, em ambiente controlado de segurança, de tal modo que apenas a parte interessada poderá requerer ao juiz a disponibilização desses dados[132] (SIMÕES; SIMÕES, 2019).

Destaque-se que a guarda desses dados se encontra em consonância com a LGPD, haja vista que conservação de dados é autorizada para o cumprimento de obrigações legais ou regulatórias, mesmo que seja reconhecido que, em regra, é direito do titular dos dados a eliminação dos seus dados da base de dados do agente de tratamento[133].

Além de tudo colocado, também é válido diferenciar o registro de conexão dos registros de acesso a aplicações de Internet para fins de guarda. Para tanto, cabe mencionar o art. 5º, do Marco Civil da Internet, que dentre as várias definições legais, no inciso VI, esclarece que o registro de conexão é "[...] o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (BRASIL, 2014).

Partindo dessa definição, nota-se que os registros de conexão revelam os rastros (horário e data) deixados na porta de entrada (*login*) e de saída (*logout*) da Internet. Esses dados acabam em posse dos provedores de conexão, os quais atuam nas camadas física e lógica da rede para prover conexão ao internauta por meio do protocolo IP (BIONI, 2021).

Já no que diz respeito aos registros de acesso a aplicações de Internet, o inciso VIII do mesmo artigo quinto do MCI, os define enquanto "[...] o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (BRASIL, 2014).

---

[131] Contudo, se o dado for coletado e se encontrar armazenado no momento da requisição, não haveria óbice para o acesso a esses dados. Dentre esses dados, ganham destaque os dados relacionados à localização do indivíduo e o histórico de pesquisa do usuário (MOURA; BARBOSA, 2020a).

[132] Ademais, pode-se dizer que essa preocupação em torno desses dados decorre, como já visto no capítulo anterior, do fato de que tais dados representam dados pessoais, inclusive, podendo assumir a faceta de dados sensíveis (MENKE; GOULART, 2021).

[133] Aliás, em regra, os dados pessoais devem ser eliminados de forma automática ao término do tratamento de dados, segundo o disposto no art. 16, *caput* da LGPD (LIMA; RAMIRO, 2020).

Em posse de tais dados, torna-se possível identificar o computador conectado à Internet e, em tese, o seu usuário[134]. Depreende-se que essa é uma das motivações para a imposição do regime de guarda dos registros de conexão e aplicação, já que dificilmente seria possível identificar a autoria dos atos praticados no ambiente digital sem eles[135].

Seguindo essa mesma linha de pensamento, editou-se a Lei nº 12.850/2013 (crime organizado), a qual impõe às empresas telefônicas o dever de manutenção dos dados referentes à origem e ao destino das chamadas pelo período de cinco anos (art.17), de forma que seja possível a solicitação de tais dados pelas autoridades policiais e pelo Ministério Público, sem uma reserva jurisdicional expressa (art. 15) (ABREU; ANTONIALLI, 2017).

Além disso, complementa a referida lei, em seu art. 21, que a recusa ou omissão de dados cadastrais, informações, documentos ou registros no curso da investigação ou do processo requisitados pelo juiz, Ministério Público ou delegado de polícia constitui crime, com pena de reclusão de 6 meses a 2 anos, e multa[136] (ABREU; ANTONIALLI, 2017).

Também cabe ressaltar que há previsão legal similar na Lei nº 9.613/1998 sobre lavagem de dinheiro (art. 17-B), haja vista que é autorizado ao Ministério Público e as autoridades policiais o acesso aos referidos dados "[...] mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradoras de cartão de crédito, independentemente de autorização judicial [...]" (FRANCISCO; VENTURINI, 2019, p. 294).

Destaque-se que essas leis vieram para tentar superar a controvérsia que existia em relação à possibilidade de quebra de sigilo de dados cadastrais sem autorização judicial. Anteriormente, a autoridade policial realizava a solicitação com base no art. 6º do Código de Processo Penal, inciso III, o qual permitia à autoridade policial a possibilidade de colher todas as provas a serem utilizadas para o esclarecimento do fato, bem como das circunstâncias (ABREU; ANTONIALLI, 2017).

Já o Ministério Público fundamentava a solicitação com base no art. 8º, inciso IV, da Lei Complementar nº 75/93, o qual possibilita a requisição de informações e documentos a

---

[134] Destaca-se que, caso não haja a guarda desses dados, a identificação dos internautas se torna praticamente impossível (YAMAGUCHI, 2021).

[135] Nesse sentido, nota-se a utilização dos "rastros" digitais, os quais se referem a tudo que é transmitido na Internet, ou seja, ao conteúdo digital (camada de conteúdo), como as postagens em redes sociais, as mensagens de e-mail, os textos de blogs etc. (BIONI, 2021).

[136] Diante do permissivo legal, nota-se que essas autoridades têm requisitado também os registros telefônicos (e até mesmo dados de localização), independentemente de autorização judicial. Mencione-se que essas requisições diretas são realizadas com a advertência de que, caso não colaborem, podem ser punidos (ABREU; ANTONIALLI, 2017).

entidades privadas, desde que a requisição seja no exercício regular das atribuições. Tal norma era aplicada subsidiariamente aos órgãos estaduais (ABREU; ANTONIALLI, 2017).

Inclusive, a legislação processual penal é expressa ao garantir a possibilidade da requisição judicial dos dados de localização das vítimas e dos suspeitos de crimes relacionados ao tráfico de pessoas (art. 13-B do Código de Processo Penal), mas admite a solicitação direta pelo delegado ou promotor, em caso de demora (art. 13-B, § 4º, do Código de Processo Penal)[137] (MOURA; BARBOSA, 2020a).

Ressalte-se que esses dados de geolocalização das pessoas monitoradas se mostram de suma relevância para o esclarecimento de fatos. Por exemplo, esses dados podem ser solicitados pela autoridade policial quando surgir a suspeita que determinado indivíduo teve participação no cometimento de algum ilícito. A partir da solicitação, repassa-se ao solicitante as informações de geolocalização que permite determinar se a pessoa suspeita estava ou não presente ou próxima do local investigado em determinado dia e hora (PIMENTA; PIMENTA; DONEDA, 2019).

Diante disso, fica evidente a importância da utilização de metadados de localização para fins jurídicos, inclusive os provenientes do setor de telecomunicações. Desse modo, em muitos casos, metadados de telecomunicações armazenados por empresas privadas transitam do setor privado para o público por imposição legal[138].

Levando em consideração isso, percebe-se que o dever legal de guarda de dados se estende tanto aos provedores que atuam na Internet como às companhias telefônicas. Neste último caso, observa-se que as empresas telefônicas não apresentam o hábito de resistir às requisições judiciais, o que difere dos provedores de aplicações na Internet que, geralmente, alegam a defesa da privacidade dos clientes para negar as requisições[139] (MOURA; BARBOSA, 2020a).

Portanto, depreende-se que alguns provedores da Internet, bem como as operadoras de telecomunicações representam alguns intermediários que são obrigados a guardar dados dos usuários nos casos e nos limites previstos em lei. Nesse sentido, ao contrário do que se

---

[137] Mencione-se que essa inovação legislativa, trazida pela Lei nº 13.344/2016, não impõe muitos obstáculos para a requisição, haja vista que basta a indicação do nome da autoridade requisitante, unidade de polícia responsável e número do inquérito. Ademais, o prazo para atendimento da requisição também é esguio, apenas 24h (ABREU; ANTONIALLI, 2017).

[138] Isso se torna complexo pela proteção que existe sobre a inviolabilidade e o segredo das comunicações. Aliás, essa garantia está presente no art. 3º, inciso V, da Lei n. 9.472/1997 (rege as telecomunicações), bem como no Marco Civil da Internet, em relação às comunicações que ocorrem no ambiente virtual (SILVA; MOURA, 2020).

[139] Nesse sentido: HC 247.331, Rel. Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 21.8.2014; AgRg no REsp 1.760.815, Rel. Min. Laurita Vaz, Sexta Turma, julgado em 23.10.2018 (MOURA; BARBOSA, 2020a).

possa pensar, nota-se que o dever de guarda vai além dos casos previstos no MCI e abrange também hipóteses previstas em outras normas, sobretudo de natureza penal. Partindo do pressuposto de que os intermediários detêm os dados que são obrigados a guardar, mostra-se interessante analisar em seguida a discussão em torno da obtenção desses dados.

4.3 COLETA DE DADOS: RESISTÊNCIA (IN)JUSTIFICADA

Os dados guardados pelos intermediários se mostram cada vez mais importantes para os mais diversos fins na seara jurídica, como a reconstituição de um fato, ou até mesmo a descoberta da identidade de um determinado usuário. Para tanto, após a guarda dos dados, nota-se que é necessário que ocorra o acesso a esses dados. Aqui surge outro ponto a ser analisado na temática da proteção de dados. Isso muito se deve, dentre outras coisas, a resistência de alguns intermediários em disponibilizar os dados captados.

Pela leitura do art. 7º, inciso VII, do MCI, depreende-se que é vedado o fornecimento a terceiros de dados pessoais, o que inclui os registros de conexão e de acesso a aplicações[140]. Desde já, frise-se que essa regra não é absoluta e comporta exceções autorizadas por lei e precedidas, de maneira geral, de autorização judicial, como se verá adiante (GAJARDONI; MARTINS, 2020).

Quanto aos destinatários da requisição na Internet, observa-se que os dados de conexão devem ser requisitados ao provedor de conexão; os de aplicação aos provedores de aplicação; e os demais, preferencialmente, para o controlador, tendo em vista o seu poder de decisão quanto ao tratamento de dados, nos termos do art. 5º, inciso VI, da Lei Geral de Proteção de Dados Pessoais (LGPD). No entanto, se não for viável a requisição para o controlador, pode-se dirigir a requisição para o operador ou o encarregado[141] (art. 5º, incisos VII e VIII, da LGPD)[142] (MOURA; BARBOSA, 2020a).

---

[140] Levando em consideração isso, o art. 8º, parágrafo único, inciso I, do MCI, garante que a inviolabilidade e o sigilo das comunicações privadas não podem ser alvo da autonomia privada contratual, sendo nulas de pleno direito as cláusulas contratuais nesse sentido. Prevalece, nesse caso, o valor social que sustenta a inviolabilidade e o sigilo das comunicações e não a autodeterminação informacional (BIONI, 2021).

[141] O operador e o controlador são apontados como agentes de tratamento. No primeiro caso, nota-se a pessoa natural ou jurídica, de direito público ou privado, que age em nome do controlador. Este, por sua vez, controla os métodos e os motivos do tratamento de dados. Isto é, a função de um é executar as ordens recebidas e a do outro é definir essas ordens diretivas (LEONARDI, 2021).

[142] Como visto, depreende-se que podem figurar como terceiro no procedimento de requisição de dados todos aqueles que tenham acesso ao fluxo de dados, aos dados armazenados, ou o controlador, operador ou encarregado de dados pessoais. O grande destaque, na prática, fica a cargo dos provedores de conexão e de aplicação de Internet.

Já no que diz respeito às telecomunicações, observa-se que é possível que o acesso aos dados de localização ocorra sem o consentimento do usuário, desde que nas hipóteses legais. Isso permite que terceiros obtenham dados de identificação e dispositivos e informações de localização (DILI). Ademais, como frisado no capítulo anterior, não se pode perder de vista que esses metadados podem ser considerados informações pessoais, de tal modo que a requisição desses dados não pode ocorrer sem cuidados mínimos (SHANAPINDA, 2019).

Focando no ambiente virtual, percebe-se que os arts. 19, 22 e 23 do MCI permitem o acesso aos registros de aplicação e de conexão, mas não especificam a forma pela qual essa postulação será efetivada. Registre-se que a LGPD, por mais que seja um diploma legislativo mais recente, também não trouxe previsão legal nesse sentido, uma vez que foca mais em temas como inversão do ônus da prova, ações coletivas e até mesmo ações de regresso[143] (GAJARDONI; MARTINS, 2020).

Inclusive, ressalte-se que não há certeza no resultado de algum procedimento que vier a ser adotado, tendo em vista que, por exemplo, pode-se descobrir que a conexão partiu de uma determinada casa com acesso à banda larga. Contudo, qualquer pessoa que resida nela, ou até mesmo um terceiro, pode ser o autor do conteúdo postado (MOURA; BARBOSA, 2020a).

Desse modo, é sempre importante ter algumas cautelas. Mesmo que o provedor de aplicação disponibilize dados cadastrais, o que nem sempre ocorre, é interessante identificar o provedor de conexão responsável pelo endereço IP naquele momento do uso e obter as informações de quem contratou o serviço para que se possa evitar diligências equivocadas.

Ainda, percebe-se que esse procedimento deve ser adotado da maneira mais célere possível, tendo em vista que a providência deve ser adotada, muitas vezes, antes mesmo da citação dos possíveis réus, haja vista que o material ilícito na Internet apresenta a grande capacidade viralização e de atingir rapidamente um número significativo de pessoas.

Some-se a esse contexto a capacidade da lesão se renovar a cada dia, a cada hora e de forma exponencial. Registre-se que isso se deve, dentre outras coisas, a difusão das redes sociais (*Facebook*, *Instagram*, e *Twitter*, principalmente) e os aplicativos de comunicação (a exemplo do *WhatsApp*, com mais adeptos no Brasil), em que se estimula o compartilhamento imediato das informações recebidas (GAJARDONI; MARTINS, 2020).

---

[143] Talvez o legislador ainda não tenha se enveredado na criação de um procedimento de identificação dada a complexidade em torno do assunto. De um lado apresenta-se a pessoa interessada na quebra do sigilo, do outro o indivíduo acobertado pela proteção dos seus dados pessoais.

Tendo isso em mente, o art. 22 do Marco civil faculta a parte interessada em formar um conjunto probatório, seja em processo civil, seja em processo penal, em caráter incidental ou autônomo, "[...] requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet" (BRASIL, 2014).

Complementando o comando legal, os incisos do parágrafo único desse artigo ainda estipulam que o requerimento deve conter, dentre outros requisitos legais, sob pena de decretação de inadmissibilidade, "[...] fundados indícios da ocorrência do ilícito; justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e período ao qual se referem os registros"[144] (BRASIL, 2014).

Destaque-se que esse procedimento não é contencioso de início. Além disso, cabe ao juiz o dever de garantir o sigilo das informações recebidas, de modo que seja preservada a intimidade, a vida privada, a honra e a imagem do usuário, seguindo o que está disposto no art. 23 do Marco Civil da Internet. Para tanto, se necessário, pode-se, inclusive, decretar segredo de justiça[145] (MOURA; BARBOSA, 2020a).

Por sua vez, se o terceiro se opor à ordem, o que deve fazer na qualidade de responsável por lei ou por contrato pela guarda dos dados, tendo em vista que não é titular dos dados, o juiz pode levar em consideração as alegações e suspender a ordem, sobretudo, quando a contestação é do controlador dos dados (MOURA; BARBOSA, 2020a).

Persistindo a resistência, que o juiz repute infundada, o terceiro pode vir a sofrer as sanções previstas em lei, como a aplicação de multa diária. Nesse caso, percebe-se que o procedimento foge da ideia de um procedimento não contencioso, o que é problemático, principalmente, quando o terceiro é um provedor estrangeiro e devem ser utilizados mecanismos de assistência judiciária internacional (MOURA; BARBOSA, 2020a).

Depreende-se, desse modo, que nem sempre os dados requisitados são prestados, mesmo diante de ordem judicial. Nesse sentido, na prática, a obtenção desses registros não ocorre de maneira tão fácil como possa supor o comando legal presente no art. 22 do MCI. Em que pese o previsto na lei, alguns provedores, sobretudo que armazenam seus dados no exterior, resistem à disponibilização dos dados requisitados (SIMÕES; SIMÕES, 2019).

---

[144] Pela leitura do supracitado artigo, percebe-se que o pedido deve ser realizado pela parte interessada, o que dá a entender que não seria possível de ofício pelo magistrado ou até mesmo pelo delegado de polícia, na esfera criminal (MOURA; BARBOSA, 2020a).

[145] Aliás, por não se tratar de um procedimento contencioso, desde o início, a obtenção dos dados pode se dar pela requisição do juiz mediante ofício ou mandado, sem formalidades inerentes à citação formal. Percebe-se que o terceiro, em princípio, não é interessado nos dados disponibilizados. Caso ele compartilhe os dados, não sofrerá quaisquer ônus de sucumbência (MOURA; BARBOSA, 2020a).

A título de exemplo, percebe-se a polêmica em torno da obtenção de dados que envolvem o *Whatsapp*, a qual originou duas ações no Supremo Tribunal Federal. A primeira no bojo da Ação de descumprimento de Preceito Constitucional (ADPF) nº 403, distribuída ao Ministro Edson Fachin, e a Ação Direta de Inconstitucionalidade (ADI) nº 5527, da Relatoria da Ministra Rosa Weber.

O plano de fundo do debate gira em torno da decisão proferida em 02 de maio do ano de 2016 pelo Juízo Criminal da Comarca de Lagarto, Sergipe, o qual decretou a suspensão do aplicativo *WhatsApp* por 72 horas, em nível nacional, tendo em vista a recusa do Facebook, proprietário do *WhatsApp*, em fornecer os dados necessários à investigação criminal. A empresa alegou não possuir meios para fornecer as informações solicitadas, haja vista a criptografia dos dados, o que impossibilitaria o acesso dela própria aos dados (SIMÕES; SIMÕES, 2019).

Sem adentrar no mérito da possibilidade técnica ou não da devassa dos dados, nota-se que não há solução simples nesse caso, uma vez que, de um lado, o intermediário busca preservar seu "segredo industrial" e não abrir brechas para vulnerabilidades, protegendo a privacidade dos usuários e, do outro, as autoridades procuram meios investigativos eficazes.

Além disso, nota-se que os provedores de aplicações de Internet costumam apresentar certa resistência nas colaborações que envolvem interceptações de fluxo comunicacional, haja vista que esses provedores colocam a privacidade do usuário, justamente, como um ativo a ser valorizado (MOURA; BARBOSA, 2020a).

Aliás, levando em consideração isso, as aplicações mais sensíveis, a exemplo dos aplicativos de trocas de mensagens, privilegiam a criptografia forte, ou seja, aquela que torna impossível a decodificação da mensagem até mesmo para os provedores. Esse é o caso, inclusive, do *WhatsApp*, aplicativo de mensagens mais popular no Brasil, o qual passou a utilizar a criptografia de ponta a ponta (MOURA; BARBOSA, 2020a).

Essa técnica consiste em permitir apenas ao emissor e o destinatário ("pontas") acessar a chave criptográfica que decifra as informações enviadas. Nesse sentido, nota-se a diminuição de ameaças de pontos intermediários e até mesmo do próprio sistema do serviço de comunicação, de tal forma que o protocolo é utilizado para garantir a confidencialidade das informações de todos que tentem acessar indevidamente (MACHADO; DONEDA, 2018).

Registre-se que a criptografia não é exclusiva do provedor que presta os serviços de comunicação, haja vista que o próprio usuário pode, por sua iniciativa e risco, utilizar-se de "[...] softwares de encriptação de dados para assegurar a confidencialidade destes antes

mesmo de carregá-los aos servidores de *cloud computing*, em aplicações como Google Drive e Dropbox, por exemplo [...]" (MACHADO; DONEDA, 2018, p. 117).

Nesses casos, inaugura-se um debate complexo que gira em torno do sigilo decorrente de ferramentas tecnológicas e não da lei[146]. Na legislação e na jurisprudência estrangeira, existem caminhos antagônicos para esses casos. De um lado, aqueles sistemas jurídicos que defendem a obrigação do indivíduo de revelar a chave privada ou senha utilizadas para criptografar os dados. Do outro, aqueles que defendem a liberdade do sujeito de não ser compelido a essa divulgação, sobretudo, para não produzir prova contra si mesmo.

Para exemplificar, no Reino Unido, promulgou-se uma lei que criminaliza o não fornecimento de senhas ou chaves privadas necessárias para o acesso de dados eletrônicos que estejam criptografados e inviáveis de serem lidos de forma inteligível. A lei se aplica para fins de segurança nacional; de prevenir ou detectar crimes; e de bem-estar econômico (LEONARDI, 2012).

Já nos Estados Unidos, decidiu-se de forma contrária a esse entendimento, privilegiando a Quinta Emenda da Constituição norte-americana (proibição de testemunhar contra si mesmo). Desse modo, o indivíduo não pode ser obrigado a revelar senhas ou remover as proteções criptográficas porventura existentes (LEONARDI, 2012).

No Brasil, levando em consideração o art. 5º, inciso LXIII, da Constituição Federal, que garante o direito de não produzir prova contra si mesmo, parece que a melhor interpretação é no sentido de que o sujeito não pode ser compelido a fornecer meios que rompam a criptografia, o que deve ficar a cargo do Estado por meio da quebra do sigilo dentro dos meios possíveis.

Ademais, também é preciso levar em consideração às várias técnicas que podem ser utilizadas para investigação envolvendo a coleta de dados e informações e o quão prejudicial ela é para o usuário. Entre elas ganha destaque a *dragnet surveillance*, ou seja, "vigilância por arrastão", a qual recai sobre um número elevado de pessoas (inocentes ou não). Isso pode ser visto desde o uso de câmeras ou drones de monitoramento nas ruas até as novas formas de pedidos de quebra de sigilo de dados em massa (são requisitados dados de um número indeterminado de pessoas para fins investigativos) (ABREU, 2021).

Percebe-se que o resultado da quebra de sigilo em massa é a formação de uma "base de dados" com dados pessoais de todas as pessoas que foram objeto da requisição. Essa base será formada de acordo com os critérios investigativos adotados, por exemplo, dados pessoais

[146] Mencione-se que esse debate não será aprofundado nesse estudo, mas é digno de menção alguns casos que exemplificam a controvérsia.

de usuários que acessaram o serviço em determinado local e hora ou que pesquisaram por determinadas palavras. Uma vez cruzadas as informações obtidas e direcionado a persecução contra os suspeitos, os demais dados perdem sua relevância investigativa (MOURA; BARBOSA, 2020b).

Nesse sentido, percebe-se que devem ser tomados cuidados em relação ao sigilo desses dados que fazem parte da base de dados, principalmente por envolver terceiros inocentes[147]. Essa preocupação pode ser vista, inclusive, no art. 23 do Marco Civil da Internet e no art. 3º da Lei Complementar nº 105/2001 (quebra de sigilo de dados bancários)[148] (MOURA; BARBOSA, 2020b).

Ademais, nota-se que até mesmo o sigilo externo, ou seja, limitado o acesso apenas às partes, é insuficiente para garantir o sigilo dos dados de terceiros. Isso ocorre devido ao fato de que todos esses dados estiveram acessíveis às partes, as quais poderiam extrair todas as informações que fossem relevantes para a defesa (evitar a caracterização da condição de suspeito) ou para a acusação[149], de tal modo que, em alguma medida, o sigilo já foi violado[150] (MOURA; BARBOSA, 2020b).

Ademais, engana-se quem pensa que essa técnica não é utilizada no Brasil. Um caso emblemático que envolveu esse procedimento é o que investiga a morte da vereadora Marielle Franco. O caso foi decidido pela Terceira Seção do Superior Tribunal de Justiça (STJ), em 26 de agosto de 2020, no bojo do RMS 61.302/RJ, sob a relatoria do Ministro Rogerio Schietti.

Percebe-se que esse caso ganhou notoriedade não apenas nacional como internacional, de tal modo que o desenrolar dos fatos é de conhecimento público. Diante das poucas pistas deixadas pelos autores do delito, a autoridade investigativa pleiteou judicialmente que o provedor de aplicação de Internet Google fosse compelido a disponibilizar para a polícia e Ministério Público informações relacionadas à quebra do sigilo telemático (FACCHINI NETO, 2021).

---

[147] Por exemplo, espera-se que a base de dados deve ser armazenada com segurança para que não seja acessada por terceiros desautorizados. Para que isso aconteça, se possível, é recomendado que o armazenamento ocorra em dispositivos que não estejam conectados à rede e protegidos por criptografia (MOURA; BARBOSA, 2020b).

[148] Diante disso, essa medida deve ser adotada em casos excepcionais e com cuidados igualmente excepcionais. Justifica-se, assim, o acesso limitado ao tratamento desses dados pessoais apenas para as pessoas diretamente envolvidas em sua análise (MOURA; BARBOSA, 2020b).

[149] Evidencie-se que, diante da falta de previsão legal mais específica, pode-se adotar o que já é disposto no CPP quanto ao momento para a defesa manifestar se ainda tem interesse no uso da base de dados. Tal momento, segundo os arts. 396-A e 406, §3, do CPP, é a resposta à acusação, tendo em vista que essa é a última oportunidade para a defesa especificar as provas que deseja produzir (MOURA; BARBOSA, 2020b).

[150] Nesse sentido, os dados referentes a terceiros que não se relacionam com o processo devem ser eliminados o mais rápido possível, até mesmo porque, em tese, após o seu uso, esses dados se tornam desinteressantes tanto para defesa como para acusação (MOURA; BARBOSA, 2020b).

Importante salientar que essa quebra de sigilo telemático foi direcionado para um conjunto indeterminado de pessoas unidas por critérios geoespaciais e de tempo. A intenção da investigação era descobrir indivíduos que tivessem acessado aplicativos como Google Maps, Waze, e similares, dentro do lapso temporal e da área geográfica fixada, o que poderia levar à descoberta de potenciais suspeitos (FACCHINI NETO, 2021).

Nesses termos, a diligência foi deferida pelo Juízo da 4ª Vara Criminal do Estado do Rio de Janeiro, em 23 de novembro de 2018[151]. Posteriormente, mantida pela maioria do Tribunal de Justiça carioca. Irresignado, a Google, alegando proteger os direitos dos usuários, recorreu ao STJ que também manteve a determinação judicial[152] (FACCHINI NETO, 2021).

Ressalte-se que o caso deixou evidente um aparente conflito entre a privacidade dos indivíduos em geral, sem se falar na proteção dos dados dos indivíduos, e o interesse público na investigação realizada pelo Estado para a responsabilização de agentes responsáveis por crimes de elevada gravidade.

Saliente-se que essa decisão tomada pela Terceira Seção do STJ, regimentalmente, vincula as duas Turmas criminais do STJ, de modo que a tese fixada, teoricamente, será observada para decisões futuras. Há de pensar como a entrada em vigor da LGPD e a sua adequada regulamentação podem influenciar na possível revisão desse entendimento, haja vista que o caso foi julgado quando a lei ainda não estava em vigor e, mesmo se estivesse, por força do art. 4º, inciso III, alínea d, da LGPD, o diploma seria afastado em face da previsão de lei específica para o tratamento de dados pessoais em atividades de investigação e repressão de infrações penais (FACCHINI NETO, 2021).

Aliás, nessa decisão não foi a primeira vez que os tribunais superiores se depararam com a temática. Em casos similares, inclusive, os provedores de Internet já conseguiram melhor sorte quando se opunham às decisões tomadas, principalmente, quando as medidas adotadas são muito genéricas, de tal modo que não se deve adotar a linha de pensamento de que essas medidas podem ser efetivadas em qualquer caso e afastar a excepcionalidade dessa técnica (FACCHINI NETO, 2021).

Diante disso, quanto à busca por localização reversa (como também é conhecida), percebe-se um custo elevado aos direitos de um número indefinido de internautas. Nesse sentido, deve-se prezar pela sua utilização em casos graves e a captação deve acontecer

---

[151] Quando da decisão, asseverou-se que a proteção conferida aos dados armazenados seria mais branda em relação ao acesso ao conteúdo das comunicações, haja vista que o ordenamento jurídico brasileiro protegeria de forma diversa as informações de conexão e de acesso a aplicações de Internet (FACCHINI NETO, 2021).

[152] Mencione-se que, atualmente, esse caso aguarda julgamento no Supremo Tribunal Federal, no bojo do RE 1301250, relatoria da ministra Rosa Weber, o qual teve a sua percussão geral reconhecida (Tema 1148).

apenas dos dados imprescindíveis. Por exemplo, inicialmente se colhe a localização momentânea do aparelho e só posteriormente, fundado em outras informações, aprofunda-se nas apurações devidas.

Ainda, deve-se levar em consideração o número de usuários atingidos por aquela medida e os danos à privacidade deles, tendo em vista que, em regra, trata-se da coleta de dados de terceiros não envolvidos nas investigações, de forma que os cuidados com o sigilo desses dados e o descarte devem ser redobrados, seguindo art. 23 do MCI (MOURA; BARBOSA, 2020a).

Outro debate travado em âmbito jurisprudencial sobre a temática da obtenção de dados diz respeito à requisição efetuada contra intermediários que se encontram no exterior. Na maioria desses casos, ocorre a requisição para a filial brasileira, a qual se nega a fornecer os dados por declarar que não dispõe de sua posse, tendo em vista que, em tese, esses dados ficariam em posse da matriz da empresa no exterior.

Por sua vez, a empresa matriz, quando requisitada, também nega o acesso aos dados, sobretudo, por acreditar que só poderia ser compelida a entregar os dados por ordem das autoridades locais estrangeiras. Diante disso, travava-se a requisição, haja vista a necessidade de pedido de assistência judiciária internacional.

O STJ[153] se inclina a rechaçar essa linha argumentativa por entender que a autoridade dos tribunais brasileiros se aplica a requisição de dados à filial brasileira. Consoante o MCI, o direito brasileiro se aplica a todas as operações que tenham conexão com o território brasileiro (art. 11) (MOURA; BARBOSA, 2020a).

Um caso que se encaixa bem nesse contexto que sempre chamava atenção era da empresa Google, a qual se recusava em fornecer dados cadastrais e de conexão capazes de auxiliar na identificação dos usuários de seus serviços, argumentando, justamente, que as informações estariam na matriz, Google Inc., nos Estados Unidos. Nesse sentido, muitas ações foram propostas sem sucesso, tanto em ações promovidas por vítimas como pelo Ministério Público Federal (LEONARDI, 2012).

Essa questão apenas caminhou na direção de uma solução quando foi proposta uma Ação Civil Pública pelo Ministério Público Federal, a qual visava obrigar a referida empresa a disponibilizar os dados, sob pena de multa diária e, em caso de persistência, até mesmo a

[153] Nessa linha, Moura e Barbosa (2020a, p. 496) apontam os seguintes julgados: “Inq 784, Rel. Min. Laurita Vaz, Corte Especial, DJe 28.8.2013; RMS 53.213, Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 7.5.2019; RMS 53.757, Quinta Turma, Rel. Min. Joel Ilan Paciornik, DJe de 5.11.2018”.

dissolução compulsória da empresa, sem contar as possíveis condenações indenizatórias (LEONARDI, 2012).

Diante de todas essas sanções, a empresa se viu compelida a realizar um termo de ajustamento de conduta, em que a empresa Google Brasil Internet Ltda. assumiu a obrigação de receber todas as citações, notificações e intimações judiciais ou extrajudiciais e diligenciar junto à sociedade controladora, para que elas sejam tempestivamente processadas e cumpridas (LEONARDI, 2012).

Tal precedente firmado não significa que a análise sobre a negativa de disponibilização dos dados deva ser feita sem considerar os argumentos apresentados pelos provedores. Por exemplo, pode ocorrer o conflito de jurisdições, em que um determinado país determina a entrega dos dados enquanto outro proíbe a entrega. Quando isso acontece, o intermediário não pode cumprir, simultaneamente, as duas ordens, o que suscita a solução por meio da assistência judiciária internacional (MOURA; BARBOSA, 2020a).

Logo, depreende-se que o acesso aos dados armazenados pode vir a ser negado mesmo diante de requisição judicial. Isso ocorre pelo intermediário acreditar que a ordem, de alguma maneira, é indevida. Pelo colocado, esses atores privados argumentam, dentre outras coisas, que estão protegendo os direitos dos usuários, que não dispõem dos dados requisitados, ou até mesmo que não apresentam meios técnicos para acatar a ordem judicial. Para contornar essa situação, mostra-se prudente que se pense em um regime jurídico de obtenção de dados unificado, como será abordado a seguir.

4.4 POSSIBILIDADE DE UNIFICAÇÃO DOS REGIMES

Desde a promulgação da Constituição Federal de 1988, nota-se que podem ser encontrados na ordem jurídica brasileira, pelo menos, dois regimes jurídicos de obtenção de dados. Um ligado ao acesso do fluxo informacional, e o outro vinculado ao acesso dos dados armazenados. No primeiro caso, nota-se a necessidade de o acesso ocorrer por algum intermediário, nos moldes já mencionado. No segundo, o acesso pode se dar tanto com o auxílio do intermediário como diretamente no dispositivo informático[154].

Diante disso, percebe-se que a proteção conferida aos dados no Brasil varia em níveis, o que já foi abordado no capítulo anterior. Em primeiro plano, aparece a proteção ao fluxo de dados, o qual só pode ser obtido por meio da interceptação e presentes os requisitos

[154] O acesso direto ao dispositivo informático pode ser útil em casos como o do aplicativo *WhatsApp*, em que o sigilo se mostra praticamente inquebrável devido à criptografia, de tal modo que só seria possível chegar a informações desejadas diretamente no aparelho apreendido.

legais e constitucionais, como a ordem judicial. Um nível abaixo, aparecem os dados armazenados, os quais podem, em determinados casos, ser acessados até mesmo diretamente pela autoridade competente, em que pese a sua aptidão de revelar até informações sensíveis sobre o titular dos dados[155].

Quanto à interceptação, nota-se que a proteção conferida pelo ordenamento jurídico brasileiro é sobre a comunicação de dados entre dois dispositivos ou sistemas computacionais[156]. Inclusive, essa comunicação está sob o manto do art. 5º, inciso XII da Constituição Federal, o qual assegura ser inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, ressalvando no último caso aquelas quebras que ocorrem para investigação criminal ou instrução processual penal, desde que por ordem judicial[157] (MOURA; BARBOSA, 2020a).

Mencione-se que estão protegidos tanto os dados que se referem à comunicação que ocorre de maneira perceptível aos usuários (texto, voz, imagens etc.), como os dados que são trocados por sistemas computacionais. Tais dados, muitas vezes, são trocados sem que o internauta tenha plena consciência do fluxo informacional, como em casos de atualizações automáticas de software (MOURA; BARBOSA, 2020a).

Na realidade brasileira, a interceptação pode ocorrer diretamente pelas autoridades competentes ou com o apoio de terceiros. Mencione-se que qualquer terceiro que tenha acesso ao fluxo informacional pode ser requisitado para apoiar a medida adotada. Percebe-se que esse papel, na maioria das vezes, fica a cargo dos provedores de conexão e de aplicações da Internet[158]. Em qualquer caso, faz-se necessária a autorização judicial, a qual deve indicar a forma pela qual a diligência será realizada, consoante o art. 5º da Lei das Interceptações Telefônicas (MOURA; BARBOSA, 2020a).

Por sua vez, os dados digitais armazenados em dispositivos locais ou na nuvem recebem um regime jurídico de proteção diferente. Inicialmente, cabe ressaltar que essa proteção conferida decorre do direito à inviolabilidade da intimidade e da vida privada,

---

[155] Não por outro motivo se torna cada vez mais comum a requisição de dados, entre eles os pessoais, e mais custosa a interceptação do fluxo de dados (MOURA; BARBOSA, 2020a).

[156] Em relação ao fluxo de dados na Internet, importante frisar que os provedores também devem observar o princípio da neutralidade da rede, o qual determina que as informações precisam ser transmitidas de maneira igualitária, ou seja, sem discriminação quanto à origem, ao destino, ao conteúdo etc. (LIMA, 2018).

[157] Seguindo o comando constitucional, o legislador ordinário editou a Lei 9.296/1996 que versa sobre as interceptações telefônicas, a qual, em seu art. 1º, parágrafo único, delimita o âmbito de aplicação da norma a interceptação das comunicações em sistemas informáticos e telemáticos (MOURA; BARBOSA, 2020a).

[158] É válido destacar que os usuários utilizam vários provedores durante as atividades diárias (um ligado à rede doméstica, outro no trabalho, a própria rede móvel no aparelho telefônico, os acessos via *wi-fi* em espaços públicos etc.). Diante disso, há o risco de grande parte da comunicação ficar perdida ou sem utilidade, caso seja realizada a interceptação em apenas um dos provedores (MOURA; BARBOSA, 2020a).

conforme disposto no art. 5º, inciso X, da Constituição Federal, e não propriamente do art. 5º, inciso XII, do texto constitucional, o qual se aplica aos casos de interceptação (MOURA; BARBOSA, 2020a).

Nesse sentido, os dados digitais armazenados são invioláveis, ainda que não comunicados (íntimos) ou não ligados à Internet, como em redes internas ou mesmo sem conexão. Ademais, a proteção independe do local em que os dados estão armazenados, seja no computador do indivíduo, seja em provedores que fornecem o serviço de nuvem.

Devido ao fundamento constitucional diferente, observa-se que muitos defendem que não se aplicam à proteção dos dados armazenados as restrições presentes no art. 5, inciso XII, da Constituição Federal, bem como as restrições presentes na Lei das Interceptações Telefônicas (MOURA; BARBOSA, 2020a).

Além disso, como já mencionado, a proteção conferida aos dados cadastrais e aos registros de acesso e de conexão é mais modesta em relação àquela conferida à interceptação das comunicações. Por exemplo, conforme o §3, do art. 10, do MCI, a garantia de proteção de dados pessoais e de comunicações privadas não obsta a requisição administrativa de dados cadastrais pelas autoridades competentes, desde que ocorra na forma da lei (BRASIL, 2014).

Inclusive, diante dessa relativização à proteção de dados, o decreto nº 8.771/16, que regulamentou o Marco Civil da Internet, complementou que são dados cadastrais aqueles que se refiram à filiação, ao endereço, à qualificação pessoal (nome, prenome, estado civil e profissão). Ademais, no ato da requisição a autoridade indicará o fundamento legal e a motivação para o pedido (art. 11), de tal modo que os órgãos da administração federal devem publicar estatísticas sobre pedidos anualmente (ABREU; ANTONIALLI, 2017).

Desse modo, depreende-se que a característica marcante da intercepção é a captura das informações em tempo real. Por sua vez, caso os dados sejam adquiridos após o armazenamento em algum dispositivo, não se estará mais diante de uma interceptação, mas sim de uma quebra de sigilo de dados, a qual ocorre por meios próprios, a exemplo da busca e apreensão digital ou requisição a terceiros.

Nesses termos, nota-se uma distinção feita em relação à maneira de obtenção dos dados armazenados, se por meio de um terceiro ou diretamente no dispositivo informático. Do ponto de vista da legislação infraconstitucional, pode-se aplicar, sobretudo, duas legislações. Quando o acesso é por meio de um intermediário, o qual detém os dados (a exemplo dos provedores de aplicações de Internet), aplica-se o Marco Civil da Internet, nos termos já apresentados. Por outro lado, se o acesso for direto ao aparelho apreendido, deve-se observar

as normas presentes no Código de Processo Penal, como aqueles relativos à busca e apreensão (arts. 240 a 250) (ABREU; ANTONIALLI, 2017).

Essa última hipótese ocorre, muitas vezes, quando as autoridades realizam prisões em flagrante e surge a necessidade de colher os elementos de prova relacionados ao crime. Nesse cenário, nota-se a dúvida sobre a possibilidade de acesso aos dados armazenados em celulares portados pelos presos.

Inicialmente, entendia-se que as provas colhidas por meio das informações presentes em celulares apreendidos durante a prisão em flagrante eram lícitas. Inclusive, posicionou-se nesse sentido o STF ao negar o HC 91.867/PA em 2012 sob a relatoria do Ministro Gilmar Mendes[159] (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

O marco para a virada desse entendimento é apontado por muitos como o posicionamento adotado no Recurso em Habeas Corpus nº 51.531/RO, julgado em 2016, em que a 6ª (sexta) Turma do Superior Tribunal de Justiça (STJ) considerou ilícita a devassa direta dos dados, mesmo em caso de flagrante, tendo em vista a necessidade de ordem judicial para preservar os direitos do agente (MOTTA, 2019).

Destaque-se que o STJ não proibiu a apreensão do dispositivo no momento da prisão em flagrante, mas apenas estipulou que o acesso aos dados e conversas presentes nele só podem ser conhecidos forçadamente mediante ordem judicial, haja vista o sigilo das comunicações e a privacidade do indivíduo.

Seguindo essa linha, o ministro relator Nefi Cordeiro defendeu a tese de que a ilegalidade do acesso às mensagens do *WhatsApp* sem prévia ordem judicial decorria da violação ao sigilo das comunicações e à intimidade e à vida privada, utilizando, além do texto constitucional, as normas infraconstitucionais presentes na Lei de Interceptações, Lei de Telecomunicações e o Marco Civil da Internet (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

Registre-se que a mudança do entendimento também decorre das mudanças tecnológicas presenciadas. Ora, agora o objeto em análise são *smartphones* que produzem e armazenam grandes quantidades de dados, de tal modo que a devassa desses dados pode caracterizar a quebra de sigilo de dados se não for precedida das devidas cautelas, como autorização judicial (ABREU; ANTONIALLI, 2017).

---

[159] Nota-se que a argumentação adotada girava em torno da não aplicação do sigilo das comunicações presente no texto constitucional (art. 5º, inciso XII, da Constituição Federal) ao caso de comunicações armazenadas (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

Por sua vez, nota-se que as decisões tomadas pelos tribunais superiores demoram certo tempo para serem aceitas em nível local. Uma pesquisa jurisprudencial realizada demonstra isso[160]. No estudo, notou-se muitas decisões que continuaram considerando válida a colheita das provas em caso de prisão em flagrante. O argumento que prevalece nessas decisões é emprego o art. 6º do Código de Processo Penal, o qual autoriza a autoridade policial a apreender objetos relacionados ao fato e colher as provas disponíveis que possam ser utilizadas para esclarecer o fato e suas circunstâncias (art. 6º, incisos II e III) (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

Mencione-se que o entendimento firmado pelo STJ no HC 51.531/RO não foi totalmente esquecido pelos demais órgãos julgadores. Em alguns julgados, percebe-se que ele foi afastado, seja pelo entendimento contrário ao STJ, seja por não considerar que ele se aplica ao caso concreto, seja pela aplicação da teoria da descoberta inevitável (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

Diante disso, nos casos em que a prova foi considerada lícita pelos tribunais, o ponto central da discussão foi o debate sobre a extensão e a aplicabilidade das garantias do sigilo das comunicações e da proteção à intimidade e vida privada. Ademais, também foram levados em consideração alegações de suposto consentimento do acusado e os argumentos que giravam em torno do princípio do prejuízo.

Por sua vez, quando da decretação da ilicitude da prova colhida, observa-se que o HC 51.531/RO serviu como fundamento em 100% dos casos. Assim, entende-se que o acesso direto às mensagens presentes em aparelhos celulares, sem ordem judicial prévia, viola o disposto no art. 5º, incisos X e XII, da Constituição Federal (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

Todavia, é interessante notar que esses acórdãos não reviveram o debate em torno da distinção entre a proteção das comunicações armazenadas e do fluxo informacional, pelo menos não de maneira expressa. Em uma hipótese, o debate chegou a ser suscitado, mas a decisão foi no sentido de que os dados acessados no celular eram protegidos pelo sigilo da "comunicação de dados" (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

---

[160] Destaque-se que essa pesquisa elegeu como método de pesquisa a consulta e análise de decisões judiciais nos sites de alguns tribunais estaduais (São Paulo, Amazonas, Roraima, Rio Grande do Norte, Rio Grande do Sul, Paraná, Ceará, Mato Grosso do Sul, Goiás e Rio de Janeiro). Tais tribunais forma selecionados para abranger todas as regiões do país. Ademais, foram utilizados os termos de pesquisa "quebra E sigilo E Whatsapp". Após, foi realizado um segundo filtro que selecionou apenas os casos em que o acesso aos celulares ocorreu em abordagens policiais ou após o flagrante. Não foi utilizado filtro cronológico. Em síntese, essa foi a metodologia utilizada, a qual pode ser aprofundada na leitura completa da pesquisa (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

Essa tendência de mudança de posicionamento também foi acompanhada pelo STF, como se depreende do HC nº 168.052/SP, cuja relatoria, justamente, foi do ministro Gilmar Mendes. Nessa oportunidade, reconheceu-se que a jurisprudência do Supremo era no sentido de não abraçar os dados registrados como merecedores da proteção conferida à inviolabilidade das comunicações. Todavia, como pontuou o relator, várias modificações fáticas e jurídicas (promulgação de novas leis) levaram a constatação da ocorrência de uma mutação constitucional e a superação do entendimento anterior (SILVA; MOURA, 2020).

Nesse sentido, em caso de prisão em flagrante, mostra-se uma tendência de consolidação do entendimento do STJ no sentido de que é possível a apreensão do celular, mas as mensagens armazenadas nele estão protegidas pelo sigilo. Essa visão pode ser vista no Informativo número 593. Em igual sentido, no Recurso em Habeas Corpus nº 89.981/MG, a 5ª (quinta) Turma da referida Corte também asseverou que são ilegais as provas obtidas oriundas das mensagens arquivadas no aplicativo *WhatsApp* sem autorização judicial. Restou vitoriosa a tese que privilegia a inviolabilidade da intimidade e da vida privada (art. 5º, inciso X, da Constituição Federal)[161] (MOTTA, 2019, p. 125).

Não obstante, a mesma 5ª (quinta) Turma do STJ, no julgamento do Recurso em Habeas Corpus nº 77.232/SC, em 2017, entendeu que não configura prova ilícita o acesso às informações armazenadas no aparelho móvel, incluindo as conversas do aplicativo *WhatsApp*, sem autorização judicial específica, quando chancelada por decisão de busca e apreensão domiciliar que vise a obtenção instrumentos que interessam as investigações. Diante disso, não é necessária nova ordem judicial para acessar as informações dos celulares apreendidos, bastando a determinação de busca e apreensão (MOTTA, 2019).

Desse modo, a regra geral é a dependência de ordem judicial para o acesso ao conteúdo dos celulares apreendidos, sob pena da ilicitude da prova colhida. Tal prova apenas poderia ter sua ilicitude afastada em casos muito excepcionais devidamente fundamentados, como nas "[...] hipóteses de absoluta imprescindibilidade, caracterizada pelo risco à vida ou incolumidade física, ou, ainda, risco de perecimento de prova indispensável e insubstituível para a elucidação do crime"[162] (SILVA; MOURA, 2020, p. 426).

---

[161] Por mais que o resultado desse julgado seja muito similar ao presente no HC 51.531/RO, nota-se que a racionalidade argumentativa diverge em alguns pontos. Por exemplo, na decisão da 5ª (quinta) Turma, chama atenção o entendimento de que não seria aplicado ao caso o Marco Civil da Internet (ANTONIALLI; ABREU; MASSARO; LUCIANO, 2019).

[162] Ressalte-se que é de suma importância que o assunto seja pacificado nas Cortes, sobretudo levando em consideração as novas disposições normativas do Marco Civil da Internet e da LGPD, as quais ressignificam outros direitos como o direito à privacidade (SILVA; MOURA, 2020).

Como depreende-se desses julgados, sem dúvidas existia uma divergência muito bem definida entre o acesso ao fluxo informacional e aos dados armazenados. Contudo, com o desenvolvimento tecnológico, nota-se que um *smartphone* pode ser até mais revelador do que a gravação de uma conversa, por exemplo. Levando em consideração isso, percebe-se uma tendência de consolidação do posicionamento dos tribunais superiores no sentido aproximar esses dois regimes jurídicos.

Pensar dessa forma auxilia no fortalecimento de um microssistema de proteção de dados, em que os regimes jurídicos pudessem ser uniformizados, de tal modo que seja garantida mais segurança jurídica e o aprimoramento de pontos ainda lacunosos. Dentre esses pontos lacunosos se encontra o procedimento de obtenção de dados, como já mencionado anteriormente.

Ora, não há um procedimento expresso nem no CPC e muito menos nas legislações mais específicas, como o Marco Civil da Internet e a Lei de Proteção de Dados. A bem da verdade, notam-se várias possibilidades de providências espalhadas contra diferentes responsáveis (provedor de aplicações, provedor de conexão, ofensor). Desse modo, torna-se desafiador definir quais seriam as vias mais adequadas (GAJARDONI; MARTINS, 2020).

Ademais, a legislação também não aborda exaustivamente os parâmetros que devem ser utilizados para relativizar o sigilo dos dados armazenados. Percebe-se que o Marco Civil apenas se limita a indicar a necessidade de ordem judicial para que a quebra do sigilo ocorra, conforme depreende-se do art. 7, inciso III. Por sua vez, observa-se que o MCI direciona seu comando normativo para os dados de registro (art. 22) e pessoais (art. 10, § 1º), não de uma maneira ampla.

Frente a lacuna normativa, faz-se necessário o uso da analogia entre os procedimentos já presentes no ordenamento jurídico, nos termos do art. 4º da LINDB[163]. Inicialmente, pode-se equiparar o procedimento em questão com a busca e apreensão presente no art. 240, § 1º, do CPP, tendo em vista a familiaridade que existe entre a busca domiciliar e a aquisição de dados. Partindo disso, cabe frisar que o comando apenas autoriza a diligência caso existam "fundadas razões" que justifiquem a medida (MOURA; BARBOSA, 2020a).

Seguindo essa linha, também é possível invocar o art. 22, parágrafo único, do MCI, o qual especifica o que poderia ser entendido como "fundadas razões", haja vista a exigência da demonstração de fundados indícios da ocorrência do ilícito; da utilidade dos registros

[163] É válido destacar que essa é uma medida paliativa para a problemática, tendo em vista que o ideal é a produção legislativa específica. Por exemplo, em causas cíveis, a busca e apreensão é comum como medida de execução, mas incomum como uma nova forma de obtenção de provas (MOURA; BARBOSA, 2020a).

solicitados para sucesso da investigação ou instrução; além da delimitação do período ao qual se referem os dados (MOURA; BARBOSA, 2020a).

Ainda, unificando os regimes, pode-se suscitar a aplicação da Lei das Interceptações Telefônicas[164], principalmente, no que diz respeito aos parâmetros fixados no art. 2º para a utilização de um meio de prova tão invasivo. Primeiramente, é necessário a prova de que o alvo da quebra tenha participado do ilícito, o que pode incluir o direcionamento da medida para terceiros. Posteriormente, deve-se atentar ao fato que a utilização desse meio de prova é excepcional, ou seja, só deve ser utilizado quando não existirem outros meios menos intrusivos. Por fim, necessita-se da indicação da proporcionalidade estrita da medida (MOURA; BARBOSA, 2020a).

Em relação à proporcionalidade da medida, é importante a demonstração que a medida é adequada à instrução, ou seja, com base nos fatos já apurados, é pertinente para o resultado desejado. Atrelado a isso, deve-se comprovar sua necessidade, de tal modo que a diligência se mostre indispensável no contexto analisado, inclusive, com a indicação dos dados a serem coletados, bem como o período de coleta. Tudo isso deve ser analisado de maneira muito bem fundamentada, seguindo o que dispõe o art. 93, inciso IX da Constituição Federal (ABREU; ANTONIALLI, 2017).

Engana-se quem acha que a complexidade do tema se esgota por aqui. Vários pontos denotam muita complexidade. Exemplificativamente, nota-se que, em muitos casos, a única forma de demandar contra alguém é com a obtenção dos dados de identificação dessa pessoa, ou seja, com a quebra do sigilo, mediante uma ação no Poder Judiciário. Contudo, pode ocorrer de ser deferida a quebra e posteriormente comprovado no processo que não existia ilicitude, de tal modo que o réu acaba com os dados violados.

Levando isso em consideração, é válido destacar que medidas voltadas à identificação de determinados usuários só devem ser utilizadas quando realmente não existir outra forma para o desenvolvimento da lide[165]. Por exemplo, se não consta em determinado site a autoria direta de material impugnado, mas é possível individualizar o responsável pela

---

[164] Um dos pontos em comum dos procedimentos é que eles podem ser efetivados mediante a requisição de dados a terceiros. Isso ocorre na quebra de sigilo de fluxo telemático, de dados armazenados, dos dados pessoais, bem como dos dados cadastrais e de registro (MOURA; BARBOSA, 2020a).

[165] Percebe-se que a vedação constitucional ao anonimato não obriga, em sentido contrário, que os usuários sempre sejam identificados. Existem situações em que deve ocorrer a identificação e outros em que não deve ocorrer, a exemplo do caso do sigilo dos votos nas eleições. Inclusive, ainda pode-se falar em situações de identificação parcial, como nos casos de pseudônimos utilizados por artistas. Assim, o anonimato não deve ser visto como uma conduta que sempre visa o cometimento de ilícitos, ao passo que também pode servir para garantir direitos, dentre os quais, a privacidade e a proteção de dados (WIMMER; CARVALHO, 2022).

página, mostra-se possível demandar contra este último para identificar o primeiro, caso realmente se trate de conteúdo ilícito[166] (GAJARDONI; MARTINS, 2020).

Em tais casos, observa-se que não se trata de anonimato propriamente dito[167], haja vista que é possível identificar alguém para figurar na lide. Entretanto, em casos que não existe essa possibilidade, depreende-se que, de fato, existe um caso de anonimato, uma vez que a descoberta do autor do material impugnado se torna obrigatório para o próprio desenvolvimento do processo, sob pena de não existir a correta definição de contra quem imputar o ato ilícito.

Algumas soluções podem ser teorizadas, mesmo que apelando para uma instrumentalidade das formas e para as peculiaridades inerentes ao ambiente digital, o que não é o ideal, mas o possível. Para tanto, parte-se da premissa de que o autor da ação nos casos de requisição de dados deseja remover o conteúdo ofensivo e conseguir uma indenização por danos materiais e/ou morais.

Em linhas gerais, o procedimento de identificação gira em torno dos seguintes aspectos: a) ordem judicial direcionada ao provedor de aplicação para que seja disponibilizado o endereço IP que postou determinado conteúdo; b) ordem judicial direcionada ao provedor de conexão para fornecer os dados cadastrais e/ou a localização do dispositivo que se conectou à Internet utilizando aquele endereço IP fornecido pelo provedor de aplicação; c) cruzando as informações, a individualização do usuário que postou determinado conteúdo ou, pelo menos, do dispositivo que o fez[168] (BIONI, 2021).

Em um extremo, nota-se a possibilidade do manejo de três ações sucessivas para conseguir o objetivo citado, o que é complicado para o autor tanto pela demora como pela onerosidade. Primeiramente, maneja-se uma ação de obrigação de fazer (art. 497 do CPC) contra o provedor de aplicações para que ele seja compelido a disponibilizar os registros cabíveis para fins de identificação (geralmente, o endereço IP), cumulada com pedido para

---

[166] Quanto à caracterização do ilícito, importante levar em consideração que o anonimato online pode ser visto sob diferentes objetivos e perspectivas. Partindo disso, o anonimato pode ser utilizado, por exemplo, para protestos pelas redes sociais ou para simples navegação na rede (obtenção de conhecimento), o que não necessariamente seria ilícito (MARTINS; LAURENTIIS; FERREIRA, 2021).

[167] Nessas situações, nota-se a figura do anonimato relativo ou impróprio, uma vez que algum terceiro pode identificar ou já sabe quem é o anônimo. Por outro lado, no anonimato absoluto ou próprio, ninguém consegue identificar o sujeito anônimo (MORAES, 2012).

[168] Em igual sentido, Gajardoni e Martins (2020) sintetizam da seguinte forma: a) ajuizamento de uma ação para exclusão do conteúdo (art. 19 MCI); b) ajuizamento de uma ação para obtenção do endereço IP do provedor de aplicação (Google, Facebook, UOL etc.); c) a partir do endereço IP, ajuizamento de uma ação para obtenção dos dados cadastrais em posse de um provedor de conexão (Vivo, Claro, Oi, Net etc.). Após todos esses passos, todos sendo bem-sucedidos, consegue-se chegar ao titular da conexão que pode, eventualmente, vir a ser processado.

que o conteúdo seja retirado do ar liminarmente (art. 300 do CPC) (GAJARDONI; MARTINS, 2020).

Em posse dos registros e com a retirada do material ofensivo, parte-se para o manejo de uma segunda ação de obrigação de fazer (art. 497 do CPC) contra o provedor de conexão, para que ele indique os registros de conexão referentes aos registros de aplicação fornecidos pelo provedor de aplicação, o qual não dispõe, em regra, dos dados cadastrais dos usuários (GAJARDONI; MARTINS, 2020).

A partir desses dados, é possível identificar o computador que realizou as conexões buscadas e obter os dados da pessoa física ou jurídica responsável pela conexão. Partindo disso, pode-se individualizar uma residência (acesso local); uma empresa (acesso no local de trabalho); ou o titular de uma linha de telefonia celular (muito utilizado atualmente) (GAJARDONI; MARTINS, 2020).

Após tudo isso, com o indivíduo autor do conteúdo contestado identificado, torna-se possível o manejo da terceira ação contra ele pleiteando o que o autor entender de direito. Nessa ação também é comum, dentre outras coisas, o pedido de retratação pública (GAJARDONI; MARTINS, 2020).

Como se depreende, ao adotar tal procedimento, o autor precisa manejar três ações com um único objetivo, o qual apenas é atingido se todas as fases forem bem-sucedidas. Ademais, cada ação requer o recolhimento de custas, além da espera pelos trâmites devidos, como citação e o manejo de agravo de instrumento contra a medida liminar ou a imposição de multa diária, fora o gasto com honorários advocatícios.

Por outro lado, também é possível a junção de pedidos em uma única ação de obrigação de fazer cumulada com o pedido indenizatório por danos materiais e/ou morais (art. 327 do CPC) contra o provedor de aplicações, para que ele disponibilize os dados registrais (endereços IP), bem como providencie a retirada liminar do conteúdo (art. 300 do CPC). Essa ação é proposta já com a indicação de um litisconsórcio facultativo eventual com corréus indeterminados (art. 319, §§ 1º e 2º, do CPC), quais sejam o provedor de conexão e o possível violador da lei (GAJARDONI; MARTINS, 2020).

Ao agir dessa maneira, já se está indicando ao juízo que, após o deferimento da pretensão inicial contra o provedor de aplicação e a descoberta do provedor de conexão, deve-se diligenciar contra ele para descobrir os dados cadastrais (pessoais) do infrator e, por fim, responsabilizá-lo por seu ato.

Importante frisar que nesse extremo se reduz o número de ações, é bem verdade. Contudo, não se pode dizer que será um processo simples, tendo em vista a presença de três partes independentes na demanda e cada uma é chamada em um determinado momento para cumprir uma obrigação específica.

Talvez a alternativa mais viável, mas não menos desafiadora do ponto de vista interpretativo, seja o manejo de uma única ação indenizatória contra réus indeterminados para, dentre outras coisas que se entenda de direito: retirada do material ofensivo e recebimento da indenização devida, seguindo o que dispõe o art. 319, §§ 1º e 2º, do CPC. Ao adotar esse procedimento, apenas figura como parte o autor do material contestado, o qual responde nos termos das leis específicas (Marco Civil da Internet e Lei Geral de Proteção de Dados), bem como do Código Civil (artigos 186 e 927) (GAJARDONI; MARTINS, 2020).

Nesse caso, o papel dos provedores é de terceiros que auxiliam no processo e não de partes. Com isso, os provedores são requisitados por meio de ofícios para que revelem a identificação do IP e retirem o conteúdo (provedor de aplicação), e apresentem os dados cadastrais do agente violador (provedor de conexão). Feito isso, o autor pode emendar a petição inicial e consolidar o polo passivo da demanda com a pessoa individualizada pelas respostas dos ofícios dos provedores[169] (GAJARDONI; MARTINS, 2020).

Ademais, a colocação dos provedores como terceiros parece ser mais assertiva em relação ao que se depreende dos artigos 18 e 19 do Marco Civil da Internet, tendo em vista que, em regra, esses provedores não respondem pelo conteúdo gerado por terceiros, de tal modo que eles são requisitados com base nos parágrafos do art. 19 e nos arts. 22 e 23 do MCI para colaborar com a investigação e não para figurar no polo passivo da demanda, como detalhado anteriormente.

Esse ponto que versa sobre qual o local que o provedor deve assumir nas demandas que requisitam dados é igualmente controverso. Em outras palavras, a dúvida gira em torno se os provedores que atuam na Internet devem ser demandados como partes ou devem ser entendidos como terceiros que colaboram com o desenrolar da lide.

Nesse sentido, tomando como base o Recurso Especial nº 1.851.328/RJ, percebe-se que o provedor de aplicação Google (um dos maiores do mundo), nesse caso, assumiu a postura de defender o conteúdo impugnado no processo, o qual foi veiculado por intermédio

[169] Esse procedimento se mostra mais cômodo para o autor, que apenas maneja uma ação, e para os provedores que não figuram como parte, de modo que não pagam custas ou precisam se preocupar com a contratação de advogados (GAJARDONI; MARTINS, 2020).

do seu serviço de hospedagem de blogs. Ou seja, atuando como se fosse parte no processo (RIBEIRO, 2021).

A empresa alegou, no momento da defesa, que o conteúdo ofensivo havia sido proferido durante uma discussão inflamada sobre duas posições que sustentavam pontos de vista antagônicos, de tal modo que o conteúdo gerado estava abarcado pela liberdade de expressão (RIBEIRO, 2021).

Registre-se que as teses defensivas apontadas pelo Google não foram apreciadas nem pelo magistrado nem pelo Tribunal de Justiça carioca, de tal modo que a empresa interpôs embargos de declaração, Recurso Especial e Agravo em Recurso Especial para que o tema fosse levado ao crivo do STJ, tendo em vista que o provedor de aplicação sustenta sua legitimidade em defender a legalidade do ato (RIBEIRO, 2021).

Tal Recurso Especial, sob a relatoria da ministra Nancy Andrighi, reconheceu a possibilidade de o Google defender o conteúdo publicado, haja vista que a empresa é proprietária do blog e o autor do conteúdo ofensivo não foi incluído no polo passivo do processo (RIBEIRO, 2021).

Desse modo, nota-se que o STJ entendeu legítima a defesa do conteúdo ofensivo gerado por terceiro apenas no caso desse terceiro não for parte do processo, haja vista o interesse do provedor de aplicação em que seu produto oferecido não sofra restrições indevidas decorrentes do cerceamento da liberdade de expressão.

É válido frisar que a sistemática processual brasileira apresenta limitações para que isso ocorra. Inicialmente, o art. 18 do CPC é claro ao dispor que não é lícito a parte defender em nome próprio direito alheio, tendo em vista que se presume: o interesse do indivíduo em não ver seu direito defendido por terceiro sem seu consentimento; do autor em litigar contra o real opositor (até como requisito validade do provimento); do intermediário em não ser prejudicado com o ônus excessivo de defender a si próprio e outrem na ação[170] (MELO, 2018).

Por sua vez, entende-se a posição adotada por muitos provedores de serviços da Internet que se encontram em uma situação complexa, já que eles são a primeira barreira para contraditar ordens abusivas direcionadas para seus usuários. Diante disso, ou assume esse ônus de impugnar as decisões judiciais, inclusive financeiro, ou repassa os riscos aos usuários de quebras de sigilo sem contraditório ou controle externo.

---

[170] Percebe-se que, até levando isso em consideração, o CPC restringe o alcance subjetivo dos efeitos da sentença, ao passo que a sentença apenas faz coisa julgada para as partes do processo e não beneficia nem prejudica terceiros, seguindo o comando do art. 506 do CPC (MELO, 2018).

Sobre o ônus financeiro, em alguns casos os provedores são condenados quase que automaticamente a valores sucumbenciais. Ocorre que a intervenção judicial se deu por imperativo legal e constitucional como requisito indispensável da legitimidade da quebra do sigilo. Levando isso em consideração, não foi o provedor que deu causa ao processo, mas a própria necessidade de judicialização do conflito (MELO, 2018).

Algumas alternativas podem ser idealizadas nesses casos. Nos Estados Unidos, por exemplo, adota-se o procedimento de demandar contra um "John Doe" ou uma "Jane Doe" (uma espécie de "fulano de tal", no Brasil). A primeira fase do procedimento é, justamente, desvendar a identidade do réu ("unmask John Doe"). As peculiaridades de como isso ocorre varia de acordo com o estado estadunidense (MELO, 2018).

Em linhas gerais, depreende-se que o procedimento viabiliza a tutela do direito fundamental a ser restringido (liberdade de expressão ou privacidade) e assegura os interesses daqueles ofendidos por usuários anônimos, além do que permite uma análise individualizada sobre a necessidade da requisição dos dados dos usuários.

Na realidade brasileira, alguns entes podem assumir o papel de defesa do "fulano de tal". Notadamente, observa-se que se pode aplicar nesse caso, através de mecanismos interpretativos, a situação de curatela especial, haja vista que a parte é titular de direitos, mas, no momento, não possui capacidade de estar em juízo[171]. Nesse caso, seguindo o CPC e a Lei Complementar nº 80, essa função recairia sobre a Defensoria Pública (MELO, 2018).

Repassar essa função para a Defensoria Pública, talvez seja a maneira mais plausível dentro do que é previsto pelo ordenamento jurídico brasileiro[172], levando em considerações os objetivos básicos presentes na lei orgânica do referido órgão nos artigos 3º e 4°, dentre os quais ganham relevo a primazia da dignidade humana; a garantia do contraditório e da ampla defesa; defesa de direitos fundamentais, entre outros (MELO, 2018).

Cabe ter em mente que esse procedimento necessita de uma calibragem correta, dada a complexidade em torno da temática. Ao utilizá-lo, toca-se em direitos como a privacidade, a proteção de dados, o devido processo legal e a presunção de inocência, além da honra e a intimidade possivelmente violadas. Riscos e benefícios devem ser analisados detalhadamente.

---

[171] Percebe-se que o instituto da curatela especial se encontra previsto no art. 72 do CPC e visa garantir a presença no processo de quem não poderia fazê-lo de outra maneira. No procedimento de quebra de sigilo de dados, nota-se uma impossibilidade de ordem lógica, uma vez que, caso o réu compareça ao processo de quebra de sigilo, estará violado o próprio direito que se buscava proteger (MELO, 2018).

[172] É válido frisar que, se o usuário tomar conhecimento da demanda, naturalmente, lhe é assegurada a prerrogativa de declinar da representação realizada pela Defensoria e constituir um advogado.

O fato é que, mesmo diante de todas essas complexidades, a quebra do sigilo dos dados armazenados pode ser executada pela busca e apreensão dos dados ou mediante requisição. No primeiro caso, percebe-se que os dados são acessados e copiados diretamente pelas autoridades. Já no segundo caso, nota-se que a requisição é realizada contra aquele que possui os dados[173].

Além disso, vislumbra-se que o terceiro pode ser entendido como aquele que tem o controle dos dados, o que geralmente recai sobre os provedores da Internet, mesmo que nem sempre esses provedores armazenem as informações dos seus usuários, como em casos do uso de criptografia.

Seguindo esses pontos elencados, pode-se dizer que podem ser extraídos alguns pressupostos do ordenamento jurídico para a requisição de dados armazenados. Aqueles que estão mais claros podem ser sistematizados da seguinte forma: a) indícios de participação do titular dos dados no ilícito; b) identificação precisa dos dados a serem requisitados; c) inexistência de outro meio menos gravoso; d) proporcionalidade estrita da medida, levando em consideração os direitos individuais envolvidos[174] (MOURA; BARBOSA, 2020a).

Por sua vez, para a interceptação, segundo a legislação pertinente, mostra-se necessário "[...] (i) 'indícios razoáveis' do cometimento de um crime; (ii) demonstração da inexistência de meios alternativos (necessidade); (iii) o crime investigado deve ser punível por reclusão (crime grave) (Lei nº 9296/1996, art. 2º); e (iv) limitação temporal (art. 5º)" (MELO, 2018, p. 218).

Essas são as hipóteses estudadas em que é possível o acesso a dados dos indivíduos. Depreende-se que em alguns casos a obtenção dos dados necessita da colaboração de terceiros e em outros, mais excepcionais, podem ser conseguidos diretamente no dispositivo informático. Ademais, percebe-se que há uma variação nos regimes jurídicos aplicados, o que dificulta na solução das controvérsias existentes, como a falta de um procedimento específico. Isso se mostra preocupante frente a latente violação de direitos fundamentais que pode ocorrer com o acesso aos dados dos indivíduos.

Todavia, pela análise mais detalhada da pesquisa desenvolvida neste estudo, bem como dos requisitos citados acima, observa-se que alguns pontos são comuns, dentre eles, a

---

[173] Destaque-se que a preferência é pela requisição dos dados, por questão de conveniência, tendo em vista que a busca e apreensão dos dados deve ser adotada em caso de resistência à requisição ou de risco à integridade dos dados (MOURA; BARBOSA, 2020a).

[174] Segundo Melo (2018), a jurisprudência exige que seja demonstrado os indícios que determinada pessoa participou do ilícito; indicação precisa dos fatos a serem provados e os indícios de que eles serão comprovados com os dados obtidos; a necessidade da medida; e o lapso temporal de captação dos dados.

necessidade, em regra, de alegação de participação do titular dos dados no cometimento de algum ato ilícito e a necessidade da obtenção dos dados pelos meios menos ofensivos possíveis aos direitos do indivíduo (como a indicação precisa dos dados e da finalidade; a limitação temporal; a não existência de outro meio menos gravoso, dentre outros quesitos).

Nesse sentido, cabe frisar que as mudanças experimentadas no país decorrentes das tecnologias digitais (difusão de dispositivos inteligentes que coletam dados) e das inovações legislativas (a promulgação de uma Emenda Constitucional e da LGPD) podem conduzir a junção desses regimes jurídicos, em breve. Isso se deve ao fato de os dados apresentarem o potencial de violação de direitos tanto quanto a devassa do fluxo informacional, de tal modo que se mostra plausível uma equivalência de regimes.

Portanto, nota-se que essa idealização, mesmo que incipiente, pode conduzir a ganhos futuros significativos na tutela de direitos fundamentais, sobretudo, da privacidade e da proteção de dados. Entre esses ganhos, a impossibilidade de devassa de dados, dentre outras coisas, sem ordem judicial, sem justificativa plausível, sem base legal, sem vinculação a determinadas hipóteses estanques, sem um procedimento bem definido.

5. CONCLUSÃO

O avanço tecnológico permitiu que as sociedades experimentassem um progresso significativo na criação e difusão de informações. Um meio que se notabilizou para tornar isso possível foi a Internet, em que as pessoas conseguem interagir sem tantas amarras. Com isso, surge o que muitos denominam como Sociedade da Informação, em que a informação se torna um elemento central na própria organização social. Contudo, devido essa mudança social, notabilizou-se que as normas jurídicas também deveriam mudar para se adaptar a esse novo contexto.

Diante disso, percebeu-se que o direito à privacidade recebeu várias delimitações ao longo da história a depender da perspectiva adotada. Na atualidade, não seria diferente, haja vista que esse direito fundamental assume uma visão plural e se aplica fugindo da dicotomia entre público e privado, de tal modo que se torna possível uma tutela efetiva da dignidade humana no ambiente digital.

Por sua vez, também se notou o surgimento e reconhecimento do direito à proteção de dados, o qual foi incluído, explicitamente, como um direito fundamental no texto constitucional. Tal direito se diferencia do direito à privacidade, dentre outros aspectos, pela sua dupla dimensão, isto é, tanto impede a devassa dos dados dos titulares como requer uma atuação positiva para a efetivação do direito.

O reconhecimento da autonomia desse direito fundamental ocorreu em um momento muito significativo, em que se observa o uso crescente dos dados gerados pelos indivíduos para vários fins. Para os atores privados, vislumbra-se que eles podem ser utilizados com finalidade financeira, dentro de uma lógica de capitalismo de vigilância. Já para os atores públicos, eles são de grande valia para a regulação da rede, uma vez que podem ser utilizados para identificar os usuários.

Seguindo essa linha, demonstrou-se que não é mais interessante assumir a ideia de que os dados são inofensivos, já que o cruzamento de vários dados pode revelar segredos íntimos dos sujeitos-titulares. Inclusive, isso também se aplica aos metadados, que se revelam como os dados que são ligados a determinada comunicação, mas não se confundem com o conteúdo transmitido. Desse modo, não é prudente a disponibilização de dados, públicos ou privados, sem levar em consideração as prerrogativas dos titulares dos dados.

Nessa perspectiva, a definição do que venha a ser um dado anônimo, dado pessoal, ou dado pessoal sensível, decorre da análise contextual e da vinculação que esse dado apresenta com o usuário. Ou seja, deve-se investigar se o tratamento desses dados pode

conduzir a informações particulares. Dentre essas informações particulares, nota-se que ganha relevância a própria identificação do usuário na rede, a qual se torna possível por meio dos "rastros" deixados pelos internautas.

Pensar dessa maneira também ajuda a abrir caminhos para a unificação dos regimes jurídicos envolvendo a captação, armazenamento e obtenção de dados. Destacou-se que no sistema jurídico brasileiro ainda existe pelo menos dois regimes jurídicos de obtenção de dados. O primeiro ligado às interceptações do fluxo de dados, em tempo real. Já o segundo, com o regime mais brando, aplica-se a requisição e a obtenção direta de dados armazenados nos dispositivos informáticos, seja na Internet, seja no próprio aparelho.

Como visto, a tendência é que esses regimes recebam a mesma relevância dentro da ordem jurídica brasileira, haja vista os avanços dos estudos em torno da privacidade e da proteção de dados. Inclusive, esse entendimento já é encampado em alguns casos julgados nos tribunais superiores que fizeram uma releitura das mudanças fáticas trazidas pela evolução da tecnologia e dos perigos em torno da obtenção dos dados. Isso se torna de suma relevância diante da previsão de um novo direito fundamental e da entrada em vigor de novas legislações, como a Lei Geral de Proteção de Dados (LGPD).

A partir dos resultados da pesquisa, concebe-se esse regime unificado como aquele que leva em consideração a realidade social e econômica pautada na centralidade da informação e na vigilância e se utiliza do microssistema de proteção de dados para entender o real vínculo existente entre o dado e o titular. Diante disso, propõe-se que a obtenção dos dados leve em consideração mais os riscos em torno da violação de direitos, do que propriamente a circunstância dos dados estarem em trânsito ou não.

Nesse sentido, o regime jurídico unificado de obtenção de dados seria aquele que utiliza as mesmas bases teóricas para realizar a obtenção de dados, independentemente se fazem parte de um fluxo informacional ou se estão armazenados em um dispositivo informático. Pensar dessa maneira possibilita que os problemas em torno da temática da privacidade e da proteção de dados possam se desenvolver de maneira mais uniforme.

Logo, esta é uma síntese do presente estudo, o qual não apresenta a pretensão de esgotar as possibilidades de pesquisa. A bem da verdade, a pesquisa foi formulada para chamar atenção para os questionamentos levantados, os quais podem servir de ponto de partida para novas pesquisas. Espera-se que a leitura dessa revisão bibliográfica consiga atingir tanto as pessoas que estudam esse campo de pesquisa, como possíveis profissionais que lidam, na prática, com os pontos abordados.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 587-607.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys Marcelo. **Vigilância sobre as comunicações no Brasil**. São Paulo: InternetLab, 2017. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Acesso em: 16 ago. 2022.

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science**, v. 347, n. 6221, p. 509–514, 2015.

ALONSO, Nicolás. Aplicativo de exercício mostra localização de bases secretas do exército norte-americano. **El País**, 30 jan. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/01/29/internacional/1517182703_981640.html. Acesso em: 17 ago. 2022.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza; MASSARO, Heloísa; LUCIANO, Maria. Acesso de autoridades a celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. **Revista Brasileira de Ciências Criminais**, v. 154, p. 177-214, abr. 2019. Disponível em: https://www.academia.edu/38789803/Acesso_de_autoridades_policiais_a_celulares_em_abordagens_e_flagrantes_retrato_e_an%C3%A1lise_da_jurisprud%C3%AAncia_de_tribunais_estaduais. Acesso em: 15 ago. 2022.

BARRIOS, Lucas de Góis; SANTOS, Marcelo Vinícius Miranda. Proteção de dados pessoais, plataformas digitais e aplicativos de smartphone. In: TOMASEVICIUS FILHO, Eduardo (Coord.). **A lei geral de proteção de dados brasileira**: uma análise setorial (volume I). São Paulo: Almedina, 2021. p. 203-238.

BAUMAN, Zygmunt. **Vigilância líquida:** diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BELL, Daniel. **O advento da sociedade pós-industrial**. São Paulo: Cultrix, 1973.

BELLI, Luca; FRANCISCO, Pedro Augusto; ZINGALES, Nicolo. Lei do Estado ou lei da Plataforma? Cuidado com a privatização da regulação e da polícia. In: BELLI, Luca; CAVALLI, Olga (Org.). **Governança e regulações da internet na América Latina:** análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: FGV Direito Rio, 2019. p. 447-470. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27164/Governan%c3%a7a%20e%20regula%c3%a7%c3%b5es%20da%20internet%20na%20Am%c3%a9rica%20Latina.pdf?sequence=3&isAllowed=y. Acesso em: 04 jul. 2022.

BERNAL, Paul. **Internet Privacy Rights**: rights to protect autonomy. Cambridge (UK): Cambridge University Press, 2014.

BESSA, Leonardo Roscoe; NUNES, Ana Luisa Tarter. Instrumentos processuais de tutela individual e coletiva: análise do art. 22 da LGPD. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 668-690.

BIASE, Nicholas Furlan di; AGUILERA, Daniel Fortes. Dificuldades interpretativas no regime de tratamento de dados pelo poder público. **Revista Eletrônica da Pge-Rj**, [S.L.], v. 4, n. 2, p. 1-30, 30 set. 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238. Acesso em: 13 ago. 2022.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 191-201, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimiza%C3%A7%C3%A3o_e_dado.pdf?d=637250349860810398. Acesso em: 26 jul. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BITTAR, Eduardo C. B. Regulação do ciberespaço, fronteiras virtuais e liberdade: desafios globais e atuais. **Revista de Economia e Direito,** v. 17, n.1/n.2, p. 37-79, 2012. Disponível em: https://journals.ual.pt/galileu/wp-content/uploads/2019/02/Galileu-XVII-1-2-2012-Miolo-FINAL.pdf. Acesso em: 17 ago. 2022.

BOTELHO, Marcos César; CAMARGO, Elimei Paleari do Amaral. O tratamento de dados pessoais pelo poder público na LGPD. **Revista direitos sociais e políticas públicas (unifafibe)**, v. 9 , n. 3, p. 549-580, 2021. Disponível em: https://unifafibe.com.br/revista/index.php/direitos-sociais-politicas-pub/article/view/1034/0. Acesso em: 10 ago. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 18 ago. 2022.

BRASIL. **Decreto no 8.771, de 11 de maio de 2016.** Regulamenta a Lei no 12.965, de 23 de abril de 2014. Brasília, DF: Planalto, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 17 maio 2021.

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: Planalto, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 maio 2021.

BRASIL. Senado Federal. **Parecer nº 242, de 2021.** Do plenário sobre a Proposta de Emenda à Constituição nº 17, de 2019, do Senador Eduardo Gomes e outros Senadores, que altera a

Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Senado Federal, 2021. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9029060&ts=1647557636370&disposition=inline. Acesso em: 05 abr. 2022.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF**. Relatora: Ministra Rosa Weber. Julgamento em 07/05/2020. Publicação em 12/11/2020. Brasília, DF: STF, 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 07 abr. 2022.

CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2002.

CELESTE, Edoardo; SANTARÉM, Paulo Rená da Silva. Constitucionalismo Digital: mapeando a resposta constitucional aos desafios da tecnologia digital. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 15, n. 45, p. 63–91, 2022. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1219. Acesso em: 16 fev. 2023.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção de direitos de personalidade e a responsabilidade civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, n. 3, p. 216-234, 2017. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4910. Acesso em: 15 ago. 2022.

CRAVO, Daniela Copetti. Aspectos processuais dos direitos do titular dos dados. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Org.). **Proteção de dados:** temas controvertidos. Indaiatuba, SP: Editora Foco, 2021. p. 217-237. Disponível em: https://docero.com.br/doc/881xe08. Acesso em: 05 jul. 2022.

DIEFENTHÄLER, Leonardo Perez; MALUF, Renata Chade Cattini. Lei Geral de Proteção de Dados e controle de acesso. In: TOMASEVICIUS FILHO, Eduardo (Coord.). **A lei geral de proteção de dados brasileira**: uma análise setorial (volume I). São Paulo: Almedina, 2021. p. 271-298.

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

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 15 jan. 2022.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo; MENDES, Laura Schertel Ferreira. Um perfil da nova Lei Geral de Proteção de Dados brasileira. In: BELLI, Luca; CAVALLI, Olga (Org.). **Governança e regulações da internet na América Latina:** análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: FGV Direito Rio, 2019. p. 325-343. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27164/Governan%c3%a7a%20e%20regula%c3%a7%c3%b5es%20da%20internet%20na%20Am%c3%a9rica%20Latina.pdf?sequence=3&isAllowed=y. Acesso em: 29 jun. 2022.

FACCHINI NETO, Eugênio. Limites à proteção de dados: dragnet surveillance e o caso Marielle Franco, de acordo com recente julgamento da terceira seção do STJ. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Org.). **Proteção de dados:** temas controvertidos. Indaiatuba, SP: Editora Foco, 2021. p. 238-278. Disponível em: https://docero.com.br/doc/881xe08. Acesso em: 06 jul. 2022.

FALEIROS JÚNIOR, José Luiz de Moura. A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados. In: LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coord.). **Estudos essenciais de direito digital**. Uberlândia: LAECC, 2019. p. 207-231. Disponível em: https://www.academia.edu/43479917/A_tutela_jur%C3%ADdica_dos_dados_pessoais_sens%C3%ADveis_%C3%A0_luz_da_Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados. Acesso em: 26 jul. 2022.

FALEIROS JÚNIOR, José Luiz de Moura; MARTINS, Guilherme Magalhães. Proteção de dados e anonimização: perspectivas à luz da Lei nº 13.709/2018. **Revista Estudos Institucionais**, v. 7, n. 1, p. 376-397, jan./abr. 2021. Disponível em: https://estudosinstitucionais.com/REI/article/view/476. Acesso em: 10 ago. 2022.

FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista de. O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 3, n. 8, jul./set. 2020. Disponível em: https://www.academia.edu/43789012/O_artigo_20_da_LGPD_e_os_desafios_interpretativos_ao_direito_%C3%A0_revis%C3%A3o_das_decis%C3%B5es_dos_agentes_de_tratamento_pelos_titulares_de_dados. Acesso em: 26 jul. 2022.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, **Universidade de São Paulo,** [S. L.], v. 88, p. 439-459. 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 07 abr. 2021.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. In: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 123-140.

FONSECA, Aline Klayse dos Santos; MURAYAMA, Daniela Duarte; ALMGREN, Felipe; NEVES, Raquel Marangon Duffles; MARTINS, Ricardo Maffeis. O devido processo legal à luz da Lei Geral de Proteção de Dados Pessoais e os desafios para os sujeitos processuais. In:

TOMASEVICIUS FILHO, Eduardo (Coord.). **A lei geral de proteção de dados brasileira**: uma análise setorial (volume II). São Paulo: Almedina, 2021. p. 71-83.

FRANCISCO, Pedro Augusto P.; VENTURINI, Jamila. Privacidade, vigilância e inteligência no Brasil: o marco legal e suas lacunas. In: REIA, Jhessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo. **Horizonte presente:** tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito - Fundação Getúlio Vargas, 2019. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27448/Horizonte%20presente%20%20tecnologia%20e%20sociedade%20em%20debate.pdf?sequence=1&isAllowed=y. Acesso em: 29 jul. 2022.

GAJARDONI, Fernando da Fonseca; MARTINS, Ricardo Maffeis. Direito digital e legitimação passiva nas ações de remoção de conteúdo e responsabilidade civil: discussão sobre o alcance do art. 19 da Lei nº 12.965/14. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 35-48, jan./mar. 2020. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Cad-Juridicos_n.53.pdf. Acesso em: 30 jul. 2022.

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Revista Direito Gv**, [S.L.], v. 14, n. 2, p. 513-536, ago. 2018. http://dx.doi.org/10.1590/2317-6172201821. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/77110/73916. Acesso em: 08 ago. 2022.

GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho; RODRIGUES, Luciano Ehlke. A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: os limites da intervenção do estado. **Relações Internacionais no Mundo Atual**, [S.L.], v. 2, n. 27, 25 abr. 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/3972. Acesso em: 25 jul. 2022.

LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Revista dos Tribunais, 2019.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de internet**. São Paulo: Editora Juarez de Oliveira, 2005.

LEONARDI, Marcel. Transferência internacional de dados pessoais. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 300-309.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LESSIG, Lawrence. **Code**: version 2.0. New York: Basic Books, 2006.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LIMA, Aires David; MEDEIROS NETO, Elias Marques. A eficiência do consentimento frente à (hiper)vulnerabilidade informacional do titular de dados no contexto protetivo da LGPD. **Revista Jurídica Direito, Sociedade e Justiça**, v. 9, n. 13, jan./jun. 2022. Disponível

em: https://periodicosonline.uems.br/index.php/RJDSJ/article/view/7005. Acesso em: 12 ago. 2022.

LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei n. 12.965/14). **R. Fac. Dir. Univ. São Paulo,** v. 110, p. 155-176, jan./dez. 2015. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/115489. Acesso em: 11 ago. 2022.

LIMA, Cíntia Rosa Pereira de. Os desafios à neutralidade da rede: o modelo regulatório europeu e norte-americano em confronto com o Marco Civil da Internet brasileiro. **Revista de Direito, Governança e Novas Tecnologias,** Salvador, v. 4, n. 1, p. 51-71, jan./jun. 2018. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/4235. Acesso em: 29 out. 2022.

LIMA, Cíntia Rosa Pereira de; RAMIRO, Lívia Froner Moreno. Direitos do titular dos dados pessoais. In: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 249-277.

LUZ, Pedro Henrique Machado. **Direito ao esquecimento no Brasil**. Curitiba: GEDAI/UFPR, 2019.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Caderno Especial - A regulação da criptografia no Direito brasileiro**, São Paulo, v. 1, p. 99-128, dez. 2018. Disponível em: https://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados. Acesso em: 31 jul. 2022.

MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação:** a proteção dos dados pessoais no Brasil. Porto Alegre, RS: Editora Fi, 2018. Disponível em: https://www.editorafi.org/494joana. Acesso em: 14 ago. 2022.

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

MALAR, João Pedro. Entenda o que é o metaverso e por que ele pode não estar tão distante de você. **CNN Brasil Business**, 10 set. 2021. Disponível em: https://www.cnnbrasil.com.br/business/entenda-o-que-e-o-metaverso-e-por-que-ele-pode-nao-estar-tao-distante-de-voce/. Acesso em: 29 out. 2022.

MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.** Montevideo: Fundación Konrad-Adenauer, 2005.

MARTINS, Leonardo; LAURENTIIS, Lucas Catib de; FERREIRA, Felipe Grizotto. Liberdade de manifestação do pensamento e anonimato: funções e limites dogmáticos na constituição federal. **Suprema - Revista de Estudos Constitucionais**, v. 1, n. 2, p. 75-111, 16 dez. 2021. Disponível em: https://suprema.stf.jus.br/index.php/suprema/article/view/65. Acesso em: 30 out. 2022.

MELGARÉ, Plínio. Notas sobre o direito à proteção de dados e a (in)constitucionalidade do capitalismo de vigilância. In: SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio (Org.). **Proteção de dados:** temas controvertidos. Indaiatuba, SP: Editora Foco, 2021.

MELO, Mariana Cunha e. Anonimato, proteção de dados e devido processo legal: por que e como conter uma das maiores ameaças ao direito à privacidade no Brasil. In: BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018. p. 213-232. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/Privacidade-em-perspectivas_DTP.pdf. Acesso em: 04 jul. 2022.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Justiça do Direito**, v. 34, n. 2, p. 06-51. 2020. Disponível em: http://seer.upf.br/index.php/rjd/article/view/11038. Acesso em: 17 jun. 2021.

MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Rev. Bras. Polít. Públicas,** Brasília, v. 7, n. 3, p. 184-198, 2017. Disponível em: https://www.rel.uniceub.br/RBPP/article/viewFile/4840/3636. Acesso em: 15 ago. 2022.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 350-370.

MORAIS, Paulo Francisco Cardoso de. A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores. **Portal de e-governo, inclusão digital e sociedade do conhecimento**, 31 out. 2012. Disponível em: https://egov.ufsc.br/portal/conteudo/veda%C3%A7%C3%A3o-constitucional-do-anonimato-aplicada-%C3%A0-internet-o-papel-do-estado-brasileiro-na-ide. Acesso em: 30 out. 2022.

MOROZOV, Evgeny. **Big Tech:** a ascensão dos dados e a morte da política. Trad. Claudio Marcondes. São Paulo: UBU, 2018.

MOTTA, Débora. (Ad)missibilidade da quebra do sigilo do Whatsapp na investigação criminal: à luz do princípio da privacidade. **Revista da ESMESC**, Florianópolis, v. 26, n. 32, p. 113-136, 2019. Disponível em: https://revista.esmesc.org.br/re/article/view/207. Acesso em: 28 jul. 2022.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In: WOLKART, Erik Navarro et al. (Coord.). **Direito, processo e tecnologia**. São Paulo: Thomson Reuters Brasil, 2020a. p. 473-498.

Disponível em: https://edisciplinas.usp.br/pluginfile.php/5349457/mod_resource/content/0/Textos%20prova%20digital.pdf. Acesso em: 04 jul. 2022.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Quebra de sigilo em massa e proteção de dados de terceiros: como minimizar o impacto da medida sem prejudicar a ampla defesa. In: ARAS, Vladimir Barros et al. (Org.). **Proteção de dados pessoais e investigação criminal**. Brasília: ANPR, 2020b. p. 457-478.

PIMENTA, Victor M.; PIMENTA, Izabella L.; DONEDA, Danilo. "Onde eles estavam na hora do crime?": ilegalidades do tratamento de dados pessoais na monitoração eletrônica. **Revista Brasileira de Segurança Pública**, v. 13, n. 1, p. 59-75, fev./mar. 2019. Disponível em: https://www.researchgate.net/publication/335967899_Onde_eles_estavam_na_hora_do_crime. Acesso em: 16 ago. 2022.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, v. 1, n. 1, p. 64-90. 2020. Disponível em: https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-privacidade-e-os-limites-a-funcao-fiscalizadora-do-estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/. Acesso em: 29 out. 2022.

REIS, Émilien Vilas Boas; NAVES, Bruno Torquato de Oliveira. O meio ambiente digital e o direito à privacidade diante do Big Data. **Veredas do Direito**, Belo Horizonte, v. 17, n. 37, p. 145-167. 2020. Disponível em: http://revista.domhelder.edu.br/index.php/veredas/article/view/1795. Acesso em: 20 jan. 2022.

RIBEIRO, Ricardo David. RESP 1.851.328/RJ – estudo de caso: possibilidade do provedor de aplicação defender a legalidade do conteúdo disponibilizado por terceiros em sua plataforma. In: ROCHA, Lilian Rose Lemos *et al.* (Coord.). **Caderno de pós-graduação em direito**: responsabilidade civil dos provedores de internet. Brasília: CEUB, 2021. p. 501-515.

RIHL, Rubens. A autoridade nacional de proteção de dados: evolução legislativa, composição e atuação. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 117-127, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_2_autoridade_nacional_de_prote%C3%A7%C3%A3o.pdf?d=637250344803704328. Acesso em: 29 jun. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROTH, Gabriela; NUNES, Samuel. A responsabilidade civil dos provedores por danos causados a terceiros: um estudo doutrinário e jurisprudencial do artigo 19 do Marco Civil da Internet. In: LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (Coord.). **Estudos essenciais de direito digital**. Uberlândia: LAECC, 2019.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. **Direito, Estado Sociedade,** n. 36, jan./jun. 2010. Disponível em: http://direitoestadosociedade.jur.puc-

rio.br/cgi/cgilua.exe/sys/start.htm?infoid=180&sid=18&tpl=printerview. Acesso em: 10 fev. 2022.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 190-211.

RUIZ, Evandro Eduardo Seron. Anonimização, Pseudonimização e Desanonimização de Dados Pessoais. In: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 101-122.

SANTOS, Camila Ferrão dos; SILVA, Jeniffer Gomes da; PADRÃO, Vinicius. Responsabilidade civil pelo tratamento de dados pessoais na lei geral de proteção de dados. **Revista Eletrônica da Pge-Rj**, [S.L.], v. 4, n. 3, p. 1-31, set./dez. 2021. Disponível em: https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/256. Acesso em: 12 ago. 2022.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SARLET, Ingo Wolfgang. Proteção da personalidade no ambiente digital: uma análise à luz do caso do assim chamado direito ao esquecimento no Brasil. **Espaço Jurídico Journal of Law [EJJL]**, [S. L.], v. 19, n. 2, p. 491–530, 2018. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/17557. Acesso em: 05 fev. 2022.

SHANAPINDA, Stanley. Habilitando a localização de dados para cidades inteligentes: explorando os regimes de proteção e retenção de metadados no Brasil. In: REIA, Jhessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo. **Horizonte presente:** tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito - Fundação Getúlio Vargas, 2019. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27448/Horizonte%20presente%20%20tecnologia%20e%20sociedade%20em%20debate.pdf?sequence=1&isAllowed=y. Acesso em: 29 jul. 2022.

SILVA, Alexandre Assunção e. A proteção pelo MPF dos dados pessoais dos usuários da internet. In: BRASIL. Ministério Público Federal. **Sistema brasileiro de proteção e acesso a dados pessoais:** análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3. Acesso em: 14 ago. 2022.

SILVA, Gabriela Buarque Pereira; MOURA, Tâmara. Prisão em flagrante e acesso a dados de celular: desafios entre a privacidade e a investigação criminal. In: ARAS, Vladimir Barros

et al. (Org.). **Proteção de dados pessoais e investigação criminal**. Brasília: ANPR, 2020. p. 399-430.

SIMÕES, Vanessa Fusco N.; SIMÕES, Hugo Fusco N. Desafios na obtenção da Prova nos crimes cibernéticos no Brasil: o caso WhatsApp. In: BELLI, Luca; CAVALLI, Olga (Org.). **Governança e regulações da internet na América Latina:** análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: FGV Direito Rio, 2019. p. 395-409. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27164/Governan%c3%a7a%20e%20regula%c3%a7%c3%b5es%20da%20internet%20na%20Am%c3%a9rica%20Latina.pdf?sequence=3&isAllowed=y. Acesso em: 03 jul. 2022.

SOLOVE, Daniel J. **The digital person:** technology and privacy in the information age. New York: New York University Press, 2004.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça. **Revista IBERC**, Minas Gerais, v.1, n.1, p. 01-28, nov./fev. 2019. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/6. Acesso em: 10 ago. 2022.

VALENTE, Jonas C. L. Regulando desinformação e fake news: um panorama internacional das respostas ao problema. **Comunicação Pública**, v. 14, n. 27. 2019. Disponível em: http://journals.openedition.org/cp/5262. Acesso em: 29 out. 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 131-162.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 25 jan. 2022.

WIMMER, Miriam; CARVALHO, Lucas Borges de. O papel e os limites do anonimato: em busca de uma interpretação constitucionalmente adequada. **Pensar - Revista de Ciências Jurídicas,** v. 27, n. 2, p. 01-16, 2022. Disponível em: https://ojs.unifor.br/rpen/article/view/13041. Acesso em: 30 out. 2022.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. In: DONEDA, Danilo et al. (Org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 282-299.

YAMAGUCHI, Tiago Ridek. A responsabilidade civil e o dever de guarda dos provedores de conexão de internet. In: ROCHA, Lilian Rose Lemos et al. (Coord.). **Caderno de pós-graduação em direito**: responsabilidade civil dos provedores de internet. Brasília: CEUB, 2021. p. 529-546.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2020.