O consentimento é uma base legal insuficiente para o tratamento de dados na LGPD?

Carvalho, Pedro Augusto Gil de

Universidade Estadual do Norte do Paraná

UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

CAMPUS JACAREZINHO

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA JURÍDICA

PEDRO AUGUSTO GIL DE CARVALHO

O CONSENTIMENTO É UMA BASE LEGAL INSUFICIENTE PARA O TRATAMENTO DE DADOS NA LGPD?

JACAREZINHO – PR

2024

PEDRO AUGUSTO GIL DE CARVALHO

O CONSENTIMENTO É UMA BASE LEGAL INSUFICIENTE PARA O TRATAMENTO DE DADOS NA LGPD?

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica (Área de Concentração: Teorias da Justiça – Justiça e Exclusão; Linha de Pesquisa: Função Política do Direito e Teorias da Constituição) da Universidade Estadual do Norte do Paraná, como requisito para obtenção do título de Mestre em Ciência Jurídica sob a orientação do Prof. Dr. Marcos César Botelho.

JACAREZINHO – PR

2024

Ficha catalográfica elaborada por Lidia Orlandini Feriato Andrade, CRB 9/1556, através do Programa de Geração Automática do Sistema de Bibliotecas da UENP

Carvalho, Pedro Augusto Gil de
C331c O consentimento é uma base legal insuficiente para o tratamento de dados na LGPD? / Pedro Augusto Gil de Carvalho; orientador Marcos César Botelho - Jacarezinho, 2023.
120 p.

Dissertação (Mestrado Acadêmico Direito) - Universidade Estadual do Norte do Paraná, Centro de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Ciência Jurídica, 2023.

1. Avanços tecnológicos. 2. Consentimento. 3. Lei Geral de Proteção de Dados. 4. Privacidade. 5. Tratamento de dados pessoais . I. Botelho, Marcos César, orient. II. Título.

CDD: 342.7

AGRADECIMENTO

Agradeço às autoridades da Universidade Estadual do Norte do Paraná, bem como aos responsáveis do Programa de Pós-Graduação em Ciências Jurídicas da Universidade Estadual do Norte do Paraná por todo o empenho em garantir o funcionamento do programa de mestrado na cidade de Jacarezinho/PR.

Agradeço ao meu orientador, Prof. Dr. Marcos César Botelho, que me deu o suporte com suas orientações para iniciar as leituras sobre Proteção de dados, leituras que serviram para iniciar este breve trabalho.

Agradeço a Maria Natalina da Costa, secretária do programa, por sua gentileza com todos os alunos do Programa de Pós-graduação.

Agradeço à Universidade Estadual do Norte do Paraná pela oportunidade de ser bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, CAPES. Agradeço à CAPES pela bolsa a mim disponibilizada.

Agradeço aos meus pais, porque nunca deixaram de confiar em mim, por serem meu exemplo, porque não duvidaram em estender seu apoio a mim quando decidi fazer o mestrado.

Agradeço a, pela compreensão e apoio em cada projeto que tive que viver, você fez e faz parte deles, obrigado por ser um exemplo de pessoa boa, por sua nobreza, por todo amor e estima que você me dá todos os dias, obrigado por tanto.

Aos colegas e amigos da Turma 19ª, agradeço todo o apoio que me deram nesta curta etapa do mestrado, com quem partilhamos ideias durante as aulas. Orgulho de formar parte dessa turma.

“Nós e Eles: no final das contas, somos todos homens ordinários”.

Us and Them, Pink Floyd.

RESUMO

O objetivo do trabalho é identificar se o consentimento, disposto na Lei de Proteção de Dados é uma base legal insuficiente para tratamento de dados pessoais. A sociedade contemporânea vive uma intensa interconexão, impulsionada por dispositivos eletrônicos e plataformas virtuais, que coletam vastas quantidades de dados pessoais. Essa coleta massiva de informações, denominada "economia da informação", gera riscos significativos para os direitos individuais à privacidade e intimidade. Desenvolvido na linha de pesquisa a função política do direito, esta investigação é classificada como qualitativa e será abordada fazendo-se uso do método hipotético-dedutivo. Quanto aos procedimentos técnicos a pesquisa pode ser classificada como bibliográfica e documental. O problema central consistente em questionar a suficiência do consentimento para proteger os titulares de dados, argumentando que a complexidade das aplicações e a falta de transparência podem comprometer a autonomia e controle efetivo dos indivíduos sobre suas informações. A pesquisa justifica-se pelo interesse em contribuir para a compreensão do papel do consentimento na Lei Geral de Proteção de Dados, o mapeamento de correntes de pensamento sobre seu papel legal, a reflexão sobre seus limites diante da assimetria informacional, a análise de dados sensíveis e a investigação de como o consentimento é abordado em dispositivos jurídicos acessórios, auxiliando para o entendimento do contexto legal e ético em torno do consentimento na proteção de dados pessoais, destacando desafios e propondo reflexões críticas para o desenvolvimento futuro da legislação e práticas relacionadas.

Palavras-chave: Avanços Tecnológicos, Consentimento, Lei Geral de Proteção de Dados, Privacidade, Tratamento de Dados Pessoais.

ABSTRACT

The objective of the work is to identify whether consent, as stipulated in the Data Protection Law, is an insufficient legal basis for the processing of personal data. Contemporary society lives in intense interconnectedness, driven by electronic devices and virtual platforms that collect vast amounts of personal data. This massive collection of information, referred to as the "information economy," poses significant risks to individual rights to privacy and intimacy. Developed within the research line of the political function of law, this investigation is classified as qualitative and will be approached using the hypothetical-deductive method. Regarding technical procedures, the research can be classified as bibliographic and documentary. The central problem consists of questioning the sufficiency of consent to protect data subjects, arguing that the complexity of applications and lack of transparency may compromise individuals' autonomy and effective control over their information. The research is justified by the interest in contributing to the understanding of the role of consent in the General Data Protection Law, mapping schools of thought on its legal role, reflecting on its limits in the face of informational asymmetry, analyzing sensitive data, and investigating how consent is addressed in ancillary legal devices, assisting in understanding the legal and ethical context surrounding consent in the protection of personal data, highlighting challenges, and proposing critical reflections for the future development of legislation and related practices.

Keywords: Technological Advances, Consent, General Data Protection Law, Privacy, Processing of Personal Data.

SUMÁRIO

INTRODUÇÃO

Os avanços tecnológicos de larga escala, que se difundiram no século passado, possibilitaram modificações nos paradigmas comunicacionais de forma nunca vista. Junto com outros processos sociais, como a globalização, as formas de se comunicar e informar tiveram muitas mudanças. Marcada pelo aumento da capacidade de produzir e difundir conteúdo, a chamada "era da informação" expandiu o volume de conteúdo produzido mundialmente, por meio da ampliação e da expansão do acesso à internet, que tornou o mundo hiper conectado nas últimas décadas. Essa tendência deu início a uma sociedade em rede, no qual avanços nos mecanismos de informação e comunicação geram importantes problemáticas e modificações nas relações sociais (Remédio, J.; Remédio, T.; Remédio, D., 2020).

No atual cenário, a sociedade globalizada tem uma organização da qual a informação é o elemento nuclear, seja para o desenvolvimento da economia, ou das relações sociais. Se as sociedades anteriores enfrentavam desafios físicos para se comunicar e distribuir informações, a relação tempo-espaço advinda do acesso à internet, do big data e da inteligência artificial apressou a cadência das relações sociais. Há, portanto, uma nova forma de organização social resultante da evolução tecnológica das últimas décadas, que criou mecanismos complexos e sofisticados para processar e transmitir informações em uma quantidade inimaginável e em uma velocidade jamais vista (Doneda, 2020).

A característica central dessa nova era, que já se pavimentou, é o fluxo informacional, especialmente através das redes sociais e da internet. Decerto, não é apenas no ambiente virtual que essa organização se apresenta, mas a computação eletrônica tem um grande papel no formato da experiência humana atual. É justamente essa capacidade de produzir e processar dados rapidamente que representa um desafio para muitas áreas da vida humana, inclusive a Ciência Jurídica, posto que a forma como se desenhou uma economia de dados gerou novos desafios para o Direito (Bioni, 2019).

A realidade atual envolve não apenas a produção e difusão de informações, mas o compartilhamento de muitos dados que, mesmo parecendo indispensáveis à era da informação, envolvem muita exposição de questões pessoais dos indivíduos. A problemática é que, para viver hiper conectado, é preciso ofertar uma série de dados que a economia da informação utiliza para prever comportamentos, avaliar adequação dos indivíduos para determinados serviços, indicar padrões de consumo e, efetivamente, acompanhar cada rastro que os titulares dos dados deixam em suas interações com esse cenário. Ou seja, se, por um

lado, a evolução tecnológica representou uma ampliação de possibilidades para o desenvolvimento dos indivíduos, diminuiu as distâncias físicas e tornou o acesso à informação mais democrático, por outro lado, representou riscos enormes para a pessoa humana, no tocante aos direitos à privacidade e intimidade (Remédio, J.; Remédio, T.; Remédio, D., 2020).

Os sistemas de informação, da maneira que são desenhados atualmente, entram nos mínimos detalhes da vida das pessoas, mesmo de sua vida privada. A noção de big data, em tradução literal "grandes dados" é útil para ilustrar o fato, porque há criação de bancos de dados cada vez mais extensos, com informações incontáveis sobre a vida dos indivíduos, que possuem interconexão com outros bancos de dados, para acessar informações da vida dos indivíduos de forma ampla. Para pensar a extensão do problema, deve-se imaginar a quantidade de dispositivos com os quais as pessoas se conectam hoje, em celulares, notebooks, tablets, televisões inteligentes, assistentes pessoais virtuais e outros (Mantovani, 2019).

Por meio desses dispositivos, acessam plataformas virtuais, redes sociais, aplicativos de bancos, lojas de comércio eletrônico e muitas outras plataformas sem as quais a vida na era da informação parece incompleta. Cada uma dessas aplicações acessa uma série de dados dos indivíduos, sejam informações pessoais, como data de nascimento e CPF, seja de outra natureza, como histórico de compra, preferência musical, tempo de acesso em rede e afins. Todas essas informações podem ser usadas de inúmeras formas pelas empresas, que captam até mesmo os "dados residuais" das operações para contribuir com a economia da informação.

Em 2006, Clive Humby afirmou[1] que "dados são o novo petróleo", para demonstrar como há uma economia bilionária por trás do fenômeno do big data e a capacidade de obter e processar dados é uma prioridade para as empresas que ocupam a economia digital. Na conjuntura atual, qualquer dado, mesmo aqueles que podem ser considerados como inofensivos por pessoas leigas, podem ser utilizados de forma preditiva. Especialmente porque, para grandes players da tecnologia e plataformas virtuais relevantes, a capacidade de processar e armazenar dados é uma chave fundamental para o seu sucesso. Ao mesmo tempo que, para os titulares dos dados, pode significar grandes violações.

[1] ARTHUR, Charles. Tech giants may be huge, but nothing matches big data. **The Guardian**, 23 ago. 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 4 jun. 2023.

Posteriormente, em 2017, o The Economist publicou[2] uma matéria com título semelhante à perspectiva de Humby, ao afirmar que o recurso mais valioso do mundo não é mais o petróleo, mas os dados. Considerados como a base da economia digital ou o "petróleo da era digital". Os titãs da tecnologia conservam o seu domínio justamente em cima da lucratividade de captar, armazenar, processar dados e prever tendências ou comportamentos. Essas empresas, como Google, Amazon ou Facebook oferecem serviços considerados gratuitos. Acessar o mecanismo de busca do Google não é uma operação paga, por exemplo. Porém, os usuários precisam oferecer seus dados em troca dessas informações. O que as empresas podem fazer e vender com uma simples previsão de quais pesquisas são feitas em determinada região é algo gigantesco. Nesse sentido, é preciso oferecer limites à economia da informação, para que os titulares dos dados não tenham os seus direitos violados.

Em face da problemática destacada, houve o surgimento de um grande debate acerca do direito à privacidade e sua adequação para o ambiente social e histórico que se apresenta. A privacidade como um direito fundamental é uma preocupação da Ciência Jurídica desde a reflexão proposta por Warren e Brandeis (1890), acerca do direito ao isolamento, ou *direito de ser deixado só*. A privacidade, como um tema de relevância social, não é algo novo, mas os seus contornos foram submetidos a reflexões diferentes, posto que o ambiente social atual requer uma compreensão alargada da privacidade. O direito à privacidade, submetido às reflexões sobre os avanços tecnológicos, precisou incorporar as modificações da ordem social criadas não pela tecnologia em si, mas pelos usos internos à sociedade que desenvolveu a necessidade de resguardar os indivíduos e proteger os seus dados.

O crescimento de tecnologias informacionais com grande potencial de violação de direitos colocou, para os mais diversos ordenamentos jurídicos, a necessidade de pensar como esse processamento de dados representa exposição das informações dos indivíduos. Na sociedade contemporânea, em que há grandes multinacionais da tecnologia e conglomerados com grande poder informacional, técnico e tecnológico, o indivíduo precisa ter controle sobre os seus dados, para não ser submetido a práticas abusivas. Um dos maiores objetos de preocupação da dominância dos conglomerados de tecnologia, no que se refere à proteção de dados pessoais dos indivíduos e do seu direito à privacidade e à intimidade é a assimetria informacional que existe entre as empresas e os titulares dos dados (Zuboff, 2021).

[2] THE ECONOMIST. The world's most valuable resource is no longer oil, but data. 6 maio 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 4 jun. 2023.

Grande parte da sociedade não tem o acesso adequado às informações sobre a profundidade de exposição à qual seus dados estão sujeitos, mesmo nas ocasiões em que consente com as operações, porque não dominam os conhecimentos técnicos necessários para compreender a complexidade do tratamento dos dados. As empresas, por sua vez, utilizam desse desconhecimento técnico para possuir o controle informacional. Nesse sentido, a privacidade torna-se sinônimo de autodeterminação informativa, à medida que se entende que o titular de dados deve ter acesso adequado - e facilitado - sobre suas informações, para ter controle sobre elas. O direito ao isolamento, decorrente de Warren e Brandeis (1890), se torna em controle sobre as informações e o direito à privacidade se transforma em direito à autodeterminação informativa e ao controle informacional (Rodotà, 2008). O objeto central da privacidade não é mais a propriedade, nesse cenário, mas a informação.

Como consequência das problemáticas abordadas, no campo jurídico, diversos países começaram a refletir sobre as implicações dos avanços tecnológicos, e de seus usos, para o direito à privacidade. A União Europeia possui uma diretiva acerca da proteção de dados pessoais desde 1995, a Diretiva de Proteção de Dados Pessoais (95/46/CE) que foi substituída pelo Regulamento 2016/679, ou Regulamento Geral sobre a Proteção de Dados, que opera sob a sigla GDPR – General Data Protection Regulation. O GDPR serviu e serve como base para que diversos países concebam leis de proteção a dados pessoais, pois, no âmbito da União Europeia, a discussão sobre a necessidade de que o uso e o tratamento de dados pessoais sejam feitos a partir de um padrão, que respeite os titulares, tem um longo histórico. Essa trajetória de proteção à privacidade foi incorporada ao GDPR, considerado como o regramento mais completo e sofisticado sobre o tema, fruto das reflexões e práticas da UE em torno dos dados pessoais (Monteiro *et al*., 2019).

A tutela relacionada aos dados pessoais no Brasil não possuía um marco legal até o trâmite da Lei Geral de Proteção de Dados - LGPD, embora outros dispositivos jurídicos abordassem o tema acessoriamente e pudessem ser acionados em caso de violação dos direitos. A tutela dos dados pessoais era basicamente concebida pelo Habeas Data, pelo Código de Defesa do Consumidor (Lei 8.078/1990), pela Lei de Acesso à Informação (Lei nº 12.527/2011), pela Lei do Cadastro Positivo (Lei nº 12.414/2011) e pelo Marco Civil da Internet (Lei 12.965/2014). Nenhum desses dispositivos consiste em uma lei de proteção dos dados ou se dedica a abordar dados pessoais de forma ampla, cada um deles consiste e cobre apenas alguns tipos de dados ou cenários específicos. O Marco Civil da Internet, inclusive, não tem como objetivo proteger os dados pessoais, mas funcionou como um importante elemento jurídico de controle estatal da rede (Mantovani, 2019).

Com isso, pode-se dizer que o ambiente protetivo brasileiro, no que tange aos dados pessoais, ainda era limitado, carecia de uma tutela ampla e específica para os titulares de dados pessoais, sobretudo se considerar a extensão da conectividade no Brasil. Mesmo que o direito brasileiro oferecesse, na conjuntura anterior à LGPD, uma tutela *post factum* para muitos problemas que os indivíduos enfrentavam com o tratamento dos seus dados, uma atualização do ordenamento jurídico pode ter diversas implicações. A primeira dela é oferecer respostas mais adequadas para as situações que os indivíduos enfrentam, que permitam a eles acessarem os seus direitos rapidamente. Além disso, os comandos legais servem para que os responsáveis pelo tratamento de dados tenham parâmetros sobre as suas operações, das obrigações que devem cumprir e dos direitos que possuem (Mantovani, 2019).

Com essa formulação, não há como alegar desconhecimento ou falta de diretrizes para adequação das operações que envolvem dados pessoais. A cada um dos interessados, e da sociedade como um todo, a Lei Geral está disponível. A Lei Geral de Proteção de Dados, Lei 13.709/2018, portanto, implica que o Brasil avançou em um cenário de segurança jurídica na tutela dos dados pessoais, por se dedicar exclusivamente a tratar sobre esse tema, inclusive com a exposição de diversos princípios para o tratamento dos dados e de mecanismos de prevenção de danos. A Lei, que entrou em vigor em setembro de 2020, prevê princípios, fundamentos e bases legais para o tratamento dos dados. Ou seja, hipóteses nas quais o tratamento pode ser realizado.

O consentimento, presente no art. 7, inciso I da lei, é uma das bases legais que permitem o tratamento dos dados pessoais. O consentimento integra a autodeterminação informativa, pois concebe ao titular dos dados o direito de obter informações sobre a coleta, o tratamento e a transmissão dos seus dados (Tepedino; Teffé, 2020). Ele é uma base central na LGPD. Apesar de não estar em posição hierárquica em relação às outras bases legais, a letra da lei explora a importância do consentimento em muitos incisos o que, na prática, pode demonstrar como o consentimento é um dispositivo prioritário (Bioni, 2019).

Ele é a primeira hipótese de tratamento de dados pessoais e constitui-se como uma fonte interpretativa máxima da lei (Soares, 2019). Para que o consentimento seja considerado como válido, a lei previu um conjunto de qualificadores, que devem ser corretamente aplicados pelos agentes de tratamento de dados. O consentimento é o objeto central desse trabalho, na medida que a Lei Geral de Proteção de Dados efetivamente o postula como requisito máximo para tratar dados. Porém, em um ambiente de assimetria informacional, consentir é o suficiente para a não violação dos dados dos titulares? Essa reflexão inicial inspirou o objetivo central dessa dissertação, que é analisar os limites do consentimento para o

tratamento dos dados pessoais. A pergunta que norteia essa pesquisa é: em que medida o consentimento, como base legal para tratar dados, é suficiente para proteger os dados dos titulares?

Os objetivos específicos dessa dissertação, que visam auxiliar a consecução do objetivo geral, é compreender como o consentimento é concebido pela Lei Geral de Proteção de Dados; mapear as correntes de pensamento acerca do consentimento, em termos de sua centralidade ou não na lei; refletir sobre os limites do consentimento em face da assimetria informacional; analisar a noção de dados sensíveis e os limites do consentimento para o tratamento de dados sensíveis e apresentar como o consentimento aparece no ordenamento jurídico de dispositivos acessórios que tratam de dados pessoais.

A hipótese central desse trabalho considera que o consentimento não é uma base legal superada e pode ser insuficiente para proteger os titulares de violações. Embora o consentimento figure como um dispositivo importante de autodeterminação informacional, essa autonomia pode encontrar barreiras no controle real dos dados. Ou seja, na capacidade e conhecimento técnico que o titular possui para fazer escolhas adequadas sobre os seus dados. O consentimento possui uma problemática relacionada à complexidade das aplicações, que muitas vezes impede que a transparência seja realizada de forma adequada. Os conglomerados tecnológicos podem aproveitar essa inabilidade técnica dos titulares e utilizar a sua capacidade de consentir como única ação relevante, sem se comprometer com a real transparência, que deve ser capaz de oferecer informações aos titulares dentro de uma linguagem que ele possa compreender.

Como alargamento dessa hipótese, entende-se que a assimetria informacional é configurada no desenho das aplicações. Para a utilização de muitos serviços e aplicações, os titulares dos dados precisam consentir forçadamente, do contrário são impedidos de acessar as aplicações, um tipo de prática chamada de *pegar ou largar*, que afeta a privacidade do usuário por não deixar qualquer zona de preferências. Para acessá-los, o titular dos dados deve assumir que concorda com toda a política, mesmo que ela seja abusiva, no sentido de coletar seus dados de localização, acesso à câmera, preferências de conteúdo e outras informações facilmente capitalizadas pela economia da informação. Nessas práticas, o consentimento pode não representar o controle real das informações por parte dos usuários, porque a autorização é total e incondicionada, normalmente informada pelas empresas com letras miúdas em textos gigantescos (Borgesius *et al.*, 2017).

Da mesma maneira que os termos técnicos minúsculos aparecem para o acesso em determinada plataforma, dados são coletados em outras operações com o mesmo padrão de

consentimento forçado. A necessidade de fornecer dados para compras em lojas, empresas de serviços de internet, farmácias e afins envolve não apenas o histórico do cliente em determinado estabelecimento, mas a coleta de dados residuais que podem ser utilizados para diversos fins. Uma vez que a transparência é fraca nesse relacionamento, os titulares podem consentir sem compreender exatamente com o que consentem (Modesto, 2020). O consentimento tem como necessidade fundamental uma escolha racional, informada e livre, para evitar o desequilíbrio de forças entre as partes. Como muitos sujeitos não têm a habilidade necessária para rejeitar as condições de determinados serviços e da política de privacidade de muitas plataformas, na prática, o que se vê é controle e uso indiscriminado dos dados pessoais, de forma que é fundamental modificar a própria arquitetura do consentimento nessas plataformas (Tepedino; De Teffé, 2020).

Essa pesquisa segue uma corrente hipotético-dedutiva. Essa perspectiva está assentada no tipo de raciocínio que norteia a prática da pesquisa. O método hipotético-dedutivo parte de conjecturas, ou seja, formula um problema, cria hipóteses sobre elas e submete as hipóteses à análise e provação, o que se enquadra no formato lógico proposto para essa pesquisa. Segundo Lakatos e Marconi (2003, p. 106), esse método é aquele: “que se inicia pela percepção de uma lacuna nos conhecimentos, acerca da qual formula hipóteses e, pelo processo de inferência dedutiva, testa a predição da ocorrência de fenômenos abrangidos pela hipótese”.

As escolhas metodológicas para essa dissertação visam responder ao objetivo geral proposto. Ela se insere no bojo da metodologia hermenêutica jurídica, como pressuposto para interpretar as leis que serão analisadas, em especial a Lei Geral de Proteção de Dados. A ideia de utilizar a hermenêutica para esse trabalho se justifica pela validade teórica e interpretativa de analisar as problemáticas do consentimento no ordenamento jurídico brasileiro de proteção dos dados pessoais. Utilizar-se-á o método de maneira que possa se dialogar com a norma em si e com o contexto social no qual ela se desenvolveu. A hermenêutica, para Maximiliano (2017) não é a interpretação apenas, mas a sistematização dos princípios que serão interpretados objetivamente.

Como auxiliar à hermenêutica jurídica, adota-se o método histórico, com vistas a explorar a capacidade de traçar o contexto histórico de desenvolvimento dos dispositivos, assim como explorar as correntes de pensamento jurídicas acerca do consentimento na LGPD. É possível traçar as modificações do paradigma da privacidade de dados pessoais no Brasil, assim como explorar a arena de reflexões na qual a lei se desenvolveu. Como o fazer jurídico envolve uma interpretação crítica dos dispositivos, há duas correntes de pensamento sobre o

consentimento, que terão as suas nuances exploradas no trabalho. O método histórico permite entender, como Montoro (2011) relembra, como um tema foi refletido no ordenamento jurídico em questão e suas divergências teóricas e jurídicas pós vigência da lei. Nesse caso, como o consentimento é interpretado na Lei Geral de Proteção de Dados e as discussões envolvidas no tema.

Além disso, essa pesquisa utiliza duas técnicas para a coleta dos dados que serão analisados. A primeira técnica, muitas vezes entendida separadamente como metodologia, é uma pesquisa bibliográfica sobre os seguintes tópicos: Lei Geral de Proteção de Dados, Direito à privacidade, Consentimento no Ordenamento Jurídico Brasileiro de proteção de dados e assimetria informacional. Essa pesquisa inicial deve nortear os pressupostos teóricos que guiarão o resto da pesquisa, assim como permitir a análise conjunta com as outras técnicas de pesquisa.

A pesquisa bibliográfica foi um dos passos metodológicos utilizados para essa dissertação. Consistiu em analisar minunciosamente as produções mais relevantes sobre algumas categorias de análise – ou palavras-chaves – destacadas acima, relacionadas à questão do consentimento. Essa etapa se deu por meio da coleta e análise de diversas produções científicas, como teses, dissertações, artigos científicos e livros (Lakatos; Marconi, 2003). O segundo caminho para a consecução dos objetivos foi a realização de uma análise documental da legislação sobre dados pessoais no Brasil, em perspectiva sistêmica, ou seja, relacionada com outros dispositivos do ordenamento jurídico brasileiro que versaram primeira ou acessoriamente sobre o tema. A análise documental utiliza materiais que não passaram anteriormente por nenhum tratamento, que podem ser analisados de acordo com o objetivo de cada pesquisa (Gil, 2002).

O corpus analisado para essa pesquisa documental foram algumas leis, a saber: Lei Geral de Proteção de Dados, o Marco Civil da Internet, Lei do Cadastro Positivo, assim como alguns artigos da Constituição Federal e do Código Civil do Consumidor. Essa etapa visa analisar, em sentido amplo, o estado da arte jurídico sobre dados pessoais e consentimento no Brasil, em especial como o tema do consentimento aparece na legislação brasileira dedicada a discutir dados pessoais, seja direta ou acessoriamente. Na análise documental, esse trabalho também incluiu alguns julgados do Tribunal da Justiça de São Paulo, para sinalizar como o tema tem sido tratado na prática jurídica brasileira.

Essa pesquisa está dividida em três capítulos. O primeiro capítulo trata do direito à privacidade e de como à privacidade se tornou, após a era da informação, um direito também relacionado aos dados pessoais. Dessa maneira, esse capítulo explora o direito à privacidade,

à intimidade e à personalidade, na perspectiva de sua relação com os dados. Além disso, trata de forma breve dos fenômenos do big data e da era da informação e suas implicações para a produção dos direitos relacionados à proteção dos dados pessoais.

O segundo capítulo remonta o histórico dos direitos à proteção dos dados pessoais no Brasil, com uma análise sistêmica dos dispositivos que versam acessoriamente sobre dados, como o Cadastro Positivo e o Marco Civil da Internet. Esse capítulo trata sobre o contexto de criação da Lei Geral de Proteção de Dados pessoais e das reflexões que a tornaram possível. O terceiro capítulo trata especificamente do consentimento, de seus qualificadores e problemáticas. Explora as características dos dados pessoais e dos dados sensíveis e os usos do consentimento para tratar dados. Essa seção também trata da assimetria informacional e das limitações que o consentimento representa no tratamento de dados pessoais.

1 DO DIREITO À PRIVACIDADE AOS DADOS PESSOAIS

A noção de privacidade não é um dado moderno. Esse conceito teve diversos sentidos e usos que podem ser identificados nas mais variadas épocas ao longo da história. Porém, começou a ser um elemento do ordenamento jurídico apenas no final do século XIX e suas feições se modificaram desde então, para assumir novas configurações atualmente. A concepção moderna da privacidade surgiu nos Estados Unidos, no final do século mencionado. Seu surgimento respondeu a um período histórico específico, em que a disseminação da imprensa escrita começou a implicar em eventuais equívocos e repercussões na vida das pessoas que eram alvo de reportagens jornalísticas.

A ideia de privacidade que surgiu nesse contexto teve relação direta e profunda com a necessidade de proteger a vida íntima dos sujeitos mencionados na imprensa. Embora a proteção da intimidade tenha sido abordada no direito comum[3], o debate moderno sobre a privacidade só assumiu feições mais robustas com a publicação do clássico artigo *The Right to Privacy*, de Samuel Warren e Louis Brandeis, em 1890. Em seus contornos iniciais, o direito à privacidade abordado pelos autores tinha um ideal individualista exacerbado, pois se transmitia pela ideia de ser deixado só. O paradigma da privacidade desse período postulava-o como uma relação zero, ou seja, a ausência de comunicação entre uma pessoa e todos os demais. Ela não precisava ceder o seu isolamento.

Nas palavras de Warren e Brandeis (1890), a proteção dos indivíduos, em termos de sua pessoa e de sua propriedade, é um princípio muito antigo, mas a natureza e a extensão dessa proteção precisam ser revisadas de tempos em tempos, porque as mudanças políticas sociais e econômicas criam desafios e implicam no reconhecimento de novos direitos. Eles relembram que há uma vida intelectual e emocional que, com o avanço da civilização, fora reconhecida pela sociedade, que assumiu que apenas uma parte das questões humanas são físicas, outras são de ordem emocional e exigem o mesmo reconhecimento legal de proteção.

Nessa seara da proteção da vida emocional, trataram do crescimento da invasão à vida privada e doméstica das pessoas, feitas pelos jornais, que invadem domínios "sagrados" da vida humana, que não devem ser violados. O próprio comércio da intrusão da vida alheia é tratado por Warren e Brandeis (1890) como uma intrusão muito complexa ao círculo íntimo das pessoas, que deve ser barrada. Não apenas por causar danos aos indivíduos que são alvos de tais empreendimentos, mas de todas as pessoas que podem estar sujeitas a invasões de suas privacidades. A civilização trouxe proximidade e exposição tão constante para a vida humana,

[3] Essa categoria, conhecida no inglês como *common law*, engloba um conjunto de leis decorrente das decisões de tribunais, dos precedentes legais das decisões de cortes, não mediante a criação de atos legislativos.

que é preciso conservar algum espaço onde os indivíduos possam ficar isolados. É por essa problemática que os autores defenderam a proteção legal do direito de ficar em paz, para que seja incorporado mais do que o princípio da personalidade privada, mas da inviolabilidade da personalidade.

Saito (2020) reflete que a privacidade como estabelecida pelos autores é uma manifestação de uma personalidade inerente a cada indivíduo, um domínio que não deve ser invadido por alguém. Ou seja, o indivíduo escolhe o que compartilhar, em que medida e quando, pois aspectos concernentes à sua personalidade e sua vida íntima não são públicos. Essencialmente, é um direito de exercer controle sobre as próprias informações e inibir ingerências e violações externas, com a finalidade de proteger sua integridade, seja psíquica ou emocional, posto que a violação desse direito pode deteriorar a própria personalidade do indivíduo. Em tradução literal, o "direito de ser deixado só" expressa a faculdade de não ser incomodado.

Warren e Brandeis não foram responsáveis por inventar o conceito de privacidade e lembram isso. A própria dualidade entre público e privado, que surgiu na modernidade, já se assentava sobre esse conceito, sobretudo com o fortalecimento da burguesia e a valorização do individualismo no a partir do século XVII. O que os autores fizeram foi tornar a privacidade um domínio mais extenso do que aquele relativo à propriedade, do ponto de vista físico. Propuseram-no como um direito pessoal, da proteção da personalidade inviolável. Nesse sentido, suas análises advieram de um contexto social real, da disseminação de informações pessoais dos indivíduos por jornais, o que fez com o conceito que estabeleceram tivesse ressonância prática na realidade. Da mesma forma, pode-se observar a relevância daquela compreensão do direito da privacidade para o contexto contemporâneo, em que as tecnologias da informação representam potenciais violações a elementos invioláveis dos indivíduos. Nesse sentido, o conceito desenvolvido e a problemática que o decorreu perdura até os dias atuais (Saito, 2020).

Ainda assim, não se pode omitir a feição burguesa do direito à privacidade em sua instância originária. Pelo seu grande potencial de destacar as individualidades das pessoas e principalmente pelo seu intuito, à época, de preservar não a privacidade de todos, mas principalmente da burguesia, que não queria ser exposta. Na segunda metade do século XIX, ele foi qualificado como tipicamente burguês, advindo do auge do liberalismo jurídico clássico. As elites burguesas demonstravam insatisfação com a intromissão que a imprensa representava em suas vidas privadas. Porém, um aspecto central da privacidade, que foi relevante para o exercício de direitos, é a sua importância para uma sociedade democrática,

porque preservar as informações pessoais, num contexto em que há um fluxo imenso delas, é um pré-requisito para exercer outras liberdades fundamentais (Doneda, 2020).

O caráter individualista do direito à privacidade reinou por muito tempo. Embora se entenda que a privacidade, atualmente, é algo muito mais complexo do que o direito ao isolamento e à tranquilidade, o direito à privacidade foi inserido em diversos ordenamentos jurídicos com um perfil burguês, reservado a extratos sociais específicos (Doneda, 2020). Um dos primeiros casos norte-americanos onde o direito à privacidade foi reconhecido foi Pavesich v New England Life Insurance, julgado pela Suprema Corte da Geórgia.

O caso tratava do uso não autorizado da imagem de um artista em uma propaganda feita por uma companhia de seguros. A corte decidiu, em 1905, que faz parte do direito à privacidade a faculdade de determinar qual o nível de exposição que o indivíduo deseja. Andrew J. Cobb escreveu que uns podem decidir viver uma vida de publicidade, outros podem escolher se manter reclusos e outros podem decidir uma balança entre as duas possibilidades, mas nenhuma interferência externa pode retirar o direito do indivíduo de escolher como quer ser mostrado. Até esse momento, e durante algum tempo, a tutela do direito à privacidade estava ligada a ser deixado só para decidir sobre si e sua exposição (Facchini Neto; Demoliner, 2019).

Houve um período em que a privacidade privilegiava apenas as pessoas com projeção social e financeira, sobretudo porque elas demandavam era preponderância e monopolizavam o direito à privacidade. Os tribunais acolheram, majoritariamente, esse elitismo, até a década de 1960. Ressalta-se que a década de 1960 foi um período histórico importante em muitos países, seja pelas consequências do pós-guerra, pela ascensão de movimentos sociais e pela mudança do modelo de Estado, que demandava a democratização dos direitos, como parte das reivindicações dos movimentos políticos e sociais. A partir desse momento, há uma mudança na tendência do direito à privacidade, correspondente, também, ao crescimento do desenvolvimento tecnológico, que aumentava a capacidade das pessoas de ter acesso à informação, mas também uma parcela muito maior da população enfrentava violações dos seus direitos (Doneda, 2020).

Na segunda metade do século XX, portanto, a utilização de informações pessoais dos indivíduos se tornou mais comum, especialmente pelo Estado. Nos mais diversos contextos mencionados, o Estado tinha muitas finalidades com a utilização de informações dos indivíduos, em especial para otimizar a eficiência da Administração Pública e controlar determinados índices. Em alguns contextos, significava a produção de um Estado de bem-estar social, do qual obter informações sobre a população é imprescindível. Com a expansão

de informações relacionadas com a personalidade dos cidadãos, o conceito de privacidade não se limitava mais a proteger o direito do indivíduo de ficar só e de conservar a sua vida íntima. Tornou-se, gradativamente, um direito relacionado à autodeterminação informativa, um direito de exercer controle sobre os dados que o ente estatal utilizava (Saito, 2020).

Fora da esfera estatal, o acesso a informações robustas dos cidadãos era limitado, especialmente pela desproporção que os organismos privados tinham em relação ao Estado. Não era atraente, à época, para os entes privados, realizar coleta e tratamento de dados, porque as informações pessoais não representavam uma economia frutífera. Do ponto de vista social, as informações sobre os cidadãos aumentavam o poder sobre os indivíduos e potencializava o controle social que o Estado poderia desempenhar. Porém, para os entes privados, não havia sentido em utilizar aquelas informações.

Com o avanço das tecnologias que facilitavam a coleta e o processamento de dados por entes privados, assim como com a diminuição dos custos de tratar dados, coletar informações sobre os indivíduos tornou-se útil e rentável. Ou seja, não apenas a tecnologia provocou o cenário atual, certamente, mas a sua relação com o contexto social, que resultou em uma relação potente entre informação pessoal e privacidade, em larga escala. Como dito anteriormente, informação é poder e controle, portanto um elemento essencial para definir os rumos de uma sociedade, mas a tecnologia foi responsável por intensificar os fluxos de informação, diversificar os agentes de coleta e tratamento de dados e os potenciais aos quais se destina. Tal modificação teve uma influência na relação entre poder - informação - pessoa - controle, que constituiu uma nova estrutura de poderes de acordo com a arquitetura informacional criada nesse contexto.

A primeira associação feita sobre a coleta de dados dos cidadãos era de que existia uma ligação entre progresso tecnológico e bem-estar social. As tecnologias desenvolvidas no século passado permitiam que o Estado tivesse maior conhecimento sobre a população, para promover melhoras na qualidade de vida das pessoas. Mas esse foi apenas um estágio inicial. Com o acesso do Estado a informações sensíveis dos indivíduos, surgiu uma insegurança sobre os usos e sentidos daquela coleta, no que se refere ao uso da tecnologia como uma ameaça ao direito à privacidade. Certamente, em regimes totalitários, por exemplo, o controle gerado a partir do acesso às informações era um dado relevante.

Então, num contexto de pós-guerra e construção do Estado de bem-estar social, não era inadequado pensar que as informações dos cidadãos poderiam ser coletadas para controle e repressão. É claro que a concentração do controle da informação é uma característica importante dos regimes totalitários e talvez seja essa dinâmica - a da concentração do poder -

deve ser evitada. É justamente por isso que o direito à privacidade é uma base da democracia, na medida em que reserva uma esfera privada para as pessoas, que podem decidir sobre a extensão da divulgação de suas informações, de forma a barrar a instalação de visões totalitárias (Bioni, 2019).

A tendência de coleta de dados que se sedimentou com o avanço das tecnologias, no entanto, não tinha grande recorrência do Estado como um risco à privacidade, especificamente, mas à criação de uma arquitetura informacional que permitiu aos entes privados construírem uma nova estrutura de poder vinculada às informações dos indivíduos. Na medida que os dados pessoais se tornaram valiosos para o mercado, sobretudo da compreensão dos dados pessoais como passíveis de serem transformados em produtos, serviços e previsões, uma economia inteira foi montada para administrar a geração de valor que começou a caracterizar o acesso a dados pessoais. Sobre as ameaças ao direito à privacidade e suas consequências para a reflexão jurídica, Fachinni Neto e Demoliner explicam:

> Em razão das novas ameaças à nossa privacidade, o Direito reagiu e procurou estabelecer uma proteção mais efetiva aos nossos dados pessoais, tentando garantir a todos uma verdadeira autodeterminação informativa. Isso se dá tanto a nível supranacional, como é o caso da União Europeia, que recentemente regulamentou a proteção de dados, como também nos diversos países, como o Brasil, que igualmente publicou normas tendentes a oferecer maior proteção aos seus cidadãos, frente aos riscos acarretados pelo acesso amplo e indiscriminado aos seus dados individuais. (Fachinni Neto; Demoliner, 2019, p. 120)

Isso não significa, no entanto, que o direito à privacidade atualmente é um direito à proteção dos dados pessoais. Pode-se entender que a privacidade estruturou a proteção dos dados, mas não são sinônimos. A proteção aos dados pessoais carece de uma compreensão específica, pois é um novo direito da personalidade, com uma dinâmica própria. Mesmo que esse direito tenha sido no âmbito da privacidade, a proteção aos dados modifica os elementos dela, aprofunda princípios e devem ser vistos em uma lógica mais abrangente. Doneda (2020) observa que o centro de gravidade da tutela da privacidade se reposicionou em função das hipóteses e necessidades do campo, de acordo com o momento histórico atual. Ele explica:

> Algo paradoxalmente, a proteção da privacidade na sociedade da informação, a partir da proteção de dados pessoais, avança sobre terrenos outrora improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamentos do indivíduo. (Doneda, 2020, p. 39)

Bruno Bioni (2019) trata da relação entre o direito à privacidade e a proteção aos dados pessoais. O autor explica que o direito à privacidade foi articulado a partir da dicotomia entre o público e o privado, como mencionado anteriormente. O indivíduo tem o direito de revelar seletivamente as informações que desejar, para deliminar o domínio da esfera pública e privada em sua vida. A noção da vida privada como um domínio inviolável é resultado da rivalidade que se estabeleceu nas esferas do público e do privado, para o direito. A esfera privada teria, portanto, dispositivos autônomos específicos para tutelar a sua intransponibilidade. Nesse sentido, o direito à privacidade é uma liberdade negativa, de que o indivíduo não sofra a interferência dos outros, e permeado por essa dicotomia, o que o torna um direito estático, ou seja: à espera de que o titular delimite quais fatos da sua vida estão reservados à esfera privada.

A evolução do direito à privacidade, a qual o direito à proteção dos dados pessoais está atrelado, teria caráter mais dinâmico, de uma proteção em movimento e de uma liberdade positiva no que tange ao controle das informações pessoais. Nessa concepção, a esfera privada não seria algo dado à espera de uma violação, mas um espaço construído continuamente, à posteriori, a partir de uma compreensão dinâmica sobre o controle das informações pessoais. Com isso, a noção tradicional da privacidade, que envolve resumidamente o direito ao isolamento, deveria conviver com uma nova dimensão, que representasse um intercâmbio entre uma tutela estatística e uma tutela dinâmica do direito à privacidade. Notadamente, porém, o direito à proteção dos dados pessoais não é uma mera evolução do direito à privacidade, mas um direito com autonomia própria (Bioni, 2019).

Diferentemente do direito à privacidade, onde o objeto jurídico é permeado pela dicotomia entre público e privado, a construção da proteção aos dados pessoais tem o conceito de dado pessoal como centro de gravidade; essas informações podem ser públicas ou privadas, indiferentemente. No caso dos dados pessoais, fatos públicos, que inicialmente não gerariam preocupação sobre a violação da intimidade e da vida privada, podem se tornar uma ameaça, se agregados a outros dados que revele elementos da personalidade de um indivíduo. Dados triviais muitas vezes se relacionam com informações sensíveis e intrusivas. Dessa maneira, a proteção de dados pessoais não está atrelada imediatamente à dicotomia do público e privado, o que o difere, em substância, do direito à privacidade. Para compreender adequadamente a relação entre o direito à privacidade e à proteção dos dados pessoais, deve-se entender que o direito à privacidade pavimentou um caminho onde a proteção dos dados se desenvolveu, mas não se confundem (Bioni, 2019).

Se uma informação está atrelada à pessoa, é suficiente para que o direito à proteção dos dados pessoais seja deflagrado. Mesmo que essa informação seja pública, a sua relação com outros dados pode representar uma ameaça ao titular. Os direitos de acesso e de retificação dos dados não se relaciona com a esfera privada, mas com a pública, pelo fato de que é nessa esfera que o titular busca proteger os seus dados. Outro ponto importante sobre a cisão entre o direito à privacidade e à proteção dos dados pessoais é na ocorrência de tratamentos de dados que podem submeter o titular a potenciais discriminações. Nessa esfera, o direito à proteção de dados pessoais se funde à própria dignidade da pessoa humana, tutela a dimensão relacional da pessoa, o que extrapola a tutela da privacidade (Bioni, 2019).

Há uma série de liberdades, relacionadas à proteção de dados, que se distanciam da privacidade. Embora esses direitos se relacionem em muitos momentos, e um tenha sido um ponto central para a pavimentação do outro, Bioni (2019) entende que a proteção dos dados pessoais deve ser alocada como um novo direito da personalidade, para ampliar a cláusula geral da tutela da pessoa humana. Se considerado como uma subespécie do direito à privacidade, pode perder a própria dinâmica na qual o tratamento de dados acontece e como representa violações à pessoa humana em outras instâncias.

Doneda (2020) trata de como a mudança do paradigma da proteção da privacidade, que trata do eixo pessoa-informação-circulação-controle, acompanha a consolidação dos direitos da personalidade, porque em suas acepções mais recentes, não se trata do direito a ter egoísmos privados. Se pensar a proteção dos dados pessoais em sua relação com a privacidade, a proteção dos dados quebra o individualismo exacerbado que constituía o direito à privacidade, sobretudo em seus contornos iniciais. A proteção da privacidade na era da informação, a partir da visão dos dados pessoais, interessa como construção de uma vida privada, mas também de uma vida em relação com o resto da sociedade. Dessa maneira, a proteção dos dados pessoais poderia ser lida como uma proteção da privacidade, mas por outros meios e com outros contornos, porque assume uma série de tarefas de magnitude considerável; além de características próprias e interesses diversos a serem protegidos no bojo de sua tutela. Por isso a característica patrimonialista da privacidade precisou ser afinada e superada, de certa forma, já que há novos mecanismos a serem observados para proteger os titulares de dados.

Mesmo que se entenda o direito à proteção aos dados pessoais como um direito ligado ao direito à privacidade, o desenvolvimento tecnológico representou desafios à noção de que o direito à privacidade é um direito de defesa e estático. Pela realidade do século XXI, interpretar a privacidade como um dever negativo de abstenção limita a esfera de proteção. O

direito à privacidade, nesse contexto, não é apenas um direito de defesa, pois abarca deveres negativos estatais, certamente, mas também deveres positivos de proteção. Sua zona de proteção não deve ser apenas definida a priori, mas analisada a titularidade em casos concretos, em face de sua multifuncionalidade. Embora possa parecer enfadonho ressaltar essa questão, é fundamental, diante da ligação que se estabeleceu entre os dois direitos. A conclusão é que o aumento da complexidade nas relações sociais e jurídicas que envolviam o direito à privacidade tornou necessário que a sua tutela não esteja restrita à esfera negativa, mas preste também uma função protecional positiva (Saito, 2020).

Há que se considerar duas reflexões para compreender a proteção aos dados pessoais. A primeira, como já mencionado anteriormente, é a possibilidade de compreender os dados pessoais como parte do direito à personalidade. A segunda reflexão trata da proteção aos dados pessoais na Constituição Brasileira, no âmbito da proteção à vida privada. Ao longo das próximas páginas, explorar-se-á essas duas camadas.

1.1 A relação entre dados pessoais e os direitos da personalidade

Os direitos da personalidade não foram lineares e atravessaram uma trajetória histórica ampla, se considerar os primeiros apontamentos, os fundamentos e a consolidação desses direitos nos mais diversos ordenamentos jurídicos. O prelúdio do que viria a ser os direitos da personalidade começa no direito grego e no direito romano. Essas duas culturas jurídico-legais postularam que a pessoa humana não carecia apenas de uma tutela física de integridade, mas também uma tutela moral. Essa primeira orientação foi importante e ressoou no jusnaturalismo, a partir do século XVII. Nesse período surge a ideia de que os homens possuem direitos inatos, que lhe são inerentes pela sua condição humana, nada mais. A ideia de que os direitos provinham de uma força divina é substituída pela noção de que a pessoa humana possui direitos como condição *sine qua non* de existir (Bioni, 2019).

A literatura jurídica grega e romana já mencionava formas antigas de proteção da pessoa, mas de maneira não integrada. Ou seja, as noções de pessoa da antiguidade clássica não protegiam os indivíduos completamente, e não havia uma noção de personalidade ou categoria que se assemelhasse à atual noção de personalidade. A proteção, portanto, era limitada, mas considera-se que alguns desses elementos presentes na antiguidade clássica foram pressupostos para os fundamentos do direito da personalidade. Por isso, há que se considerar que o direito e a sociedade, tanto grega quanto romana, devem ser considerados em perspectiva histórica, sem incorrer em um anacronismo que considere válidas e atuais as

estruturas jurídicas daquelas sociedades, que não se parecem com as problemáticas sociais vividas na contemporaneidade (Doneda, 2020).

Para abordar a noção de "pessoa", é preciso considerar como o cristianismo contribuiu para essa ideia elementar. A doutrina cristã, por reconhece no ser humano um princípio divino, esteve na base da construção da ideia de dignidade. Nessa perspectiva, a pessoa não é considerada apenas em si, mas em suas aspirações e potencialidades. Outra perspectiva relevante para a ideia de dignidade advém de Kant, que considera a dignidade como um atributo do homem, em sua autonomia prática, não apenas como um elemento de sua natureza. A ideia de "pessoa" passou por muitas transformações até se tornar um ponto de referência normativa para a ciência jurídica, não apenas de forma dogmática e instrumental, mas como representação de um valor em si mesmo, da dignidade como uma condição inerente à pessoa humana (Doneda, 2020).

Esse foi o fundamento dos direitos da personalidade, concebidos como uma promoção do ser humano de forma integral, mas eles só vieram muito depois. Após a dessacralização da ciência jurídica, emergiu um profundo racionalismo na cena jurídica, o que tornou o direito mais metodológico-sistemático, submetido a conceitos abstratos - dogmas - que compunham um sistema fechado, que deveria fornecer premissas matemáticas. Com essa perspectiva, a ciência jurídica se distanciou de uma visão antropocêntrica e tornou-se muito patrimonialista, o que impediu que os direitos da personalidade tivessem espaço à época. Sobre o contexto jurídico-dogmático que travou a consolidação dos direitos da personalidade, Bioni explica:

> Aliás, a própria dissidência histórica instaurada por Savigny quanto à recepção dos direitos da personalidade derivava de uma questão única e exclusivamente dogmática. Argumentava-se que o sujeito de uma relação jurídica não poderia ser ao mesmo tempo o seu objeto, sob pena de se legitimar o suicídio. Ou seja, negava-se reconhecer os direitos da personalidade por faltar uma norma que os positivasse. De acordo com esse raciocínio dogmático, era imprescindível a inserção dos direitos da personalidade na categoria de um direito subjetivo para, daí, serem escoados. (Bioni, 2019, p. 95)

A pessoa humana perdeu espaço em função da preocupação que o direito tinha em relação aos aspectos patrimoniais. Foi um período pouco acolhedor para o desenvolvimento dos direitos da personalidade, até que contextos históricos significativos intervieram para obrigar que as sociedades, e a ciência jurídica, reconhecessem a importância dos direitos do homem. Mesmo que a pessoa humana tenha sido considerada relevante anteriormente, foi após a Segunda Guerra Mundial que se proliferaram princípios relacionados à dignidade humana nas Constituições. O mundo já havia experienciado séculos de escravidão e

genocídio, regimes nazistas e fascistas, com a chancela da ciência jurídica, que fortalecia esses regimes com os seus pressupostos anteriores. A necessidade de garantir os interesses existenciais da pessoa de forma universal, em sua integridade moral e física, só se tornou popular no direito no século passado. Nesse sentido, modificou-se o foco da tutela jurídica, que posicionou o ser humano como seu centro de gravidade, em uma visão antropocêntrica novamente.

Algumas Constituições, como a alemã, passaram a prever, junto com o princípio da dignidade da pessoa humana, o direito à personalidade. Foi o pontapé para uma previsão da tutela dos direitos da personalidade no país. No Brasil, já havia o reconhecimento dos direitos da personalidade de forma implícita, a partir do Código Civil de 1916. Eram dispositivos que tratavam acessoriamente dos aspectos extrapatrimoniais das relações, que só foram adequadamente sistematizados anos depois. O projeto de Código Civil de Orlando Gomes visava romper com a visão patrimonialista e personalizar o direito civil, como uma forma de garantir a humanização do direito privado. O projeto de Código Civil do jurista baiano enumerava os direitos da personalidade, como o direito ao nome, à liberdade, à imagem, à honra e outros. Ele foi responsável por iniciar um tripé na teoria do direito civil brasileiro, que considerava a personalidade, o negócio jurídico e o patrimônio.

Gradativamente, todo o ordenamento jurídico passa a se relacionar com o valor máximo da pessoa humana. Não apenas o conjunto de situações previstos no Código Civil brasileiro sob a alcunha de direitos da personalidade, mas sobretudo sua relação com outros dispositivos e com a Carta Magna. Mesmo nas situações em que o Código Civil não prevê hipóteses, é possível relacionar os direitos da personalidade com outras cláusulas de proteção da personalidade implícitas que estão previstas na Constituição. Entende-se, portanto, que o Código Civil não funda os direitos da personalidade, mas os positiva, no sentido de orientar a interpretação jurídica e facilitar a aplicação, de forma a inspirar o legislador a observar os interesses da pessoa humana com mais detalhes.

Vários autores têm assinalado que os direitos da personalidade foram inovadores no direito civil brasileiro, mas eles representam mais do que isso: são parte de uma cláusula geral de proteção de tutela e promoção da pessoa humana, que é, notadamente, elástica. Nesse sentido, os direitos da personalidade não se limitam às situações previstas no Código Civil, pois devem estar atentos aos desafios da sociedade atual, de forma a promover categorias jurídicas que enquadrem às necessidades contemporâneas de proteção dos direitos da personalidade. Sobre a reflexão dos dados pessoais como um direito da personalidade, Ingo Sarlet defende:

> Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa. (Sarlet, 2020, p. 185)

Danilo Doneda (2020) explica que essa cláusula geral do valor representado pela pessoa humana deve ser observada em todas as relações jurídicas, sejam patrimoniais ou não. Deve ser observada não apenas nas situações previstas como hipóteses de incidência dos direitos da personalidade, mas em todos os contextos que tenham a personalidade como um elemento objetivo, sobretudo ao considerar a importância que a noção de "pessoa humana" tem para o ordenamento jurídico como um todo, irradiada para a Constituição Federal.

Mesmo que a Constituição Federal de 1988 não tenha uma previsão de cláusula geral expressa para a proteção da personalidade, como existem em outras Constituições - a exemplo da alemã e da italiana -, a doutrina entende que se absorve o direito geral da personalidade, observado nos princípios fundamentais, em que se busca proteger a dignidade humana e os direitos fundamentais do homem. Não obstante, algumas categorias especiais de direitos da personalidade foram previstas, como o direito à igualdade, à intimidade, à vida privada e afins. Esses direitos, expressamente, são muito importantes ao discutir os dados pessoais como tema, posto que se relacionam diretamente com essa nova categoria jurídica. Por meio dos princípios inseridos na Constituição, ela eleva o direito geral de personalidade, tendo a dignidade humana como matriz (Mota; Abagge; Knoerr, 2019).

Para debater a proteção dos dados pessoais como um direito da personalidade, é preciso refletir sobre o que os caracteriza, para posicionar de que maneira é possível encaixá-lo como um deles. Ressalta-se que a doutrina não tem um posicionamento único sobre o conceito e a caracterização dos direitos da personalidade, então adota-se uma definição que os considera como direitos essenciais, inatos e permanentes, com algumas características específicas, a serem destrinchadas.

A dignidade da pessoa humana é a fonte dos direitos da personalidade. Na construção dogmática desses direitos, existe uma compreensão de que, para que se viva uma vida plena, a pessoa precisa de uma série de elementos para desenvolver-se de forma plena e com satisfação pessoal. Esses elementos podem ser móveis e externos à pessoa, mas são relevantes para a construção de sua vida. Outros bens são de ordem interna, necessários à dignidade e à

moral. Cada um desses elementos são fundamentais para a experiência humana, para garantir a sua integridade. Entende-se que os direitos da personalidade são prerrogativas fundamentais, que já nascem com o indivíduo (Tepedino, 2004).

São direitos absolutos, constituídos de uma série de caracteres especiais sem os quais a dignidade não seria alcançada. Os direitos da personalidade não são direitos patrimoniais e regulam as relações particulares, ou seja, não representam uma proteção contra o Estado, mas "contra" outras pessoas. São fruto do reconhecimento da própria condição humana em sua inteireza. Há pelo menos cinco características importantes acerca desses direitos: a generalidade, a imprescritibilidade, a intransmissibilidade, a inalienabilidade e a extra patrimonialidade (Tepedino, 2004).

Podem ser considerados como direitos generalistas porque a condição de sua existência é que o ser humano esteja vivo. Se eles antecedem ou não à ordem jurídica é algo que extrapola o consenso na ciência jurídica, mas entende-se que eles são direitos generalistas. São considerados como absolutos porque carecem de respeitabilidade, ou seja, impõe a obrigação a todas as pessoas de os respeitarem, opondo-se a todos. Os titulares não podem dispor desses direitos, de maneira que eles são intransmissíveis e se extinguem com a morte do titular. Mesmo que um indivíduo se abstenha de exercê-los, sempre pode utilizá-los, então são considerados imprescritíveis. Em relação à extra patrimonialidade, trata-se do fato de que eles não são suscetíveis à avaliação econômica (Tepedino, 2004).

Não é incomum a relação entre dados pessoais e direito à privacidade e parte dessa dinâmica tem raízes na própria construção desse direito. Porém, pode-se entender os dados pessoais como parte do desenvolvimento da personalidade, que carece de uma proteção autônoma. Alguns direitos relacionados aos dados pessoais, como por exemplo o direito à retificação, não se relaciona somente com a privacidade, mas com direitos daqueles que protegem a personalidade. Não tem, portanto, o intuito de não publicizar determinada informação, mas de ter controle sobre a informação a seu respeito, seja ela pública ou privada. Os dados pessoais se relacionam com a identidade das pessoas, motivo pelo qual advoga-se pela configuração desse direito como um direito personalíssimo (Mota; Abagger; Knoerr, 2019).

Adriana Scheleder e Patricia Noschang (2018) abordam outros elementos acerca dos dados pessoais, que trata da formação de uma identidade específica do indivíduo na esfera digital. Embora a proteção da identidade digital não seja a única forma de observância dos dados pessoais, é importante posicionar que essa identidade é uma das formas de exercício da personalidade na realidade contemporânea. Como tal, ela merece proteção legal tendo como

fundamento o direito geral de personalidade, de forma que o direito se adapte à evolução da esfera digital. A identidade digital é uma forma central de participação social e política na sociedade da informação, então todos os meios de identificação da pessoa, seja digital ou não, devem ser preservados; nesse contexto, ela representa uma expressão da personalidade do indivíduo, num contexto de conexões, relações e transações por meios digitais. Pode-se entender, portanto, que o direito de proteção dos dados pessoais extrapola a privacidade, trata da honra, da liberdade, da retificação de dados incorretos, da imagem e de uma série de direitos personalíssimos que permitem o livre desenvolvimento da personalidade do indivíduo.

1.2 O direito à proteção de dados na Constituição Federal

A outra reflexão a ser debatida, que trata do direito à proteção dos dados pessoais na Constituição Federal de 1988, explora alguns detalhes conceituais e históricos, que permitiu à doutrina deduzir uma proteção aos dados, sobretudo pela relação entre conceitos sinônimos que foram construídos na legislação e na doutrina brasileira, de forma a contribuir para a criação do direito aos dados pessoais, mesmo antes da positivação do direito na Constituição.

A primeira questão terminológica é justamente como o termo "privacidade" foi utilizado com correlação direta com sinônimos, tal como vida privada, intimidade, segredo, sigilo, etc. Dentro desses conceitos sinônimos, há uma série de possibilidades tuteladas como direito à privacidade, num terreno em que o próprio ordenamento jurídico não separou as suas definições âncoras. A Constituições Federal de 1988, em seu artigo 5º, que trata das garantias e dos direitos fundamentais, menciona a "proteção da intimidade" e da "vida privada", em um entendimento de que a proteção da pessoa humana abrange esses aspectos. Outros termos, como "imagem" e "honra" também são mencionados, o que possibilita interpretações diferentes (Doneda, 2020).

A Constituição Federal de 1988, embora tenha referência ao sigilo das comunicações em seu art 5º, não previu expressamente um direito à proteção dos dados pelo seu titular até o ano de 2022, então o reconhecimento desse direito é algo recente no ordenamento jurídico brasileiro, sobretudo o seu posicionamento supralegal. Isso não significa dizer, no entanto, que não pôde o direito à proteção dos dados decorrer implicitamente da Constituição, e é isso que nos interessa nesse tópico. Uma das previsões constitucionais que incorrem num direito ao conhecimento e retificação dos seus dados é o habeas data, do qual trataremos com mais

profundidade no próximo capítulo, mas que expressa uma garantia do exercício de autodeterminação informativa (Sarlet, 2020).

Sarlet (2020) argumentou que, embora tenha se reconhecido historicamente uma proteção dos dados como direito fundamental implícito, sua positivação formal traz uma carga substancial em relação ao avanço brasileiro no campo da proteção de dados, em diversos sentidos: assegurar-se-ia a proteção de dados como um direito fundamental autônomo, com âmbito de proteção específico; passa-se a atribuir à proteção de dados o regime jurídico-constitucional integralmente; os direitos fundamentais integrados à Constituição possuem status normativo hierarquicamente superior ao resto do ordenamento jurídico e outros aspectos que advogam pela necessidade de positivação formal do direito à proteção dos dados.

Embora compreenda-se a proteção aos dados pessoais na Constituição Federal em sua articulação com a dignidade da pessoa humana e os direitos da personalidade e da privacidade, o objeto de proteção de dados é eminentemente diferente. A opção terminológica por "proteção de dados pessoais" não representa um mero sinônimo, mas uma virada conceitual, no sentido de que os dados pessoais devem ser compreendidos em sentido amplo para efeitos de sua proteção jurídica. Não há, na economia da informação, dados que podem ser considerados "irrelevantes", há potencial para que qualquer dado seja utilizado de maneira a violar direitos fundamentais. Postula-se esse direito em interação com o direito à privacidade e à autodeterminação informativa, mas apenas no sentido de que se formam zonas de contato, embora sejam todos autônomos (Sarlet, 2020).

A Emenda Constitucional 115, de 10 de fevereiro de 2022, representou uma mudança significativa na proteção de dados no Brasil, por positivar a proteção aos dados como um direito e garantia fundamental. Essa mudança representou a concretude de um direito que já era reconhecido pela doutrina e pela jurisprudência como um elemento implícito à Carta Magna. Com a positivação, a Emenda também fixou como competência privativa da União as legislações sobre proteção e tratamento de dados pessoais. Dessa maneira, a Constituição reforçou a segurança jurídica sobre o tema e tornou a proteção dos dados pessoais um elemento essencial de proteção estatal, associado à dignidade da pessoa humana. Com essas modificações, entende-se que a União impede os riscos de iniciativas legislativas estaduais e municipais que pudessem intervir na aplicação da Lei Geral de Proteção de Dados e na tutela dos dados pessoais de maneira ampla (Martins; Guariento, 2022).

Uma abordagem mais sólida sobre a sociedade da informação e o contexto do big data podem auxiliar a pavimentar um cenário para discutir os dados conceitualmente, a diferença

entre dados e informação e a construção de um cenário de proteção dos dados pessoais no Brasil, a partir da criação da Lei Geral de Proteção de Dados, mais substancialmente, mas também de outros dispositivos legais que sustentaram essa proteção anterior à LGPD.

1.3 Big data, era da informação e o direito à proteção dos dados pessoais

Para entender a importância da proteção de dados pessoais, é preciso explorar algumas nuances do contexto do big data e quais os impactos que esse fenômeno gera para a sociedade e para o direito. Como já mencionado anteriormente, as informações sobre os indivíduos se tornaram muito importantes nas últimas décadas para consolidar uma economia voltada para dados e informações. Essas inovações possuem muitos usos positivos para diversas áreas da vida humana, mas também representam desafios particulares, do ponto de vista jurídico e social, para assimilar os seus usos de forma adequada com o Direito, como aponta Hoffman-Riem:

> As inovações provocam respostas à questão de saber se e em que medida as regras jurídicas tradicionais são adequadas para fazer justiça à problemática da situação em transformação e para implementar de forma otimizada os novos valores-alvo ancorados na ordem jurídica e social até à data ou mesmo os valores importantes sob as novas condições. Entre os importantes objetivos contam-se a proteção da liberdade individual, a observância dos princípios do Estado de direito, o funcionamento da ordem democrática, mas também um maior desenvolvimento econômico e tecnológico e a necessária capacitação para as inovações. (Hoffmann-Riem, 2020, p. 436-437)

Uma dessas questões é o surgimento da sociedade digital, na qual os dados possuem um protagonismo significativo para a condução das relações sociais e econômicas. O termo "big data" surgiu na década de 1990, para se referir à manipulação e análise de um grande volume de dados. Pode-se entendê-lo como um fenômeno, no sentido de configurar-se como um registro amplo de qualquer tipo de dados (Botelho, 2020).

No contexto do big data, é possível produzir e registrar dados em larga escala, o que o caracteriza efetivamente como um fenômeno. Nesse sentido, *big data* é a capacidade que uma sociedade possui para obter informações, de maneiras inovadoras, para gerar predições, políticas, produção de bens, serviços e toda uma economia em volta de informações que se tornam dados. Há pelo menos três elementos que caracterizam o termo: o volume, a variedade e a velocidade. Refere-se à possibilidade de acessar, produzir ou tratar grandes quantidades de dados digitais, de diferentes tipos e funções, bem como várias formas de coletar, armazenar e acessar, com uma velocidade de processamento nunca vista (Hoffmann-Riem, 2020).

Trata-se de um volume descomunal de dados, que são acessados, coletados, estruturados e analisados para uma gama incompreensível de finalidades. A extensão do seu processamento é tão significativa, que dificulta a representação da magnitude desse fenômeno. Essa magnitude não diz apenas do volume significativo de dados processados, que é uma característica importante, mas também da variedade de dados processados que excede as tecnologias tradicionais de processamento, de maneira que é possível utilizar todos esses dados para uma série de processos, inclusive que interagem com técnicas de comportamento preditivo, muitas vezes, o que pode ser uma problemática social relevante (Bioni, 2019).

Em outro trabalho, Hoffmann-Riem (2022) apresenta uma extensão do conceito de *big data*, com cinco características para descrever o fenômeno. Além do volume, da variedade e da velocidade, ele incluiu a relação entre o big data e a inteligência artificial, para defender que o uso de inteligência artificial possibilita novas formas de processar os dados, mas também de verificar a sua consistência e a sua veracidade, que seria o "quarto V" do big data. Por fim, o autor enfatiza como as novas bases de processamento e análise de dados implicam em um novo valor de mercado, agregado às operações. O "valor" é o quinto V do big data.

O fenômeno do big data dialoga com a inteligência artificial, sem a qual seria impossível chegar ao estado da arte de tratamento de dados e predição que existe atualmente. Os algoritmos aumentam a eficiência no tratamento de dados, garantem a qualidade do tratamento e verificam a coerência para a finalidade as quais os dados se destinam. O big data é uma base para vários modelos de negócio que tem como intuito criar valor, suas aplicações são inúmeras, em diversos setores da vida humana.

O big data é utilizado para muitos fins, como controle e previsão de comportamentos, sejam individuais ou coletivos; registro de tendências econômicas ou sociais, o que possibilita novas abordagens para as tarefas estatais e a produção e distribuição de produtos, em organizações privadas; mas também há outro cenário, em que o big data é utilizado na ilegalidade, para efetuar crimes cibernéticos. Alguns exemplos de aplicações para o uso de big data são: tecnologias de rede, como medidores inteligentes e dispositivos automatizados; comunicação eletrônica, como exemplo os smartphones; interação e comunicação em redes e mídias sociais; vigilância eletrônica, sistemas de assistência virtual e afins (Hoffmann-Riem, 2022).

Uma das considerações mais importantes sobre a centralidade da economia de dados atuais é que não basta ter um volume significativo de dados dos indivíduos. A coleta, por si só, não representa grandes avanços. É preciso ter capacidade de interpretar os dados, para expandir as possibilidades de utilização, especialmente numa combinação com a inteligência

artificial. Certamente, no âmbito dessa dissertação, não se advoga pelo uso irrefreado dos dados pessoais, pelo contrário. No entanto, é necessário compreender que há etapas e procedimentos que permitem o uso dos dados para os mais diversos fins. A esse respeito, há uma análise de grandes dados, que são procedimentos analíticos para gerar valor a partir dos dados obtidos com os mecanismos de coleta (Hoffmann-Riem, 2020).

Há três tipos de análises que fazem parte desse grande guarda-chuva de métodos de utilização. A análise descritiva, que filtra e processa os dados para avaliação. Esse método prioriza a classificação e a filtragem, com o intuito de sistematizar os dados e catalogá-los. A análise preditiva tem como objetivo identificar padrões, com base nos dados existentes, e criar correlações significativas, com previsões e probabilidades para determinado evento. Um dos maiores objetivos desse tipo de análise é identificar tendências e prever comportamentos das pessoas. Esse método de análise tem sido um dos mais críticos, em termos da autodeterminação informativa. A análise prescritiva se dedica a recomendar ações, a partir da análise dos dados obtidos, para alcançar determinados objetivos. Todas essas estratégias analíticas têm como objetivo a expansão dos usos possíveis dos dados, para utilizá-los em diversas aplicações e com muitas finalidades. É um quadro que permite muito mais do que coletar e armazenar dados, posto que obter dados não é um fim em si, mas um meio, para a maioria dos players que tratam dados pessoais (Hoffmann-Riem, 2020).

A análise de big data visa expandir e utilizar o conhecimento gerado por diversos campos, para uma infinidade de aplicações, com a utilização de todos os tipos de dados possíveis. O faz sobretudo por meio da inteligência artificial, o que significa que ela não se limita à coleta, armazenamento e tratamento dos dados pessoais, que é o foco tradicional do direito em torno da proteção de dados. Enfatizar esse ponto é importante porque os métodos de análise permitem usos extensos, tanto por atores estatais quanto privados. É fundamental que a tutela jurídica proteja os titulares dos dados, mas também é necessário considerar que há usos socialmente responsáveis e benéficos. Ou seja, o uso de big data envolve tanto oportunidades sociais e econômicas, quanto riscos de violação de direitos; esses fatores devem ser equilibrados por meio de uma proteção jurídica adequada à complexidade do fenômeno, por considerar os riscos para bens jurídicos individuais e coletivos (Hoffmann-Riem, 2022).

Como Bioni (2019) explica, na medida em que se aumenta a variedade de dados, há também a necessidade de empregar mais tempo para organizá-los. O big data, de certa maneira, descarta essa necessidade prévia de estruturação dos dados, porque utiliza metodologias de análise, por meio de inteligência artificial, para estruturar os dados. Nesse

contexto, os dados não são analisados em amostras, mas em toda a sua extensão. Esse é o grande potencial do fenômeno big data; há um volume enorme de dados processados que, ao serem analisados em sua inteireza, correlacionam uma série de fatos para desvendar padrões e tomar decisões, sejam automatizadas ou não. A probabilidade de acontecimentos futuros é o ápice - positiva ou negativamente - desse cenário de profunda sofisticação tecnológica. Notadamente, o big data não é um sistema inteligente, é uma metodologia, uma ferramenta para coletar, processar, organizar dados e analisá-los para tomar decisões. Não é um fenômeno focado nas causas de determinado evento, mas na probabilidade de que determinada coisa aconteça, sustentada por informações já existentes. Uma representação muito utilizada para exemplificar a potencialidade do Big Data é o caso que envolve a varejista americana Target.

A Target tinha o intuito de identificar as suas consumidoras grávidas. A gravidez é uma fase da vida em que as consumidoras compram uma série de produtos, com uma determinada lista, associada às necessidades da gravidez e às mudanças, sejam hormonais ou comportamentais, que ocorrem nesse período. A equipe de análise de dados da Target conseguiu categorizar um padrão de lista de produtos que as consumidoras adquiriam nessa fase. Isso permitiu que eles não apenas previssem que a consumidora x estava grávida, mas o período da gestação em que as grávidas compram determinados produtos, para direcionar anúncios para elas de acordo com a fase da gravidez (Hill, 2012).

Os algoritmos foram programados para estabelecer essa correlação e sugerir produtos específicos para consumidoras com esse perfil. Como destacado anteriormente, a inteligência artificial é um braço do big data, sem o qual esses dados seriam dificilmente utilizados de forma ampla. Com esses dados em mãos, a Target sugeria cupons de descontos e ofertas personalizadas para as consumidoras que considerava como potenciais mães; esse modelo de análise preditiva pode ser muito útil, mas tem um potencial gigantesco de violação de direitos, não no sentido individual, mas da experiência de um "capitalismo de vigilância" como Zuboff (2021) critica, ou seja, como uma ordem econômica que utiliza os dados da experiência humana para extrair informações, prever comportamentos e vender produtos.

Essa tecnologia utilizada pela Target teve muito sucesso, até que foi questionada após um pai furioso entrar em um dos estabelecimentos da empresa e acusar a loja de incentivar a sua filha adolescente a engravidar. O pai em questão queria explicações do porquê de sua filha adolescente receber cupons de descontos em produtos relacionados a gravidez. Para ele, essa lista de produtos poderia incentivar uma gravidez precoce. O gerente da loja desconheceu a situação e conferiu junto à Sede da Target para apurar o que havia acontecido. Ligou para o

cliente para se desculpar, em nome da empresa, porque de fato havia um envio de cupons relacionados a roupas para gestantes e itens para recém-nascidos. Dias depois, o pai da adolescente ligou para a loja e informou que, de fato, sua filha estava grávida, situação que ele desconhecia até o momento. Dessa vez, ele que se desculpou pelo ocorrido (Hill, 2012).

Desde então, a empresa decidiu redirecionar a sua análise preditiva, de maneira a mascarar os resultados de suas previsões no envio de anúncios publicitários. Uma vez reconhecido um potencial de que determinado cliente esteja passando por um período específico de sua vida - como gravidez -, eles enviam produtos relacionados com isso, mas também ofertas de outra natureza, de maneira aleatória. De certa maneira, isso suaviza a ideia, para os clientes, de que eles são espionados. Uma oferta aparentemente "sem sentido", muitas vezes é resultado de uma correlação entre diversos dados de um indivíduo, coletados ao longo do tempo, que são utilizados como média do padrão de consumo daquele indivíduo especificamente ou de outras pessoas com o mesmo perfil; ao explorar essas correlações, as empresas direcionam anúncios que podem ser tentadores para o consumidor de determinado perfil (Hill, 2012).

Esse caso ilustra perfeitamente o potencial que o fenômeno big data representa. As milhares de bases de dados criadas, agregadas e analisadas, inclusive conjuntamente, servem para identificar uma série de padrões de comportamento e inferir as possibilidades reais de que determinado evento aconteça no futuro. A predição cruza dados importantes do comportamento humano. Um banco de dados pode ser utilizado não apenas para uma gama de finalidades, mas podem ser reutilizados, por meio da redefinição dos algoritmos, para operar sob novos usos e configurações. Cada vez mais, os dados dos indivíduos servem a propósitos amplos da economia da informação, o que representa uma mina de ouro para essa indústria (Bioni, 2019).

Hoffmann-Riem (2020) abordou a discussão pública de que os dados são o "petróleo bruto da sociedade moderna" e sua reflexão pode ser útil para entender o contexto do big data e suas reais utilizações. Seu objetivo é posicionar um entendimento sobre a importância econômica e o potencial de utilização dos dados para as economias regionais e globais. Essas "oportunidades" são, ao mesmo tempo, o maior problema dos dados para a violação de direitos. Ao contrário do petróleo, os dados podem ser produzidos em alta velocidade e a sociedade da informação gira em torno deles, de maneira que o particular sempre fornece seus dados.

Dados não são um tesouro estanque, seu estoque é ilimitado e alimentado todos os dias, a nível mundial, até mesmo contra a vontade das pessoas afetadas. Os dados estão em

todos os lugares e atualmente são fáceis, do ponto de vista técnico, de capturar e armazenar, há uma infinidade de "tanques" de dados, desde um computador a bancos de dados de empresas, inclusive aqueles armazenados em nuvem, em todos os lugares do mundo. Os "tanques" estão cheios, não há escassez deles. O processo de análise e tratamento de dados são, de fato, um refinamento, como acontece com o petróleo. A diferença é que a sofisticação da inteligência artificial permite agregar um novo valor ao produto refinado e esse produto pode ser transformado em outra coisa rapidamente. Ele conclui:

> Ao mesmo tempo, podem ser observadas assimetrias consideráveis nas possibilidades de utilização dos recursos de dados, por exemplo, na clarificação da questão de saber se é dada a devida atenção à usabilidade dos dados, se todas ou quais as partes interessadas têm acesso aos dados, se são tratadas de forma responsável e se os diferentes interesses dos membros da sociedade são tidos em conta de forma equitativa através da utilização dos dados. (Hoffmann-Riem, 2020, p. 441)

O período histórico atual é fruto de uma revolução da informação. No meio desse acontecimento, surge o conceito de "sociedade da informação" para explicar uma modificação profunda cultural, social, econômica, dos valores, da ciência jurídica e de uma série de elementos e instituições, que foram influenciadas pelas novas formas de comunicação e produção de informações. A mudança nos meios de comunicação foi fundamental para a existência da sociedade informacional. Enquanto a revolução industrial visava o desenvolvimento de bens materiais e tangíveis, a revolução da informação desenvolveu tecnologias de produção do conhecimento e de facilitação do acesso de informações (Lisboa, 2006).

Alguns efeitos da revolução informacional foram: a transnacionalização, um movimento de integração socioeconômica mundial, que permite que os Estados se comuniquem com mais rapidez e eficiência, assim como que instituições e empresas diversifiquem a sua atuação sem a necessidade de intensa presença física; o surgimento do e-commerce, que possibilita adquirir produtos e serviços na rede, com desafios para o Direito, que teve que adequar-se à proteção dos direitos do consumidor, dos direitos da personalidade e da privacidade nesse âmbito; a economia da informação, no sentido de que há um valor econômico relevante na informação, reconhecida como um ativo pessoal, na medida em que não apenas pode ser mercantilizada, mas como algo que faz parte do patrimônio do indivíduo; a formação de banco de dados, sobretudo no amplo fenômeno de big data, que permite coletar, armazenar e analisar dados com mais sofisticação do que os métodos tradicionais de pequena escala e outros efeitos (Lisboa, 2006).

Como um conceito, a sociedade da informação denomina um período histórico no qual a informação é um importante meio de produção e distribuição de bens e produtos. Lisboa apresenta uma definição interessante:

> "Sociedade da informação", também denominada de "sociedade do conhecimento", é expressão utilizada para identificar o período histórico a partir da preponderância da informação sobre os meios de produção e a distribuição dos bens na sociedade que se estabeleceu a partir da vulgarização das programações de dados utiliza dos meios de comunicação existentes e dos dados obtidos sobre uma pessoa e/ou objeto, para a realização de atos e negócios jurídicos. (Lisboa, 2006, p. 88)

Não se trata, portanto, apenas de uma marca do advento da internet, nem do uso de computadores e smartphones. Isso, por si só, não configuraria a sociedade da informação. A questão é o modo como a informação circula, como ela é produzida e o papel que opera nas relações sociais, econômicas e jurídicas. A ascensão dos 3V'S - velocidade, volume e variedade - é o ponto chave da sociedade da informação, porque ela muda a forma como os seres humanos se relacionam entre si. Esse período histórico fundou um ecossistema social que depende do superávit informacional para existir. É tão predominante que, na atual conjuntura, seria difícil imaginar uma sociedade sem a presença dessa atmosfera informacional. Nessa organização social, gerar, processar e transmitir informações são etapas fundamentais da produtividade, da economia e do poder; se assenta nas condições tecnológicas, mas amplia e se retroalimenta cotidianamente (Boff; Fortes; Freitas, 2018).

É por tal característica que, muitas vezes, a sociedade da informação é acompanhada por uma reflexão sobre a economia da informação: a produtividade econômica atual depende do superávit informacional que acompanhou o período histórico. Como a informação é o elemento nuclear de uma economia, entende-se que há uma infraestrutura preparada para extrair esses recursos informacionais. É importante destacar que, apesar da sociedade da informação não se resumir à existência - per si - dos computadores, os instrumentos computacionais sustentam a infraestrutura econômica (Mota; Abagger; Knoerr, 2019).

Os meios de comunicação foram modificados com a microeletrônico e tanto o Estado quanto à iniciativa privada utilizam a internet, as redes sociais e a potência computacional para realizar as suas atividades, sejam econômicas ou sociais. A sociedade da informação é um paradigma que extrapolou as barreiras físicas e os limites territoriais e fundou uma revolução na comunicação humana e na forma de produzir bens e serviços. Há uma sofisticação tecnológica que se desenvolve a cada dia, mas há também um potencial gigantesco de violação dos direitos, decorrente justamente da capacidade que os players da

tecnologia adquiriram de explorar o superávit informacional como superávit do comportamento humano.

Essas reflexões partem de um princípio muito importante para entender a extensão do potencial de violação de direitos no que tange aos dados pessoais na atualidade: a ideia de que a informação tem um valor econômico. Com o termo "economia da informação", diz justamente de um modelo em que qualquer dado, se tratado para fins específicos, pode expor informações dos indivíduos que tem potencial para serem capitalizadas. Portanto, entende-se que se trata de uma economia informacional, que supera o modelo de economia passado, no sentido de que quem retém mais informações, mais poder de venda possui, independente da veracidade ou do potencial lesivo que essas informações representam. De certa maneira, essa economia é facilitada pelo volume imenso de dados que os indivíduos oferecem, na sociedade da informação, para as mais diversas instituições, organizações e empresas (Coelho, 2019).

Os players que exploram dados não precisam mais buscar incessantemente por informações, elas são oferecidas com meros "cliques" pelos próprios indivíduos, que não são mais clientes, mas sim produtos, no sentido de que os dados que disponibilizam são o "pagamento" pelas plataformas que acessam. Nessas operações, as empresas sabem que um cliente deseja comprar determinado produto antes mesmo que ele se apresente para realizar a compra, por exemplo, já que os dados residuais de suas navegações são capitalizados, por meio do uso de inteligência artificial, para prever a sua condição de potencial comprador.

No campo das análises, a informação é um elemento capaz de dissipar as incertezas e proporcionar ativos para tomar decisões, prever comportamentos, reduzir custos e afins. Na economia da informação, ela é utilizada para alterar ou avaliar o comportamento das pessoas e incentivar outras ações. Como parte de uma dinâmica de produção de compradores e consumidores, as informações são utilizadas como ativo de originalidade, para prender as pessoas, seja para compra de um produto, para adquirir um serviço ou para alimentar determinada aplicação com mais dados (Cohen, 2002).

Os indivíduos podem ter a sensação de que estão sendo "vigiados", dada a riqueza de precisão com que são atingidos por anúncios e aplicações atualmente. Essa pretensa "originalidade" da economia da informação é capaz de soar para as pessoas muitas vezes como uma vantagem, posto que, em tese, diminui o tempo que uma pessoa deve se esforçar para comprar ou acessar algo. Por isso o contexto é tão importante e a economia da informação sabe capitalizar isso: qualquer informação pode ser capaz de gerar um resultado, se utilizado em um contexto propício para tal. Essa máxima conduz um novo mercado em torno da coleta, produção, análise e uso dos dados pessoais (Zuboff, 2021).

Como a experiência na sociedade da informação sempre deseja marcas e registros do caminho percorrido pelas pessoas na internet, aqueles que buscam vender precisam apenas indicar, ou facilitar, a chegada do indivíduo ao produto. Diferentemente de outras revoluções econômicas que marcaram a história, a revolução tecnológica e a economia da informação se difundiram muito rapidamente por todo um globo, nas últimas décadas, e a informação, por mais inofensiva que pareça, pode movimentar toda uma economia, em meio digital ou não (Mota; Abagger; Knoerr, 2019).

Na economia da informação, é comum que as organizações utilizem dados para vender produtos e serviços para usuários específicos, mas também compartilham dados dos titulares com terceiros, para ampliar a base de dados de outras organizações, com fins principalmente preditivos. Uma parcela desses dados é utilizada para aprimoramento da experiência dos usuários, certamente, mas a venda dos dados dos titulares é o fenômeno mais comum. Nesse contexto, monetizam-se os dados, em duas esferas: interna, na utilização de dados pessoais para alavancar os próprios resultados e se posicionar de forma mais agressiva e específica; externa, ao transformar os dados em produtos, posto que estes possuem grande valor de mercado, de modo que a sua venda representa uma grande fonte de receita (Modesto, 2020).

As organizações utilizam as informações para entender como os clientes agem; embora a monetização desses dados não seja ilegal em algumas circunstâncias, é imprescindível tratar da forma com que a experiência humana, sobretudo digital, tem funcionado como insumo para uma economia rentável e pouco criteriosa, no sentido de garantir os meios pelos quais os indivíduos podem garantir a autonomia das suas informações de forma facilitada (Modesto, 2020).

As transações mediadas por computador tiveram efeitos indescritíveis para a economia moderna. Porque há um computador no centro de basicamente toda transação no cenário atual. Ele representa diversos usos como centro da economia atual, a saber: extração e análise de dados, novas formas contratuais para oferecer melhor monitoramento, personalização e customização e contínuos experimentos. Zuboff (2021) explora essas quatro dimensões para situar a lógica daquilo que chamou de capitalismo de vigilância. Essa perspectiva da autora tem tudo a ver com o tema do consentimento e da violação de direitos dos titulares de dados. Para ela, esses quatro usos dos computadores na economia atual molda uma civilização de informação que é útil para sustentar o capitalismo de vigilância. Uma das mais importantes instâncias é a "extração e análise de dados", por exemplo, pois se refere à noção de que os dados são matérias-primas para a vigilância dos indivíduos no capitalismo atual; a extração é uma operação realizada pelas empresas para operacionalizar os dados como matéria-prima,

tanto para oferecer produtos e experiências aos indivíduos, quanto ofertar informações sobre os indivíduos para outras empresas.

O conceito de capitalismo de vigilância é útil para compreender como a experiência humana tem sido apreendida como dado comportamental, na economia da informação, e como essa discussão dos dados pessoais perpassa por um profundo debate de assimetria informacional e comportamento preditivo, que será refletido melhor em outros capítulos. Para fins desse capítulo, é importante examinar a economia da informação a partir do conceito de vigilância que Zuboff (2021) apresenta. A autora explica esse conceito como um fenômeno de reivindicação da experiência humana como matéria-prima gratuita para produzir dados comportamentos.

Embora alguns dados decorram da necessidade de aperfeiçoar produtos e serviços e até mesmo de oferecer experiências para os indivíduos, o resto dos dados que os titulares fornecem são considerados como superávit comportamental do proprietário, ou seja, alimentam processos que se tornam, posteriormente, produtos de predição, aptos a prever um padrão de comportamento dos indivíduos. Esses produtos de predições são vendidos num mercado específico para esse fim, que alimenta uma máquina gigantesca de operações comerciais; muitas companhias estão ávidas pelos "dados residuais" que, com uso de IA, se tornam verdadeiras minas de predição sobre as pessoas (Zuboff, 2021).

Nessa seara, há uma dinâmica competitiva muito forte dentro desse mercado, pela busca incessante de adquirir novas fontes, com maior potencial preditivo, em torno de um superávit comportamental. Os produtos e serviços dentro do capitalismo de vigilância não oferecem uma reciprocidade tradicional da relação de compra e venda, como numa dinâmica produtor-consumidor. Na verdade, são ganchos que levam os usuários para operações extrativistas, que utilizam as experiências pessoais dos titulares para outros fins, como de criar personas comportamentais, com base nos dados de determinado indivíduo, para compreender qual a média de pessoas semelhantes a ele que comprariam determinado produto ou serviço (Zuboff, 2021).

Embora haja uma oferta imensa de aplicações, produtos, redes sociais e plataformas que você possa utilizar "de graça", os titulares dos dados não são os clientes, porque as suas experiências nesse cenário são utilizadas como material de vigilância para outras operações. Nesse sentido, os titulares de dados pessoais são objetos de uma extração de matéria-prima, que é quase uma condição intransponível para viver a experiência em rede. Os "clientes" não são os titulares que usam as redes, que compram em sites, que acessam aplicativos; esses são

os objetos, os "clientes" desse formato de vigilância são os players que negociam dados no mercado de predição (Zuboff, 2021).

O exemplo utilizado nesse capítulo, que se refere à Empresa Target, é um retrato de como o mercado preditivo funciona e como ele é um dos maiores braços da assimetria informacional que os titulares de dados pessoais enfrentam. Por isso, é fundamental apresentar como o Brasil se posicionou, ao longo das últimas décadas, no que se refere à proteção dos dados pessoais, para compreender o panorama de proteção e os desafios para os próximos anos.

2 DIREITO À PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL

A disciplina para proteção de dados pessoais surgiu no âmbito da sociedade da informação, como enfatizado muitas vezes no último capítulo, como uma possibilidade de tutela da personalidade do indivíduo contra os potenciais lesivos que o tratamento de dados pessoais pode gerar. A função dessa disciplina não é proteger os dados, certamente, mas a pessoa que é titular destes. Esse é o período histórico que mais gerou dados pessoais em toda a história da humanidade, o que pode ser retratado com base nos inúmeros bancos de dados que são alimentados com dados dos indivíduos, nos mais diversos setores.

As informações pessoais são formas através das quais as pessoas se relacionam em sociedade, elas são intermediários na dinâmica indivíduo/sociedade e por isso possuem um potencial tão alto de violação à personalidade do indivíduo porque constituem, em si mesmas, uma parcela dessa personalidade. A tutela jurídica dos dados pessoais assegura ao titular a liberdade, a privacidade e a equidade diante do contexto grave de assimetria informacional (Mendes, 2014).

2.1 Antecedentes históricos globais: as gerações de leis

A disciplina da proteção de dados pessoais passou a envolver o problema da igualdade. É importante enfatizar isso, pois entender o desequilíbrio que o indivíduo sofre na sociedade da informação é imprescindível para compreender como a arena da proteção de dados se desenvolveu e como a noção da desigualdade pavimentou muitas arenas de proteção setoriais. A igualdade se apresentou como um tema à medida que a vigilância, seja privada ou estatal, passou a fazer parte da vida dos indivíduos, de maneiras que suas informações poderiam acarretar seleção e classificação dos indivíduos, segundo níveis de adequação, para as suas oportunidades de vida (Mendes, 2014).

Na prática, as operações de tratamento de dados realizadas por organismos privados e pelo Estado tem como um dos propósitos identificar a capacidade – a priori – do indivíduo de cumprir ou não determinado compromisso, ter ou não habilidade para determinada função e afins. Muitas dessas decisões, que se baseiam nos dados tratados, geram prejuízos para o titular dos dados pessoais, porque se embasam em vieses discriminatórios. Nessa seara, a tutela jurídica dos dados deve combater o tratamento de dados com vieses discriminatórios, sejam dados sensíveis ou não. Os dados representam, na sociedade e na economia da informação, a identidade do indivíduo; muitas vezes são o único retrato que determinada

organização possui sobre uma pessoa. Dada a relevância dos dados nesse contexto, a tutela jurídica deve ser sofisticada (Mendes, 2014).

A tutela dos dados pessoais garante a autonomia informacional, mas também o protege de situações discriminatórias. Em âmbito internacional, assim como no Brasil, a disciplina da proteção de dados foi concebida, desenvolveu-se e passou por muitas evoluções, em razão das transformações sociais, econômicas e tecnológicas. Trata-se, atualmente, de mais de cinco décadas de desenvolvimento da tutela jurídica dos dados pessoais, por isso os desafios, ao longo desse período, também se modificaram.

Mayer-Schönberger (1997) foi o responsável por dividir as leis de proteção de dados em uma classificação evolutiva, o que é muito útil para fins didáticos e para compreender o panorama da matéria nas últimas décadas. O autor propõe uma classificação com quatro gerações de leis, que iniciam em abordagens mais restritas e técnicas e avançam, assim como a tecnologia, para noções mais amplas e expansionistas. Sobre isso, Doneda explica:

> [...] vislumbra quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais. (Doneda, 2011, p. 96)

A demanda regulatória para proteger os dados pessoais surgiu com a formação do Estado Moderno. Após a Segunda Guerra Mundial, uma configuração do funcionamento burocrático do Estado demandou a coleta de informações pessoais dos cidadãos, para coordenar ações sociais com vistas a crescer ordenadamente. Mais do que isso, a configuração do Estado de bem-estar social como relembrado anteriormente, incluía a intenção de utilizar informações dos cidadãos como base para alimentar novas políticas de bem-estar. A primeira geração de leis surgiu como reflexo dessa demanda estatal, da preocupação do Estado Moderno com o processamento massivo dos dados pessoais, de forma a garantir a estruturação do Estado, inclusive (Bioni, 2019).

Temia-se que o uso dos dados das pessoas ensejasse regimes autoritários, arbitrariedade e uma vigilância ostensiva, então a própria tecnologia foi “domesticada” para se orientar por valores democráticos e havia controle dos bancos de dados, por meio de análise e autorização para que eles funcionassem. A primeira geração de leis, portanto, refletia o próprio estado da tecnologia do momento: os bancos de dados eram limitados e a quantidade de atores envolvidos na coleta e no processamento também o era, embora tivessem grande porte, não se comparam ao fenômeno do big data. O núcleo das primeiras leis girou,

portanto, em torno dessas concessões para que os bancos de dados funcionassem e nas normas de controle para que os órgãos públicos fizessem essa fiscalização. Como o Estado era o utilizador principal – senão único – dessas informações pessoais, as leis enfatizavam o papel do estado nesse controle (Doneda, 2011).

A primeira geração de dispositivos jurídicos de proteção de dados pessoais surgiu na década de 70, com o processamento eletrônico não apenas nas Administrações Públicas, mas também nas empresas privadas, e por conta das iniciativas de centralizar os bancos de dados em grandes bancos nacionais. Entre os exemplos de normas da primeira geração, estão: a lei do Estado Alemão de Hesse (1970), a lei de Dados da Suécia, o Estatuto de proteção de dados do Estado alemão de Rheinland-Pfalz (1974), etc. Um caso nos Estados Unidos foi muito importante pela reação que a população teve ao projeto, conhecido como caso do National Data Center. Esse projeto nunca saiu do papel pela reação popular (Mendes, 2014).

A proposta, feita em 1965, visava a criação de um banco de dados único, a nível nacional, que reuniria todo tipo de informação de todos os cidadãos americanos, como data de nascimento, registros de impostos e até mesmo registro criminais. Depois de vários debates na arena pública, e da ampla divulgação dessas reflexões nos meios de comunicação, as críticas estimularam um grande debate público sobre o potencial lesivo, violador, da centralização de dados, para a vida dos cidadãos. A reação dos cidadãos americanos foi muito forte porque, para eles, tal iniciativa oferecia um poder inigualável ao Estado Americano, em termos de controle sobre a vida das pessoas. O National Data Center nunca foi construído (Mendes, 2014).

O problema do projeto era a lógica tecnocrática que o ensejou. Os idealizadores do National Data Center sequer refletiram sobre o que o projeto significava, em termos de privacidade para os cidadãos, porque estavam focados na eficiência técnica, na funcionalidade do Banco para o planejamento administrativo. Como aquele terreno era muito recente, a sociedade civil e diversos setores reagiram imediatamente.

Do ponto de vista técnico e burocrático, sem dúvidas, havia grandes vantagens em concentrar todas as informações em um único pólo. Isso significaria, com o nível tecnológico da época, acessar as informações de uma única fonte, de forma mais rápida, ter informações unitárias, racionalizar as ações do governo e facilitar os planos de ação estatal para desenvolvimento socioeconômico, sem mover efetivos diferentes para manter uma quantidade substancial de informações dos cidadãos. Porém, ignoraram a autonomia e o poder de controle que tal projeto oferecia para o governo, de maneira a desequilibrar completamente o direito à

privacidade e à personalidade do indivíduo em relação aos seus dados pessoais (Doneda, 2020).

O que marcou a primeira geração de normas de proteção de dados foi esse foco governamental e gerencial que, pela configuração dos atores que tinham acesso aos dados, se tornou uma categoria de normas voltada para dominar o uso da tecnologia, limitar o acesso e obter controle sobre os bancos de dados. Porém, o processamento de dados ocasionalmente ultrapassou a esfera governamental, o que aumentou a quantidade de atores que se dedicava a coletar e tratar dados pessoais. Na mesma medida, aumentou o número de bancos de dados que deveriam ser regulados, segundo a estrutura normativa vigente. Com um cenário mais plural em termos dos agentes de tratamento, eram necessários novos instrumentos jurídicos, capaz de acompanhar a rapidez do processo de desenvolvimento da tecnologia e de pluralização do tratamento de dados (Bioni, 2019).

Uma característica marcante das legislações de proteção de dados que surgiram na década de 70 é sua perspectiva funcional, com o controle dos dados ex ante, ou seja, condicionados à autorização previa para funcionamento. Percebe-se que essa geração de leis não considerava o direito à privacidade ou a autodeterminação informacional como bases para as normativas, tinham como intuito principal o controle rígido dos procedimentos de autorização do funcionamento dos bancos de dados. No que se refere ao caso do *National Data Center*, inclusive, entende-se que o debate público teve um grande papel no bloqueio do projeto, mas a transformação tecnológica foi o que descredibilizou o projeto, já que, com o avanço da tecnologia, tornou-se possível descentralizar os dados eletrônicos, em pequenas unidades organizacionais, seja do governo ou da iniciativa privada. Essa configuração expôs a fragilidade das normas da primeira geração, porque a criação de bancos de dados proliferou-se e tornou as normas existentes ineficazes para a proteção dos direitos dos titulares (Mendes, 2019).

A segunda geração de leis foi caracterizada por uma mudança na estrutura regulatória, porque era preciso se preocupar não apenas com a ação estatal no tratamento de dados pessoais, mas também com a regulação da atividade privada. A ação limitada dos órgãos de autorização, advinda da primeira geração de normas, era inviável, porque os bancos de dados haviam se proliferado e havia muitos atores envolvidos no tratamento. Era impossível suprir a demanda de autorização e funcionamento dos bancos de dados. A mudança de chave da segunda geração de leis é a transferência da responsabilidade de proteger os dados para os próprios titulares. A partir daí, cabe ao cidadão a ingerência de seus dados, por meio do consentimento, e ele passa a fazer escolha no que tange à coleta, uso e comportamento de seus

dados. Não era mais o Estado o regulador central, mas o próprio cidadão. Essa nova fase normativa priorizou o direito à privacidade e às liberdades; nesse momento, proteção de dados pessoais e privacidade se tornam mais íntimos (Bioni, 2019).

A segunda geração de leis sobre o tema já representou uma mudança de consciência na esfera da proteção dos dados, motivada pelo crescimento dos bancos de dados informatizados. O primeiro modelo dessa geração foi a lei francesa de proteção de dados pessoais de 1978. A característica central dessas normas, como mencionado anteriormente, é o foco no conceito de privacidade e no posicionamento da proteção dos dados como uma liberdade negativa. Essa evolução refletiu duas coisas: a impossibilidade de que o Estado regulasse sozinho os bancos de dados, já que a informatização havia se tornado muito extensa, e a insatisfação dos cidadãos, que requeriam instrumentos que defendesse os seus interesses diante da assimetria informacional. Se antes as técnicas de controle dirigiam-se imediatamente à tecnologia, para 47ontrola-la como algo doméstico, nessa fase normativa as autoridades de controle atuam como auxiliares, não mais como órgãos de autorização. Doneda argumenta:

> Estas leis apresentavam igualmente seus problemas, o que motivou uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão – ou seja, a atuação direta da liberdade do cidadão de interromper o fluxo de informações pessoais – implica não raro na sua exclusão de algum aspecto da vida social. (Doneda, 2020, p. 167-168)

Como o tema dessa dissertação é consentimento, é necessário analisar uma controvérsia muito relevante da segunda geração de normas. À primeira vista, pode parecer exclusivamente positivo a mudança de chave normativa, que levou os dispositivos a considerarem melhor o direito à privacidade. Porém, como o consentimento passou a ser uma das chaves para o tratamento dos dados, questiona-se em que medida ele é efetivo, num contexto no qual não disponibilizar esses dados podem resultar em exclusão social. Mendes (2019) explica que há uma relação complexa que precisa ser encarada. Se por um lado o Estado Social tem dificuldade de assegurar a liberdade informacional sem comprometer as funções de sua burocracia, por outro, principalmente na relação com entes privados, é difícil exercer o direito à privacidade informacional, posto que há uma lógica de *pegar ou largar*.

Ou seja, o exercício do direito à privacidade informacional pode impedir que o indivíduo acesse determinadas facilidades, que só estão disponíveis caso ele conceda as suas informações pessoais. Esse paradigma, que surgiu na segunda geração de normas, ainda tem

profunda relevância para a discussão de proteção dos dados pessoais. Destaca-se que, naquele momento, o consentimento parecia uma assinatura única, ou seja, não carecia de análise, informação e revisão contínua para o tratamento dos dados (Mendes, 2019).

Uma limitação da segunda geração de normas, que ensejou um novo paradigma, foi a compreensão de que, naquela dinâmica, o fornecimento de dados pessoais se tornou um requisito indispensável para participação social. O que deveria ser uma exceção, e que na primeira geração de leis focava na autorização de funcionamento, havia se tornado uma regra, da qual os titulares dos dados não poderiam fugir. A coleta, o tratamento e o uso dos dados pessoais se tornou uma prática comum, tanto os Estados quanto os entes privados utilizavam em larga escala as informações pessoais que conseguiam dos indivíduos. Passaram a considerar os dados pessoais como condição *sine qua non* para funcionamento tanto da estrutura estatal quanto da atividade privada. Os cidadãos, nessa equação, se tornaram invalidados pois, caso houvesse questionamento do uso dos seus dados, isso significaria uma exclusão de algum acesso importante a serviços, produtos ou políticas, em sua vida social. Era uma rua sem saída, nesse sentido (Doneda, 2011).

A terceira geração de leis busca ampliar o papel de protagonismo do indivíduo, mas com observância dos direitos que os titulares possuem, em termos de autodeterminação informacional, sobre os seus dados. Um dos aspectos mais emblemáticos da segunda geração de normas, que foi a centralidade do paradigma da privacidade, ensejou uma nova reflexão na terceira leva de normas. Não bastava transferir para os indivíduos a responsabilidade pelos seus dados, era preciso oferecer mecanismos de vigilância, de acesso à informação, para que os titulares de dados efetivamente acessassem as suas informações. Nessa etapa, as normas buscaram assegurar que os indivíduos tivessem direito a acompanhar todos os movimentos que seus dados faziam, desde a coleta até o tratamento e como esses dados eram utilizados para tomar decisões (Mendes, 2019).

Essa terceira geração de leis surgiu na década de 1980 e sofisticou a tutela dos dados pessoais. Embora tenha continuado centrada no cidadão, ela ampliou a proteção e a autonomia, diante dos desafios enfrentados pelos titulares de dados para acessar os seus direitos. Num contexto em que os cidadãos eram excluídos caso questionasse sobre os usos de seus dados, era necessário garantir instrumentos que impedissem essa violação. Os indivíduos podiam não apenas recusar o fornecimento dos seus dados, o que era inviável por conta da exclusão de setores da vida social, mas efetivamente exercer a liberdade sobre suas informações. Há um novo conceito de proteção de dados pessoais a partir dessas normas, que compreende a proteção como um processo complexo, no qual muitas vezes a liberdade do

titular de decidir é afetada por diversos condicionantes. A perspectiva de estabelecer novos meios de proteção proporcionou maior exercício de autodeterminação informacional (Mendes, 2011).

Os autores são unânimes em indicar que é nessa fase que a terminologia "autodeterminação informacional" ganha contornos reais. Ela surgiu como uma extensão das liberdades presentes na segunda geração, que foram ampliadas para a nova estrutura de leis da terceira geração. A autodeterminação informacional era um privilégio de poucos. Na terceira geração, há uma compreensão de que o tratamento de dados não é uma etapa única, mas um processo composto de várias fases. Portanto, o simples consentimento do indivíduo para o tratamento de seus dados não era o suficiente para garantir os seus direitos. Como havia várias fases nesse processo, procurava-se garantir que o indivíduo titular dos dados estivesse incluso em todas as fases o tratamento de dados, inclusive que os responsáveis pelo tratamento tinham o dever de informar como os dados eram utilizados (Doneda, 2011; Mendes, 2014; Bioni, 2019).

O direito à autodeterminação informativa, no entanto, esbarrava em questões sociais e econômicas importantes. Era considerado como um privilégio de poucos, porque os custos de enfrentar o exercício dessas prerrogativas, do ponto de vista econômico, eram muito altos. Um dos processos que marcou a terceira geração foi a decisão do Tribunal Constitucional alemão, em 1983, que declarou parte da lei do censo como inconstitucional. Na referida decisão, o Tribunal, à luz de uma interpretação da lei federal de proteção de dados pessoais, declarou que os cidadãos têm o direito à autodeterminação informacional, portanto, total controle sobre os seus dados (Mendes, 2019). Sobre a evolução após o julgado no Tribunal alemão, Mendes destaca:

> Nessa formulação de um direito à autodeterminação informativa, o Tribunal reconheceu uma carga participativa muito maior que a reconhecida pelas interpretações das normas de proteção de dados pessoais em períodos anteriores. A principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre "tudo ou nada". (Mendes, 2019, p. 40)

O mesmo julgado focou também nos deveres para quem coleta e trata dados pessoais, o que, embora possa minimizar o protagonismo do titular de dados em torno de suas informações pessoais, também avança em responsabilização daqueles que realizam atividades de tratamento. A responsabilidade não é exclusiva dos titulares, os agentes de tratamento devem observar boas práticas (Bioni, 2019).

O consentimento balizou as normas em proteção de dados pessoais desde a segunda geração, mas havia questionamentos sobre a efetividade de um quadro normativo que alocasse todo o poder na escolha dos indivíduos. A emergência do consentimento gerou fissuras em diversas relações sociais, já que o uso dos dados pessoais era considerado como uma condição de aperfeiçoamento em diversos setores. Não apenas para a burocracia governamental, é claro, mas principalmente no acesso às relações de consumo. Os dados pessoais eram chaves dessas relações, por isso havia um custo social tão amargo em recusar fornecê-los (Bioni, 2019).

Mesmo que o ideal de autodeterminação informativa tenha crescido nesse período, sua existência no mundo real era limitada, porque, ao exercer controle seguro sobre suas informações pessoais, os titulares tinham que optar por uma das duas coisas: ou arcar com os custos monetários para exercer seus direitos ou arcar com os custos sociais de não acessar bens e serviços. Uma outra controvérsia, que envolve o consentimento, era a reflexão de que, ao autorizar o processamento de dados pessoais, em caso de violação do direito do titular, ele teria dificuldade de lutar por reparação, posto que havia consentido previamente com o tratamento. A noção de consentimento naquele período era quase um presente para que os agentes de tratamento, em algumas situações, alegassem que o indivíduo aprovou o uso, portanto não haveria violação (Mendes, 2019).

Por isso, a quarta geração de normas buscou resolver diversos problemas apresentados nos dispositivos anteriores. Uma das evoluções foi o deslocamento do enfoque individual que havia como paradigma nas duas gerações anteriores. Havia muitas desvantagens em considerar exclusivamente o consentimento, e de uma perspectiva individualizante, então a quarta geração procurou enfocar o problema da informação de forma geral, ao assumir que as escolhas individuais não podem ser a única base para tutela dos dados pessoais, é preciso constituir elementos coletivos de proteção. Esse quadro normativo fortaleceu alguns pontos, por exemplo o reconhecimento de que as entidades de coleta e processamento dos dados possuem uma abundância de poder em detrimento do titular de dados, então reconhecer simplesmente o direito à autodeterminação informativa não era suficiente, era preciso ter medidas mais eficazes. Do outro lado, paradoxalmente, houve uma redução do protagonismo individual na autodeterminação informativa, porque se compreendeu que algumas modalidades de tratamento não podem estar à mercê exclusivamente de uma decisão individual, é preciso uma proteção extensa, em alto grau, para oferecer o cuidado necessário (Doneda, 2011).

O interessante é que as normas divergem no sentido de quais problemas buscaram enfatizar. Algumas fortaleceram a posição dos indivíduos e seu poder de controle, enquanto outras retiraram parte do controle individual, sobretudo no que se refere a dados considerados como sensíveis, cujo tratamento pode acarretar algum tipo de discriminação. Nessa esfera, a disposição individual não é o suficiente. Outra característica que surgiu na quarta geração de leis e que se tornou comum em diversos países, foi a edição de normas setoriais junto às normas gerais de proteção de dados. Esse cenário é muito importante para ampliar a proteção dos indivíduos e contemplar melhor as hipóteses de tratamento dos dados pessoais, com observância às necessidades específicas de cada setor. Muitos países europeus, por exemplo, conduziram a proteção aos dados pessoais por meio de regulamentações gerais, mas com adoção de códigos de conduta setoriais (Mendes, 2014). Num importante resumo sobre o processo evolutivo das normas de proteção de dados pessoais, Mendes conclui:

> Como se pôde perceber a partir dessa análise evolutiva das normas de proteção de dados, tal disciplina passou por uma transformação dinâmica e significativa no período das últimas quatro décadas, especialmente em razão das modificações tecnológicas. Ademais, percebe-se que a evolução das gerações de normas de proteção de dados pessoais reflete a tentativa de se buscar, cada vez mais, um modelo que garanta efetivamente a autodeterminação do indivíduo, não obstante as diversas dificuldades encontradas para tanto. Por fim, é notável como, ao longo do desenvolvimento do regime de proteção de dados pessoais, fortaleceu-se o conceito da tutela da personalidade do cidadão, tanto na sua vertente da proteção da autodeterminação, como na vertente de proteção dos dados sensíveis. (Mendes, 2014, p. 40)

Enfatiza-se que esse processo não eliminou o consentimento e seu protagonismo. A centralidade do consentimento permaneceu no centro da abordagem regulatória, inclusive ele passou a ser adjetivado, o que discutiremos em outro capítulo. Com a qualificação do consentimento, desenhou-se um movimento que basicamente assumiu o consentimento como sinônimo de autodeterminação informacional, há muitos desafios envolvidos, tanto sociais quanto jurídicos, na discussão sobre o consentimento. Desde que o consentimento surgiu no quadro normativo da proteção de dados pessoais, ele passou por diversas etapas, questionamentos, alargamentos e reafirmações, mas segue como um dos vetores centrais. Quase como uma representação da importância do titular de dados, o consentimento é replicado em diversos dispositivos e na hermenêutica jurídica, com base no norte regulatório definido nessas décadas (Bioni, 2019).

2.2 Antecedentes históricos da proteção de dados pessoais no Brasil

A proteção de dados pessoais no ordenamento jurídico brasileiro só se estruturou em uma Lei Geral de Proteção de Dados recentemente. Isso não significa que não há normas no Brasil que protejam os dados pessoais, porque existem previsões legais e infralegais sobre a matéria. Porém, não havia uma lei abrangente que regulasse o tema para além de uma proteção setorial. Ainda assim, é importante revisar o caminho que os dispositivos jurídicos percorreram para proteção ao tema no país.

Um dos primeiros antecedentes históricos para proteção dos dados pessoais, de forma setorial, ocorreu por meio da Constituição Federal de 1988, que contemplou o problema da informação, por meio da garantia de liberdade de expressão e do direito à informação. Em termos da noção da proteção dos dados pessoais como uma das formas do direito à privacidade, a Constituição considerou, como já mencionado anteriormente, que a vida privada e a intimidade são invioláveis, em seu art 5º. Além disso, o constituinte reconheceu a importância do fenômeno da informação, ao prever, em diversos momentos, formas de regulação desta, como postula Mendes:

> A Constituição Federal de 1988 regula o fenômeno da informação, direta ou indiretamente, por meio de diversos dispositivos, ao garantir, entre outros, a livre manifestação do pensamento, o direito de resposta, o sigilo da fonte, o acesso à informação, a inviolabilidade da intimidade e da vida privada, bem como o sigilo das comunicações de dados, telegráficas e telefônicas. A Constituição reconheceu, assim, os efeitos da circulação e da não circulação da informação sobre os indivíduos e a sociedade e buscou regular esses efeitos por meio do estabelecimento de diversos direitos fundamentais. (Mendes, 2018, p. 192)

Em constituições anteriores, as previsões que incidiam sobre a privacidade tratavam desta como um domínio físico, no geral, e não mencionavam a intimidade ou a vida privada de forma expressa. Com a tutela constitucional sobre a privacidade e a intimidade, há um avanço para o âmbito subjetivo do direito, que é relevante para o tema dos dados pessoais, na medida em que garante outras esferas de proteção da privacidade do indivíduo. Por serem direitos de caráter subjetivo - a privacidade e a intimidade - há que se considerar as fronteiras do que deve ser considerado privado e público, uma questão central para os dados pessoais, que de certa maneira quebra essa dicotomia. Certamente, o amparo constitucional ao direito à privacidade e a intimidade protegem outros direitos, mesmo que não os menciona de forma expressa. São direitos que tanto limitam a atuação do Estado, quanto dos particulares entre si,

ao resguardar o "direito de ser deixado só", mas também a autodeterminação informativa, caso considere os dados pessoais como decorrente dessa proteção (Da Rosa; Ferrari, 2014).

A Constituição Federal também foi responsável por garantir a inviolabilidade para a interceptação de comunicações telefônicas, telegráficas e de dados, assim como instituiu o habeas data, que é um importante remédio jurídico, destinado a garantir o acesso, a retificação e complementação dos seus registros. Basicamente, o habeas data é uma modalidade de direito que garante o acesso e retificação dos dados pessoais e ele representou um grande avanço sobre o tema no país. Outras dinâmicas do direito à privacidade, como a invasão de domicílio e a violação de correspondência, também estão previstas na Constituição, embora não tratem especificamente dos dados pessoais, mas do direito à privacidade como um todo. Conquanto não haja previsão constitucional expressa do direito à proteção dos dados pessoais, há o reconhecimento jurisprudencial da importância que esse tema tem para os direitos constitucionais brasileiros. Sobre o habeas data, Saito enfatiza:

> O habeas data é um instituto originariamente brasileiro, tendo sido introduzido pelo art. 5º, LXIX, LXXII e LXXVII da Constituição Federal, que o preveem como instrumento jurisdicional apto a assegurar o direito do impetrante de conhecer e retificar dados relativos à sua pessoa constantes em bancos de dados públicos, além de ser também regulamentado por lei própria (Lei nº 9.507/1997). Há uma razão de ser para o surgimento do instituto em solo brasileiro e a sua disseminação para outros ordenamentos da América Latina entre as décadas de 1980 e 1990, uma vez que em muitos destes países “persistia o trauma pelo uso autoritário da informação” promovido durante os regimes militares. (Saito, 2020, p. 63)

O habeas data foi uma importante inovação no ordenamento jurídico brasileiro. Originalmente concebido como um instituto brasileiro, influenciou não apenas o cenário de proteção de dados no Brasil, mas em outros ordenamentos latino-americanos, não por acaso: é um instuto capaz de fazer frente ao autoritarismo informacional que foi promovido em outros regimes ditatoriais na América Latina. A proposição de um direito sobre as próprias informações desafiou o trauma vivido por muitos latino-americanos em alguns contextos geopolíticos (Saito, 2020). Nos termos da Constituição Federal de 1988, ao disciplinar as hipóteses de cabimento, postula-se:

> LXXII - conceder-se-á "habeas-data":
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL, 1988, art 5º, LXXII)

Barroso (1998) explica como o ciclo militar autoritário foi sustentado pelo abuso de utilização de informações dos indivíduos. Os organismos de inteligência armazenavam muitas informações de todos, especialmente de pessoas que consideravam como ameaças ao regime. Havia serviços de inteligência voltado para a segurança estatal autoritária e esses organismos se entranharam na política ordinária, conduziam perseguições a adversários e opositores, muitas vezes extrapolando as fronteiras da legalidade e da dignidade humana. Nesse contexto, uma comunidade de informações se constituiu como um poder paralelo que não apenas se sobrepunha ao poder institucional, mas valia-se de meios ilícitos para mantê-los. O habeas data foi uma forma que o legislador encontrou de rejeitar formalmente essa prática que se constituiu no Brasil como elemento-condutor da cultura de poder nas décadas anteriores. Tinha fins políticos e jurídicos importantes, no sentido de prover ao cidadão uma salvaguarda do seu direito de autodeterminação informativa.

Um instituto como o habeas data representava um avanço enorme para as sociedades latino-americanas, recém-saídas de regimes militares, que conviviam com os resquícios e reatualizações do trauma do uso de suas informações de forma abusiva. A capacidade do habeas data de promover dignidade e autonomia da informação, de requerer do poder público essas alterações quando necessário, teve repercussão para muitos países, tanto para a tutela dos direitos fundamentais, quanto para a consolidação de culturas mais democráticas.

Por isso, Doneda (2020) acredita que o legislador não se inspirou no pensamento jurídico europeu ou norte-americano para criar o habeas data, mesmo que alguma experiência com a proteção dos dados pessoais já existisse nessas linhas por lá. Parece que a particularidade da América Latina, no que tange aos regimes militares, foi mais decisivo nesse sentido. Além disso, as tecnologias se apresentavam de forma mais defasada na América Latina, então se pode cogitar que outras influências sociais consolidaram a necessidade de um instituto como o habeas data.

Anteriormente à promulgação da lei 9.507/97, que passou a regular o direito de acesso a informações e propôs disciplina sobre o habeas data, a doutrina e a jurisprudência já tinha um perfil de como esse instituto funcionaria, com base na Constituição Federal. As formulações anteriores a lei foram, em ampla medida, incorporadas por ela. Na previsão constitucional, o habeas data tem dupla função: conhecer e retificar informações. O entendimento era de que, por meio de um único habeas data, o requerente teria acesso às informações, com um rito sumário - o mandado de segurança, por exemplo -, até que o legislador editasse uma lei específica. Uma vez acessadas as informações, se o impetrante não

tivesse ressalvas, o processo seria extinto. Caso considerasse retificá-las, haveria uma segunda fase, de caráter mandamental. Destaca-se que a jurisprudência, até esse momento, rejeitava a ideia de habeas corpus preventivo (Barroso, 1998).

Outro posicionamento jurisprudencial anterior à lei específica entendia que o habeas data só era cabível em via administrativa caso tivesse o seu pedido de acesso à informação negado. Ou seja, se o interessado não tiver formulado requerimento prévio para o detentor da informação, não cabe habeas data. Haveria a necessidade de constituição de um advogado habilitado, para juntar instrumento de mandato. Firmou-se o entendimento de que o direito de conhecer e retificar dados é um direito da personalidade, um direito personalíssimo, o que significa ser essencialmente intransferível e inalienável (Barroso, 1998). Há algum paralelo possível entre o habeas data e o direito à proteção de dados pessoais, nesse sentido, pela vinculação à titularidade.

O habeas data foi uma oportunidade do legislador de sanar um déficit de liberdade individual, que era um dos resquícios do período não democrático. Funciona como um instrumento de garantia imediata para o cidadão, com vistas a acessar direitos materiais. Porém, a introdução do habeas data no ordenamento jurídico brasileiro não foi pacífica. Luís Roberto Barroso considerou o habeas data como um remédio "simbólico", porque visava proteger direitos já passíveis de outros remédios existentes. Em termos formais, a crítica ao habeas data envolve uma questão de arquitetura constitucional, posto que o remédio visava corresponder a um problema específico, mas teve que enfrentar o desafio de demonstrar sua aplicabilidade para situações diversas (Doneda, 2020).

A Constituição limitou o habeas data na Constituição, de maneira que impediu que esse direito fosse absoluto, ao ressalvar que as informações sigilosas, imprescindíveis à segurança da sociedade e do Estado, não devem ser compartilhadas (BRASIL, 1988). Dessa maneira, o titular das informações não pode requerer habeas data nos casos em que houver possibilidade de divulgação de dado sigiloso. Não cabe ao órgão que detém a informação, no entanto, o julgamento sobre a necessidade de sigilo sobre a informação, mas à autoridade judiciária competente (Barroso, 1998).

A Lei 9.507/97 reproduziu as hipóteses previstas na Constituição e acrescentou uma terceira previsão, que representou uma importante pavimentação para o campo antecedente de proteção dos dados pessoais. Na letra da lei:

Art. 7° Conceder-se-á habeas data:

> I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público;
>
> II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
>
> III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável. (BRASIL, 1997, art 7º)

A grande mudança advinda desse dispositivo infraconstitucional é o direito do indivíduo obter informações relativas a si decorrentes de bancos de dados de diversas entidades, mesmo que sejam privadas, caso tenham caráter público. O instrumento considerou como "de caráter público" os registros ou bancos de dados que possuem informações que não sejam de uso privativo do órgão que tem as informações em seus registros. Barroso (1998) é enfático ao considerar que o habeas data teve sua razão de ser condicionada a uma circunstância histórica já superada. Portanto, mesmo que seja possível aplicá-lo para novas situações, os alvos não são mais os mesmos.

Sobre a consideração apresentada no dispositivo jurídico que envolve o conceito de "caráter público", alguns apontamentos precisam ser feitos. Primeiro que as consequências da escolha terminológica apresentada pelo legislador se arrastam até os dias atuais. Embora o habeas data não seja um remédio que represente uma mudança no que tange ao direito à privacidade, atraiu a responsabilidade de sua tutela. Ou seja: chamou a atenção, tanto do operador quanto da sociedade, para um direito negligenciado, embora ele tenha sido limitado a alguns contextos e enfrentado uma difícil trajetória no reconhecimento de sua eficácia para a proteção de dados, sobretudo no que se refere à expressão "de caráter público", mas que teve a compreensão alargada pela jurisprudência posteriormente.

Mendes (2018) relembra de um acórdão do TRF da 1ª região que decidiu pela improcedência do habeas data, porque era incabível obrigar a Fazenda Pública a apresentar informações que não eram de caráter público. O RE nº 673.707, Minas Gerais, relatado pelo Min Luiz Fux em 17 de junho de 2017, gerou um voto inédito na Corte, que posicionou um conceito de dado e informação pessoal mais amplo, como informações que dizem respeito ao contribuinte, em bancos de dados públicos ou de caráter público, e que as informações não são de uso privativo de um órgão, mas sim conteúdo do próprio contribuinte. O caminho até esse cenário, no entanto, não foi nada pacífico. Mas é fundamental posicionar o habeas data como um dos mecanismos antecessores da proteção dos dados pessoais e relembrar que esse entendimento foi anterior à aprovação da Lei Geral de Proteção de Dados no Brasil. Sobre a importância desse entendimento ela explica:

> A importância do referido trecho reside no reconhecimento de que as informações pessoais, armazenadas e processadas por outras entidades, – pelo simples fato de possibilitarem a identificação de determinado indivíduo –, podem afetar a sua esfera de direitos e, por isso, merecem a tutela constitucional a partir da garantia do habeas data. Isto é, o julgamento acabou por extrair da garantia constitucional do habeas data também um direito material à autodeterminação informativa. (Mendes, 2018, p. 198)

A maior limitação do habeas data como parte do sistema de proteção dos dados pessoais é que um sistema de proteção de dados pessoais que tem como base instrumentos voltados a uma ação judicial, após trâmite administrativo, não é adequado para as exigências que a matéria carrega, sobretudo nos dias atuais. Os problemas relacionados ao uso lesivo no tratamento dos dados pessoais são silenciosos, sorrateiros, pois os dados são processados cada vez mais "em branco", o interessado sequer percebe que seus dados foram utilizados. Se o titular das informações desconfiar que está em sua situação em que há falsidade ou incompletude dos seus dados em algum registro, ou suspeitar que há uso violador dos dados, precisa recorrer a uma via administrativa que não gera penalidade ao responsável pelo armazenamento - ou até pelo tratamento - desses dados. Então há pouca eficácia atual para uso do habeas data, inclusive ao considerar a necessidade de constituir um advogado para interpor. Nesse sentido, a trajetória árdua que envolve o uso do instrumento habeas data é pouco produtiva num contexto mais complexo de dados pessoais (Doneda, 2020).

O instituto sofreu muitas críticas, em especial porque a redação da lei brasileira considerou hipóteses restritas de aplicabilidade, sua limitação tanto ao acesso e à retificação, quanto às esferas de acesso desse direito. Mesmo que o Brasil tenha sido o ponto originário do instituto, a legislação brasileira é vista como uma das mais fracas, dentre as outras produções latino-americanas, por não ter fixado os parâmetros específicos de proteção do direito. Parte dessa questão se espelha na irrelevância que o habeas data teve, do ponto de vista da produção acadêmica e jurídica, assim como a sua utilização marginalizada na prática jurídica. Esse panorama constituiu o habeas data como, de fato, uma garantia majoritariamente do passado; certamente há utilização, mas de forma limitada, porque consolidou-se um consenso de que o instrumento é incapaz de responder às exigências atuais. Por esse motivo, sua disseminação para outros ordenamentos jurídicos foi mais frutífera e uma parte das diversas modalidades de conceber o habeas data advém da experiência de outros países (Saito, 2020).

Em tese, o habeas data não tinha como função limitadora a proteção dos dados pessoais, pois é o reflexo do acesso à informação e subscreve o exercício dos direitos políticos

e democráticos, como promoção do direito à igualdade. A lei não explicita essa questão, mas a doutrina acolheu modalidades diferentes de habeas data. Vale demonstrá-las a fim de considerar os rumos que o legislador poderia ter seguido no Brasil. Entende-se que o habeas data pode ser informativo, quando tem como objetivo o acesso aos dados, e essa modalidade se divide em três categorias: exibitória, quando os dados estão registrados; finalista, para realizar o registro; e autoral, de quem obteve os dados registrados. Outra categoria é a aditiva, que visa inserir dados, sejam dados atualizadores ou inclusivos (Saito, 2020).

Há também a modalidade retificadora, com o intuito de corrigir informações falsas ou incerta. E a de reserva, que assegura acesso apenas a pessoas legítimas. A modalidade impugnativa tem como objetivo barrar o tratamento de dados em decisões automáticas; a bloqueadora evita completamente o uso de dados. Há ainda a dissociativa, que visa eliminar qualquer associação entre o dado e o titular, mesmo que ainda conste a informação registrada; e a reparadora, com vistas a corrigir os danos decorrentes do uso inadequado das informações. Esse rol extenso de modalidades de habeas data, que marca a experiência de outros países com esse instrumento, demonstra a limitação que o Brasil teve no sentido de assumi-lo como um elemento mais eficaz para a proteção dos dados pessoais (Saito, 2020).

Os fundamentos para a tutela do consumidor, que são primordiais para o campo dos dados pessoais, foram inspirados pela constatação da vulnerabilidade que as práticas comerciais representavam para as relações de consumo. Em um mercado competitivo e voraz, compreendeu-se, no Brasil, a necessidade de proteção estatal. Não apenas no Brasil, na verdade, pois a compreensão de que havia desequilíbrio nas relações de consumo ensejou normas em diversos países na década de 1970, com o intuito de proteger os interesses dos consumidores. A repercussão do tema foi tão significativa, que a Organização das Nações Unidas - ONU se manifestou, por meio da resolução nº 39/248, de 1985, para reconhecer expressamente que há desequilíbrio nas relações de consumo e os consumidores experienciam desvantagens econômicas, de níveis educacionais e poder aquisitivo (Pezzi, 2007).

Sartori (2016) explica que o ramo do direito conhecido como direito do consumidor foi um fruto das mudanças socioeconômicas do século passado, com modificações proeminentes na produção, distribuição e no consumo, que teve como características a massificação e a despersonalização das contratações. Segundo a autora, nesse período ampliou-se a figura do intermediário, que se posiciona entre o fabricante e o comprador e foi possível visualizar o aumento do conflito entre fornecedor e consumidor, marcado pela desigualdade socioeconômica e informacional. Talvez esse tenha sido um dos primeiros cenários em que se reconheceu uma vulnerabilidade por parte do consumidor, principalmente

informacional, mas também técnica e jurídica, o que o condicionou como elo mais fraco das relações de consumido. O direito privado foi instado a evoluir, para personalizar as relações e ajustar as condutas. O avanço do direito nesse sentido foi baseado na constatação comum de que o consumidor sofre dessa vulnerabilidade, enquanto o fornecedor possui muitos mecanismos de sobrepujança na dinâmica de consumo.

Há que se destacar que a ONU já havia reconhecido os direitos do consumidor como fundamentais e universais, em 1973, e outros passos foram dados em décadas anteriores. Porém, foi com o dispositivo mencionado que o organismo recomendou para os países o desenvolvimento de uma política adequada de proteção do consumidor, que atendesse diversas necessidades, a exemplo da proteção dos interesses dos consumidores; educação do consumidor; acesso à informação adequada para os consumidores para promover escolhas fundamentadas e afins (Pezzi, 2007).

O Código de Defesa do Consumidor, ou Lei 8.078/90, foi fundamental para regular a proteção dos dados pessoais nas relações de consumo. Sua existência garantiu a capacidade legislativa de regulação do mercado, com vistas a equilibrar a relação entre fornecedores e consumidores, por meio de um regime civil distinto para controlar as relações de consumo e com o objetivo de assegurar a liberdade e a igualdade nessas transações. O Código de Defesa do Consumidor foi o resultado de um amplo debate no país durante o período histórico da redemocratização e foi fundado por um dos Atos das Disposições Transitórias, em que os constituintes determinaram que um Código de Defesa do Consumidor seria elaborado no período de 120 dias após a Constituição ser promulgada. Notadamente, a Constituição Federal já havia identificado que o consumidor era um sujeito de direitos que deveria ser preservado numa relação especial. Positivou um direito fundamental, em seu artigo 5º, XXXII, que trata da obrigação do Estado de promover uma lei em função da defesa do consumidor. Em outro trecho, a Carta Magna previu que a defesa do consumidor é um dos princípios da ordem econômica (Mendes, 2008).

A tutela dos interesses dos consumidores no Brasil é relativamente recente. O Conselho Nacional de Defesa do Consumidor foi criado em 1985 e posteriormente substituído pelo Departamento Nacional de Proteção e Defesa do Consumidor, mas o triunfo mais significativo das entidades e organizações para a defesa do consumidor foi a proclamação da Constituição Federal Brasileira, que previu essa proteção em quatro dispositivos e posicionou o país de forma mais assertiva nessa defesa. O primeiro incluiu a necessidade do Estado de prover uma lei, no período já mencionado acima. Reconhecer os direitos dos consumidores é um avanço significativo no que se refere à cidadania, mas esses direitos não devem ser apenas

reconhecidos, mas eficazes. A proteção do consumidor exigiu do Brasil uma nova mentalidade, um novo paradigma de atuação para proteção difusa e coletiva dos consumidores, não apenas uma proteção individual (Pezzi, 2007).

O Código de Defesa do Consumidor estabelece garantias e direitos para o consumidor no que tange as suas informações pessoais, em especial para os dados presentes em bancos de dados e cadastros. A ideia do legislador era posicionar um sistema moderno que estivesse, de fato, preocupado com a proteção do consumidor e tal cuidado perpassa pela utilização inadequada e abusiva que os bancos de dados fazem em relação às informações dos indivíduos. O panorama disposto no CDC revelou uma preocupação ampla do legislador com o equilíbrio nas relações de consumo e essa balança se sustenta justamente em limitar o uso que o fornecedor pode fazer das informações do consumidor (Doneda, 2020).

Essa base sólida prevista pela legislação infraconstitucional veio em decorrência da Carta Magna e uma de suas características centrais é justamente o equilíbrio entre consumidores e fornecedores. O Código de Defesa do Consumidor baliza e equilibra as relações de consumo, então não se trata de privilegiar o consumidor, mas de frear os desequilíbrios existentes nesse cenário, como Pezzi enfatiza:

> Todavia, o CDC deve ser analisado de forma conciliatória posto que a codificação da defesa do consumidor não pode ser conduzida a proteger somente os interesses dos consumidores, ignorando e, muitas vezes, inviabilizando a produção. Ao contrário, a regulamentação das relações de consumo deve compatibilizar de forma transparente, harmônica e adequada os interesses das partes envolvidas, que seja, consumidores e fornecedores. (Pezzi, 2007, p. 123)

Uma das características do CDC é a amplitude com que trata as questões de consumo, mas sem se limitar a elas, no que tange à proteção dos dados dos consumidores. Por isso, em seu art 43, há disposições muito importantes. No caput do artigo, ele aplica uma abrangência significativa das informações do consumidor, e aponta que qualquer informação existente em cadastros, fichas, registros e dados pessoais e de consumo, que estejam arquivados e que lhes digam respeito, pode ser acessado por ele (BRASIL, 1990). Nota-se na lei uma noção muito sofisticada sobre o tema, posto que ela permite que os titulares acessem informações externas aos dados de consumo, numa noção expansionista da informação: ele tem o direito a acessar qualquer informação arquivada sobre ele, seja de consumo ou não.

Com a interposição de limites ao uso das informações que o fornecedor pode fazer, o Código de Defesa do Consumidor prevê exemplos como a proibição de que o fornecedor mantenha um registro negativos sobre o consumidor por mais de cinco anos, além da

necessidade de comunicar ao consumidor sobre o tratamento de suas informações. Outro ponto importante é o direito ao acesso das informações, à correção e, a depender da situação, o cancelamento justificado (BRASIL, 1990).

Há uma forte proteção dos dados pessoais, inserida em um contexto das relações de consumo, que fornece importantes parâmetros para o tratamento de dados no Brasil. A doutrina interpretou de forma expansiva o Código de Defesa do Consumidor, de forma a identificar alguns princípios de proteção dos dados pessoais, que podem ser transferidos para outras situações. A existência do princípio da finalidade, por exemplo, que postula que os dados do consumidor só podem ser utilizados dentro dos fins que motivaram a sua coleta. Há aplicação da cláusula de boa-fé objetiva, o que pode fundamentar um princípio muito importante: a não-comercialização de bancos de dados de consumidores (Doneda, 2020).

2.3 Normas Setoriais e Análise Sistêmica: Lei Do Cadastro Positivo, Lei Do Acesso À Informação e o Marco Civil Da Internet

A evolução das normas de proteção de dados no Brasil também passou pela criação de normas setoriais, antes da construção de um dispositivo de normas gerais. Dentre elas, a lei do cadastro positivo, a lei do acesso à informação e o marco civil da internet, cada uma dessas normas contribuiu para que o país tivesse uma base sólida de proteção de dados pessoais, mesmo que ainda não houvesse uma norma geral. Pode-se dizer que esses dispositivos estimularam a urgência de normas gerais de proteção de dados pessoais.

2.3.1 Lei 23.411/2011 – Lei do Cadastro Positivo

Uma das leis importantes nesse processo é a Lei do Cadastro Positivo, lei 23.414/2011, que disciplinou a formação e a consulta a bancos de dados que contém informações de adimplemento, para formação de histórico de crédito, seja de pessoas naturais ou jurídicas (BRASIL, 2011).

Os bancos de dados têm sido utilizados para fins diversos desde o século passado, cooperando com as exigências de informações tanto do Estado quanto do mercado. Eles são operados tanto para fins simples, como arquivamento de informações básicas - nome e endereço, por exemplo - para facilitar a relação com fornecedores, quanto para responder às exigências de um mercado complexo, quando operados para traçar perfis dos usuários ou

consumidores, seus gostos, suas preferências e afins. Os usos das informações pessoais dos cidadãos não são novos, nem mesmo no que tange às relações de consumo, mas algumas normas vieram com o intuito de proteger essas relações diante dos desafios contemporâneos (Oliva; Pessoa, 2016).

No que se refere à vida creditícia do cidadão brasileiro, muitas vezes eles fornecem os seus dados para obter oportunidades de crédito. Há empresas especializadas em traçar o perfil creditício do postulante e até mesmo *negativá-los* com base nas informações cadastradas nesses bancos de dados, que representam o plano de fundo financeiro do indivíduo. Bessa (2019) explica que "negativar" é um neologismo que surgiu no Brasil, no âmbito do mercado, relacionado com as atividades que os serviços de proteção ao crédito desenvolvem no país. Como o principal registro que essas entidades realizam referem-se às dívidas vencidas e que não foram pagas, há um juízo de valor negativo em face da intenção do consumidor de obter crédito, para financiar compras de bens, produtos ou serviços. Com isso, consolidou-se a ideia de "negativado" como um símbolo do status de devedor do consumidor.

Os bancos de dados de proteção ao crédito surgiram inicialmente com o objetivo de fornecer informações adequadas as empresas que pretendiam conceder empréstimos a consumidores, parcelar o preço de uma compra ou até mesmo adiar o pagamento de uma fatura. Essas informações visavam a avaliação dos riscos de conceder empréstimo ou crédito à determinada pessoa, mas as práticas de avaliação de risco de concessão de crédito podem incluir potenciais violações de direito, o que influenciou a criação de normas de proteção dos dados pessoais nesse setor (Oliva; Pessoa, 2016).

Havia um debate no Brasil, desde o início dos anos 2000, de que era importante ampliar as informações que circulam nos bancos de dados de proteção ao crédito, para diminuir a taxa de juros que os consumidores têm que pagar. A literatura econômica defende que é importante haver tratamento de informações positivas nas entidades de proteção ao crédito, para reduzir a taxa de juros, especificamente para os bons pagadores. A aposta do tratamento de informações positivas segue a lógica de que informações precárias, que envolvem apenas dívidas vencidas e não pagas, não permitem a distinção entre os bons pagadores e os que falham no cumprimento do compromisso com crédito; sem essa distinção, o bom pagador divide os custos da inadimplência com os devedores. É importante frisar que essas considerações são focadas nas desvantagens para aqueles considerados como "bons pagadores" e que não representam, nem mesmo consideram, as circunstâncias nas quais os "consumidores ruins" se encontram. O intuito do tratamento de informações positivas,

inicialmente, era esse: cobrar do "bom pagador" uma taxa reduzida de juros, o que significaria uma motivação, inclusive, para os inadimplentes (Bessa, 2019).

O Código de Defesa do Consumidor figurou, por muitos anos, como a única norma que tratava especificamente da coleta de dados pessoais para as relações de consumo, especialmente na formação de arquivos de consumo, que são muito relevantes para os consumidores, porque afeta principalmente a sua capacidade de obter crédito frente às instituições financeiras. A Lei do Cadastro Positivo trouxe um rol extenso e inovador para os direitos dos cadastrados e extrapolou às previsões anteriores, de acesso à informação e direitos de retificação. O acesso e a retificação não são suficientes para cobrir os desafios que os cadastrados enfrentam com os usos de seus dados financeiros e de consumo. Zanatta (2019) afirma que foi identificada uma tendência de análises e de juízos de valor sobre os consumidores, alimentados pela construção de um "perfil digital", o que incluía tratamento discriminatório e acesso a dados sensíveis dos indivíduos.

Mais do que isso, a ideia de "cadastro positivo" é relevante porque as informações financeiras do postulante a crédito não incluem mais dados relativos apenas a dívidas não pagas, mas informações alternativas, que exprimam também a sua capacidade financeira e de adimplemento. Se antes os postulantes eram avaliados apenas em seu histórico de dívidas, e isso constituía um enorme empecilho para adquirir crédito, a avaliação do crédito após a Lei 12.414/2011 ampliou o número de informações analisadas para conceder crédito, de maneira mais neutra. Acerca dos objetivos desta, Monteiro destaca:

> Entre os principais objetivos desta lei estão reduzir a assimetria de informações e possibilitar a coleta de dados de adimplência após o consentimento prévio do consumidor. Afirma-se que isso possibilitaria a redução de taxas de juros e uma consequente ampliação das relações comerciais, o que favoreceria e protegeria todo o ecossistema consumerista. A norma visa, também, a adequada proteção de dados pessoais de consumo, ao prever uma série de novos direitos, entre eles o direito à explicação. (Monteiro, 2018, p. 7)

A concessão de crédito é um processo feito após uma análise de risco. Há uma coleta de dados sobre o histórico financeiro do indivíduo, para a formulação de um cadastro nas instituições financeiras, que os ranqueiam por meio de uma fórmula estatística, para atribuir uma nota ao cliente segundo sua capacidade prevista de honrar o crédito solicitado. Quanto maior a nota do cliente, menor o risco para a instituição financeira, e maior a chance de obtenção de crédito. Esse processo é chamado de pontuação de crédito e consiste justamente na coleta de dados submetidos a técnicas estatísticas. Por meio dessas informações, as

instituições decidem se aprovam ou não a solicitação de crédito de determinado postulante (Peres; Simão Filho, 2021).

A aplicação da fórmula de pontuação de crédito utiliza as principais informações cadastrais dos clientes e atribuem os pesos, de acordo, principalmente, com as políticas internas de crédito praticadas pela instituição. Esse sistema busca minorar os riscos para as empresas de crédito, em termos de inadimplência, e constitui perfis sobre os clientes. Ele interfere não apenas no limite de crédito que o cliente poderá receber, mas também na base de juros aplicada para ele e afins. O potencial discriminatório dessa operação, notadamente, é muito alto. Se o sistema de avaliação dimensiona os riscos de inadimplência, o faz por meio da identificação e divisão entre os "melhores consumidores" e os "piores consumidores".

Aos últimos, as instituições financeiras e empresas muitas vezes sequer oferecem ofertas de crédito, de acordo com a sua classificação como um consumidor ruim. As condições de concessão de crédito para pessoas consideradas como "consumidores ruins" implicam em limites menores de créditos, altas taxas de juros para empréstimos e afins e um período bem menor de adimplemento, o que inviabiliza o acesso de muitos consumidores a oportunidades de crédito, principalmente para os financeiramente mais vulneráveis (Peres; Simão Filho, 2021).

A Lei do Cadastro Positivo estimulou a construção de bancos de dados de “bons pagadores”, mas principalmente representou uma vedação expressa à utilização de informações sensíveis e excessivas, para mitigar o potencial de violação desses bancos de dados, em termos de vieses discriminatórios. O dispositivo jurídico gerou um impedimento à prática comum no mercado financeiro e nas relações de consumo, que consideram que "quanto mais informação, melhor" para avaliar a capacidade do indivíduo de cumprir com os compromissos financeiros firmados. O direito tem a obrigação de garantir a proteção jurídica da privacidade e por isso assinalou, na lei 12.414/2011, que é vedada a anotação de informações que não possuam relação com a análise de risco do consumidor e, principalmente, vedação à anotação de informações sensíveis. Dentre os dados sensíveis, considera-se aqueles concernentes à origem social, racial, étnica, de saúde, orientação sexual, convicções e afins (Zanatta, 2019).

No que se refere ao objeto central dessa dissertação, que é o consentimento, a lei sedimentou o consentimento como uma base para o ingresso nas relações que estruturam o cadastro positivo. Condicionou a relação consumidor-birô de crédito à permissão do postulante. Sobre a originalidade da sistematização do consentimento na Lei referida, Bioni assinala:

> Essa nova peça legislativa setorial acabou por trazer, de uma forma original e mais sistematizada, a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los. Nesse sentido, requer-se mais do que a simples comunicação da abertura do banco de dados, tal como fez a legislação consumerista. Exige-se o consentimento do titular dos dados pessoais que deve ser, por seu turno, informado e externado por meio de assinatura em um instrumento específico ou em cláusula apartada. (Bioni, 2019, p. 185)

O artigo 4º da lei 12.414/2011 previa justamente que a abertura do cadastro de determinado consumidor estava condicionada ao consentimento informado por ele por meio de assinatura. Porém, esse trecho foi suprimido na lei complementar nº 166, de 2019, que substituiu o consentimento informado. Na nova versão, o gestor pode abrir o cadastro com informações de adimplemento de pessoas naturais e jurídicas, mas só pode acessar o seu histórico de crédito mediante à autorização do cadastrado e deve, além disso, informar ao cadastrado sobre o cadastro, de maneira clara e objetiva, num prazo de 30 dias (BRASIL, 2019).

Bessa (2019) explicou o contexto que mudou substancialmente a questão do consentimento na Lei do Cadastro Positivo. Como a lei 12.414/2011 tinha o propósito de disciplinar o tratamento de informações positivas, por meio da adesão voluntária ao cadastro, o Brasil experienciou um resultado frustrante. Após oito anos de vigência da lei, apenas 10% dos tomadores de crédito no Brasil aderiram ao cadastro positivo. Vale frisar que o consentimento para o cadastro do postulante era fornecido por meio de assinatura em instrumento específico ou em cláusula apartada. O modelo *opt in* não teve muito sucesso, posto que os consumidores não aderiram massivamente. Em julho de 2019, com a vigência da Lei Complementar n. 166, modificou-se o consentimento substancialmente, assim como diversos dispositivos da norma que foram revogados ou modificados. O modelo *opt in*, no qual o consumidor integra opcionalmente o cadastro positivo, foi substituído pelo modelo *opt out*, em que todos estão incluídos no cadastro positivo, até manifestação contrária, por meio de cancelamento do cadastro.

Dois elementos do histórico de evolução do cadastro positivo são imprescindíveis. As entidades de proteção de crédito já estavam num processo de ampliar o rol de informações pessoais armazenadas para os bancos de dados do mercado antes mesmo da lei do cadastro positivo. O tema nunca foi pacífico na área econômica e jurídica, principalmente porque entidades de defesa do consumidor são contrárias a este porque não acreditam na redução prometida da taxa de juros, mas também porque visualizam o potencial de invasão do direito à privacidade do consumidor. Certamente, a lei do cadastro positivo é compatível com as

prerrogativas constitucionais e não violam a priori o direito à privacidade, mas há uma necessidade de atenção quanto aos usos dos dados dos consumidores. Embora o sistema *opt in* tenha sido cortado com a nova lei, ainda há garantia de que o consumidor opte por não participar do cadastro positivo. Nesse caso, há que se refletir sobre a possibilidade de que o exercício do consentimento implique em maior empecilho para obtenção de oportunidades de crédito (Bessa, 2019).

No entanto, é mister assinalar que há um arranjo de controle dos dados pessoais por parte dos consumidores na lei do cadastro positivo. O legislador avançou no que tange ao princípio basilar da finalidade, por vedar a coleta de informações excessivas, para fins que extrapolem a finalidade creditícia. Esse quadro normativo limita a coleta dos dados pessoais e contribui com a autodeterminação informacional, por capacitar que o consumidor exerça o controle sobre suas informações e não tenham os seus dados submetidos a juízo de valor (Bioni, 2019). Portanto, entende-se que o referido dispositivo contribuiu com a evolução da proteção dos dados pessoais no Brasil e estimulou, inclusive, o debate para as normas gerais de proteção de dados.

Zanatta (2019) relembra, ainda, o pioneirismo da lei do cadastro positivo no reconhecimento de um direito de revisões exclusivamente automatizadas. Interpreta-se que o legislador considerou a existência do sistema de perfilização para fins de crédito, que existe mundialmente desde a década de 1970. No art. 5º da referida lei, têm-se que é direito do cadastrado solicitar a revisão de decisões realizadas por meios exclusivamente automatizados, o que é um avanço imenso para proteger das violações de dados que ocorrem por meio dos usos de supercomputadores e da técnica de perfilização. Essa previsão pode ter sido a raiz para as regras sobre decisões automatizadas que existem na Lei Geral de Proteção de Dados. Embora a lei do cadastro positivo não proíba a prática de perfilização, ela atribuiu o direito de revisar decisões automatizadas, o que contribui para a não discriminação. Revisar decisões automatizadas é, em muitos casos, a única via para identificar violações de direitos e corrigi-las, posto que, em decisões tomadas por algoritmos, muitas vezes os dados relacionados para o tratamento possuem vieses que estarão incorporados na decisão. Nesse sentido, essa norma foi imprescindível para estabelecer bases jurídicas que inspirassem a norma geral de proteção de dados no Brasil.

2.3.2 Lei 12.527/2011 – Lei de acesso à informação

Uma breve passagem pela lei 12.527/2011, conhecida como lei de acesso à informação pública, também pode ser útil. Esse dispositivo disciplinou o direito de acesso a informações, inclusive as informações pessoais, junto à administração pública, sob a observância dos princípios internacionalmente aplicados ao tratamento de informações. Essa lei regulamenta os procedimentos de acesso às informações produzidas em todos os âmbitos da administração pública, inclusive das entidades privadas, sem fins lucrativos, que recebem recursos públicos. A norma é resultado de um longo processo democrático para garantir que os cidadãos comuns tenham instrumentos de participação e controle no destino dos órgãos públicos. Não se destaca apenas a possibilidade de acesso às informações pessoais, mas às informações de interesse público, para promover uma cultura de transparência e de controle social frente à administração pública (Calderon, 2013).

Na Lei de Acesso à informação, o sigilo é uma exceção e a publicidade é a regra. Ela segue às premissas fundamentais de que o direito à informação é operacionalizado por meio da máxima divulgação das informações, do acesso facilitado e sem custos e das limitações apenas em casos excepcionais, como nas informações caracterizadas como sigilosas. Como as informações são de interesse público, elas são divulgadas sem necessidade de solicitação, tendo como base o princípio da publicidade que rege a administração pública. Esse dispositivo converge com a seara de proteção de dados pessoais no sentido de que contribui para a redução da assimetria informacional entre o Estado e o cidadão. Embora não se confunda com um direito de acesso a dados pessoais, que é objeto da Lei Geral de Proteção de Dados, estimula uma cultura geral de segurança jurídica em relação às informações públicas - e às pessoais - e estimula, ao mesmo tempo, princípios importantes de transparência e garantia de um fluxo informacional adequado, o que é muito positivo para a proteção dos dados (Bioni; Silva; Martins, 2022).

2.3.3 Lei 12.965/2014 - O Marco Civil da Internet

Logo nos primórdios da internet, havia uma compreensão geral de que o país que criasse normas para regulamentar a internet, sob a égide de sua soberania, ficaria isolado diante das oportunidades que o mundo virtual representa. Mas o cenário se mostrou outro. Há esforços individuais e coletivos entre os países para regular a sociedade em rede (Mendes, 2014). Os debates sobre a regulamentação da internet começaram a se avolumar a partir da

década de 90 do século passado, mais precisamente nos Estados Unidos. Esse processo passou por muitas concepções sociológicas e jurídicas, expostas a longos debates acadêmicos e civis, para traçar regras aplicáveis ao controle do espaço virtual.

O direito também ofereceu muitas contribuições para a compreensão da internet como um território, mas com suas particularidades. Um dos aportes teóricos mais proeminentes foi construído por Lawrence Lessig (2000), que defendeu a regulação da rede por meio de uma modalidade tríplice, que considerasse as leis e as normas sociais, que deveriam ser implementadas na própria arquitetura do ciberespaço. A regulação da internet não poderia estar separada da construção algorítmica do ambiente virtual, porque isso significaria que o design da rede comporta violações a priori. Num modelo ideal de regulação, as leis, o mercado e as normas sociais influenciam o código e se completam mutuamente.

Certamente a aplicabilidade das leis na internet deve considerar as distinções próprias do espaço virtual, que evolui rapidamente, o que necessita de novas previsões legislativas que se ajustem a essa realidade. Já era compreendido, desde o começo deste século, que o ordenamento jurídico existente não poderia cobrir as peculiaridades do que se passa na internet. Com isso, o Brasil começou a debater há mais de duas décadas como construir uma regulamentação específica, em razão do crescimento do uso de internet no país, com vistas a proteger os direitos fundamentais (Lima, 2014). À medida que a internet se tornou um fenômeno de alta relevância social, proteger os cidadãos significava, sem dúvidas, regular as relações na internet. O Marco Civil foi o resultado mais avançado de um marco jurídico que também perpassa pela proteção dos dados pessoais, anterior à Lei Geral de Proteção de Dados.

Uma das questões complexas para o direito, no que se refere ao alcance do ordenamento jurídico na internet, é o princípio da territorialidade. Dentre as reflexões importantes para o Marco Civil da Internet, havia apontamentos sobre como abranger o mundo virtual, posto que a internet é um território dificilmente demarcável, com caráter muito fluido. Esse é um problema que extrapola a regulação da internet, que é um resultado profundo da globalização, em que muitas vezes é difícil determinar qual o território em que essas relações jurídicas de fato acontecem. Em muitos casos, um dilema importante da internet que não é comum no mundo real é a dificuldade de reconhecer de onde o interlocutor interage. Por não saber "de onde", é difícil prever uma responsabilização cabível (Pinheiro, 2021).

O Marco Civil foi um avanço nesse sentido, ao encarar a questão da territorialidade de forma prática: o princípio do endereço eletrônico, que indica a origem do interlocutor; o local

onde a conduta exerceu seus efeitos e outros elementos de localização que podem sanar tal problemática. Com o Marco Civil, a lei deve ser aplicada para qualquer atividade que tenha sido, de alguma forma, realizada a partir do território brasileiro ou em contato com o território. Qualquer ato de coleta, armazenamento e tratamento de dados, em que um dos terminais da operação tiver no Brasil, incide a legislação brasileira, obrigatoriamente (Pinheiro, 2021).

A lei 12.965/2014, ou Marco Civil da Internet, inaugurou uma norma específica para garantir os direitos dos cidadãos nas relações estabelecidas na internet. O marco foi uma reação da sociedade civil contra iniciativas legislativas que pretendiam regular penalmente a internet no Brasil. As características do Marco Civil demarcaram uma natureza principiológica, com vistas a proteger direitos e assegurar garantias aos cidadãos no ambiente eletrônico, mas sem restringir pesadamente as liberdades individuais, pois isso poderia significar uma restrição à própria capacidade de inovação em âmbito virtual. Por conta disso, evitou-se uma abordagem prescritiva e restritiva, que configuraria maior semelhança com uma norma própria do âmbito criminal (Bioni, 2019).

O marco civil começou a se desenhar a partir de uma consulta pública iniciada em 2009, e feita via internet, e teve o seu trâmite no Congresso entre os anos de 2011 e 2014. Diversos setores da sociedade civil, dos movimentos sociais e das comunidades técnicas revisaram o projeto, antes que ele fosse aprovado. O interessante do marco civil é justamente ter utilizado as redes para garantir ampla participação dos atores interessados para a construção da proposta legislativa, o que significou, também, diagnosticar e assimilar os erros e acertos, enquanto o processo acontecia. Da concepção até a aprovação da lei, foram sete anos de desenvolvimento. A regulação tem como objetivo preservar os direitos fundamentais e garantir que o desenvolvimento tecnológico não ande em um caminho contrário ao desenvolvimento da personalidade; que este esteja a serviço da sociedade, com consideração para o cenário social e econômico dos indivíduos e das coletividades, e não o contrário. Ou seja, o desenvolvimento da tecnologia não pode definir os rumos que são tomados socialmente, mas o contrário (Souza; Lemos, 2016).

O marco civil foi criado com base na concepção de que, para a internet ser livre, é preciso existir leis que garantam que as liberdades sejam usufruídas, mas de forma que não viole os direitos e garantias fundamentais e que seja possível que todos possam contribuir com as bases para promover inovação e liberdade na internet. O Brasil privilegiou uma abordagem de consideração dos direitos civis, ao invés de uma linguagem repressiva para regular a rede. É importante destacar que a construção do projeto de lei foi, de fato, submissa

a contribuições amplas e debates com diversos atores relevantes. Uma nova redação do projeto de lei foi elaborada para incluir as contribuições recebidas, até que o texto final foi encaminhado ao Congresso Nacional em 2011. O processo de tramitação legislativa também foi longo e resultou na aprovação da referida norma, em 2014 (Souza; Lemos, 2016).

O estudo desse dispositivo jurídico revela como é difícil a tarefa de legislar sobre a regulação da internet. Ele possui trinta artigos, com o objetivo de estabelecer princípios para que a internet se tornasse mais inclusiva, livre e justa para os cidadãos brasileiros. Dentre eles, destacam-se a neutralidade da rede e o acesso à internet como um direito essencial para os cidadãos, a liberdade de expressão e manutenção do conteúdo na rede, com remoção apenas em casos excepcionais. Observa também a proteção da privacidade, que tem como instrumento de salvaguarda o consentimento, a proteção dos dados pessoais e o princípio da transparência, com regras claras para todos os agentes que proveem as conexões e aplicações na web (Pinheiro, 2021).

Além disso, trata também da segurança da rede e da formação em ética digital, preferência por códigos abertos e mecanismos de responsabilização dos agentes envolvidos. Notadamente, há uma previsão ampla de diversos elementos que constituem uma internet mais inclusiva e juridicamente responsável. Cobrir tal desafio não é fácil e o marco civil da internet segue uma tendência mundial de regular a liberdade de expressão na internet de maneira adequada. Mundialmente, havia a pressão dos usuários digitais para se manifestarem "sem censura", mas os efeitos legais das práticas na internet não podem ser ignorados e o MCI implica nisso (Pinheiro, 2021).

O Marco Civil da Internet prevê, dentre os seus princípios, a garantia da liberdade de expressão, a proteção da privacidade e a proteção dos dados pessoais, que são pilares da norma, junto com a neutralidade da rede. O direito à privacidade e a proteção dos dados pessoais foram enfatizados em muitos ordenamentos jurídicos, a nível mundial, após o episódio do escândalo revelado por Edward Snowden, que revelou que os Estados Unidos conduziam atividades de vigilância global e espionagem, por meio de sua Agência de Segurança Nacional.

Esse caso revelou um esquema profundo de espionagem e trouxe a reflexão sobre os riscos aos quais os cidadãos estão submetidos, em termos de sua privacidade e dos seus dados pessoais, sobretudo com o uso da internet. A repercussão do caso Snowden ressoou no ordenamento jurídico de muitos países e o marco civil da internet endureceu seu texto, no sentido de garantir a proteção da privacidade e dos dados pessoais. A título de exemplificação, no texto inicial, o art. 7º da lei, que trata dos direitos e garantias dos usuários

da internet, tinha cinco incisos e passou a ter oito, todos direcionados à proteção dos dados pessoais (Bioni, 2019).

O reconhecimento da importância do proteção da privacidade e da proteção dos dados pessoais no âmbito da internet é um dos maiores triunfos do Marco Civil da Internet, porque corrobora com a autodeterminação informacional na rede e combate as práticas que violam direitos em âmbito digital. Demonstra, acima de tudo, uma profunda observância do legislador à amplitude dos desafios de um mundo conectado, inclusive após violações reais da privacidade em outros países. Nesse sentido, Mendes enfatiza:

> Acertou o Legislador ao estabelecer um regime jurídico de proteção de dados pessoais no âmbito da regulamentação do uso da internet no país. Tendo em vista que a internet constitui um ambiente de exercício de diversos direitos fundamentais – como, por exemplo, o direito à liberdade de expressão, associação, informação, comunicação e profissão – a proteção da privacidade e dos dados pessoais apresenta-se como um pressuposto para o exercício desses direitos. Afinal, para que o usuário possa se comunicar e se expressar livremente, é preciso que ele confie na funcionalidade e na segurança da estrutura da rede, ou seja, que ele confie que o seu ambiente de navegação está livre de vigilância e interceptações. Ao contrário, se o usuário acreditar que seus dados e informações de navegação poderão ser utilizados para fins alheios às suas expectativas ou de forma a prejudicá-lo no futuro, ele não agirá livremente no ambiente virtual nem compartilhará as suas ideias com liberdade. (Mendes, 2016, p. 39)

Sobre o consentimento no Marco Civil da Internet e a contribuição do dispositivo no que se refere à proteção dos dados pessoais, ele aparece em quatro trechos, dois deles no capítulo que trata dos direitos e garantias dos usuários. Uma dessas previsões garante ao usuário o não fornecimento dos seus dados a terceiros, de qualquer natureza, inclusive registros de conexão, a não ser em caso de consentimento livre, expresso e informado (BRASIL, 2014). Percebe-se aqui a exposição dos classificadores do consentimento, que vieram a ser muito úteis posteriormente, a partir a qualificação do consentimento na Lei Geral de Proteção de Dados Pessoais.

Ainda acerca do direito dos usuários, eles devem ter informações claras e completas sobre todas as etapas de utilização dos seus dados pessoais, seja o uso, coleta, armazenamento o tratamento. O marco civil também observa o princípio da finalidade, ao postular que os dados só podem ser utilizados para fins que, de fato, justifiquem a coleta. No art. 7º, inciso IX, a lei conclama como direito o consentimento expresso acerca da coleta, uso, armazenamento e tratamento dos dados, que deve ocorrer à parte, ou seja, destacado das demais cláusulas contratuais (BRASIL, 2014). A previsão de consentimento expresso e destacado é importante para garantir que o usuário tenha informação adequada e transparente

quanto ao uso dos seus dados, de maneira que o consentimento não se perca dentre as outras cláusulas do contrato.

Para garantir que o usuário tenha acesso adequado às informações concernentes às operações com as quais ele consentiu, os provedores de conexão à internet e de aplicações de internet devem esclarecer as suas políticas de uso, de forma clara e com ampla divulgação. Isso ocorre principalmente por meio dos contratos, tanto de prestações de serviços quanto dos termos de uso, que devem observar as normas de proteção existentes no país, para não incorrer em práticas vedadas pela legislação. Para consolidar o controle que os usuários possuem sobre seus dados na esfera digital, o Marco Civil da Internet prevê a exclusão definitiva dos dados pessoais dos usuários, a seu requerimento, em caso de término da relação contratual entre as partes, exceto nos casos de guarda obrigatória de registros. A combinação de todos os elementos destacados acima, para Bioni, contribuem com o compromisso do Marco Civil da Internet com a autodeterminação informacional:

> Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação. (Bioni, 2019, p. 187)

Certamente, o Marco Civil da Internet representou alguns avanços, no plano normativo, para a tutela dos dados pessoais, mas de forma limitada. Não é possível deduzir a segurança jurídica que o tema carece porque o dispositivo consagrou uma natureza muito principiológica, mas pouco conceitual ou operacional, o que constitui um empecilho para garantir a proteção de dados. Por exemplo, o Marco Civil tem como um de seus princípios a proteção dos dados pessoais, mas não há um conceito do que seria "dados pessoais" (Zanatta, 2015).

Bioni (2016) é enfático ao afirmar que qualquer normativa de proteção de dados pessoais perpassa, obviamente, pela consolidação de um conceito de dados pessoais. É um pilar normativo central para definir o escopo da proteção. Quando uma lei define o que é dado pessoal, ela demarca o terreno que irá ocupar, e permite sua aplicação integral. Certamente, o Marco Civil da Internet não tinha o intuito de cobrir a tutela da proteção de dados, o que deveria ser feito por uma norma geral, mas é exatamente essa lacuna que demonstra a

insegurança jurídica à qual os titulares de dados pessoais e os agentes de tratamento estavam submetidos até a Lei Geral de Proteção de Dados.

Dessa maneira, o Marco Civil buscou garantir maior segurança aos usuários da internet, sem que isso incorresse em violações quanto aos direitos já protegidos, seja pela Carta Magna ou pelas normas infraconstitucionais, mas tem as suas lacunas. Cada uma das normas analisadas nesse capítulo guiaram as premissas protetivas da proteção dos dados pessoais ou contribuíram, direta ou indiretamente, para esse cenário protetivo.

2.3.4 Notas sobre o percurso regulatório da Lei Geral de Proteção de Dados Pessoais

As seções anteriores demonstram como, até o ano de 2018, o Brasil não possuía uma norma geral de proteção de dados pessoais, então o tema era regulado por leis setoriais, como uma colcha de retalhos normativa. Esse cenário esteve suscetível a inúmeras críticas porque regular a proteção de dados pessoais de forma setorial não é suficiente e demonstra um arcabouço jurídico frágil para a complexidade dos potenciais de violação. Essa insegurança jurídica não afetava apenas os titulares de dados, mas também as empresas que tinham como base principal do seu negócio o tratamento de dados. Frente à economia da informação e com uma sociedade cada vez mais movida a dados, o Brasil se tornava menos competitivo no contexto global e até mesmo atrasado para estabelecer conexões globais com outros países que estavam à frente na segurança jurídica dos dados pessoais (Tepedino; De Teffé, 2020).

O debate público, político, teórico e jurídico sobre a necessidade de uma lei geral de proteção de dados acontecia no Brasil há muitos anos. Há muito, importantes juristas da academia brasileira apontavam a insuficiência da proteção de dados pessoais no Brasil e essa lacuna era reforçada por atores de diversos setores, pela defesa da edição de uma norma geral, para garantir um sistema coerente com padrões mínimos para o tratamento de dados no país, na esteira da evolução jurídica que ocorria em outros países. A construção da Lei Geral de Proteção de Dados e a sua aprovação pode ser vista como um resultado dessa pressão acadêmica e política, feita a muitas mãos, que contribuíram com o processo legislativo. Outros fatores externos também estimularam o avanço da norma, como a entrada em vigor do Regulamento Geral sobre Proteção de Dados da União Europeia, em 2018, assim como os escândalos relacionados com a empresa Cambridge Analytica na campanha eleitoral estadunidense de 2016, que violou gravemente o direito dos titulares de dados pessoais no país (Mendes, 2019).

As primeiras discussões em torno de um anteprojeto de lei para proteger os dados pessoais foram o resultado de uma parceria firmada entre o Ministério da Justiça e o Observatório Brasileiro de Políticas Digitais, que deu início à discussão pública, por meio de uma consulta realizada via internet, que se desenrolou nos anos seguintes. A comunidade especializada sobre o tema participou ativamente nessa construção e esse primeiro momento foi fundamental para começar a construir consensos no assunto, o que já era um grande avanço, diante da lacuna legislativa existente (Zanatta, 2015).

As iniciativas legislativas, no entanto, não foram as primeiras articulações sobre a proteção de dados no Brasil. Alguns nomes, como Danilo Doneda (2020) e Laura Schertel Mendes (2008) encaravam há alguns anos, no campo do direito civil e do direito do consumidor, a difícil tarefa de traçar um panorama da legislação brasileira e suas lacunas, para defender a adoção de um modelo de proteção de dados para o país. O trabalho de Doneda (2020) é um dos pioneiros e mais completos no tema, publicado em sua primeira edição 12 anos antes da aprovação da Lei Geral de Proteção de Dados brasileira. Nessa obra, o autor demonstrava como os instrumentos disponíveis no Brasil eram inadequados para a autodeterminação informativa e propôs, inclusive, com base na análise de experiências internacionais, os critérios para adotar instrumentos de efetiva proteção dos dados.

A jornada legislativa para aprovar uma lei de proteção de dados no Brasil começou em 2010. A primeira iniciativa foi uma consulta pública lançada pelo Ministério da Justiça, sobre um anteprojeto de lei nesse tema. Anos depois, com o Marco Civil da Internet, criou-se um microssistema de proteção de dados pessoais, mas apenas aplicado à internet. Dois anos depois, em 2015, um segundo processo de consulta pública foi lançado, com um novo texto de anteprojeto de lei, com um nível de afinação mais qualificado. A participação pública também se modificou, possivelmente em face dos acontecimentos globais nesse tema, mas também à urgência de debater a proteção de dados pessoais e a qualidade da proposta lançada. Esse texto, inclusive, se tornou a base do PLC 53/2018. Um pouco antes do impeachment da presidenta Dilma Roussef, ela encaminhou o texto do anteprojeto para a Câmara dos Deputados e esse texto se tornou o projeto de lei 5276/2016. A iniciativa desse último PL foi registrada como mais equilibrada, em termos da balança entre a proteção da privacidade e a abertura para a inovação tecnológica. Diversas entidades apoiaram o texto (Bioni, 2018).

Na primeira versão do anteprojeto de lei que foi colocada para consulta pública, o consentimento era a única base legal para tratar dados pessoais. No texto atualizado, em 2015, semelhante abordagem prosseguiu: as bases legais que hoje figuram na LGPD eram meras situações nas quais o consentimento poderia ser dispensado. Para fins desse trabalho, não há

necessidade de examinar minuciosamente os detalhes históricos de construção da Lei Geral de Proteção de Dados, apenas enfatizar que o Brasil enfrentou longos anos de discussão política e pública para chegar a um regime de proteção de dados consolidado. Diversas iniciativas, na Câmara dos Deputados e no Senado Federal, antecederam o processo de amadurecimento do texto, e sobretudo das condições, fundamentos e princípios, que regeriam o tema no Brasil (Bioni, 2019).

Em 14 de agosto de 2018, a Lei 13.709, a Lei Geral de Proteção de Dados, foi sancionada e institui um regime de proteção de dados, completando o marco normativo que o país carecia há anos. A LGPD veio para consolidar a plataforma jurídica que o Brasil necessitava para regular o tema, para além das premissas setoriais que já existiam por meio de dispositivos anteriores. A lei inaugura um modelo de proteção de dados *ex ante*, ou seja, fundado na ideia de que todos os dados são relevantes na sociedade da informação e, portanto, a tutela começa na própria suposição da relevância, antes mesmo do uso. Como os dados são uma expressão da personalidade do indivíduo na sociedade, qualquer tratamento de dados pode afetar direitos. Por isso, aplica-se uma tutela jurídica horizontal dos dados pessoais, a todos os setores. Mendes defende que a norma foi inovadora, pelo modelo de proteção que estabeleceu:

> A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo ex ante de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação. Os dados pessoais são projeções diretas da personalidade e como tal devem ser considerados. Assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais. (Mendes, 2019, p. 45)

O capítulo seguinte aprofunda as inovações advindas da Lei Geral de Proteção de Dados e discute as concepções sobre o consentimento no dispositivo normativo, assim como sua relação histórica, já trabalhada ao longo da dissertação, com a autodeterminação informacional.

3 O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

3.1 Dados pessoais e dados sensíveis

Em uma abordagem teórica, Doneda (2020) explica como o dado, diferentemente do conceito de informação, apresenta uma posição mais primitiva e fragmentada. Ou seja, é uma informação em potencial, antes de ser analisada. Um dado, descolado do seu contexto de utilização, pode não representar muitos perigos ou potenciais. É uma espécie de pré-informação, no sentido de que está em seu estado bruto, anterior a um processo de análise e de elaboração de um quadro de informações. A informação é entendida como o resultado do tratamento de um dado. É uma representação, um conteúdo, contido no dado, posterior ao seu estado de incerteza. Com a desenvoltura da manipulação dos dados, como resultado da diferença tecnológica, há uma variedade de formas pelas quais os dados se tornam informações e são utilizados. Como se expande a utilidade, como consequência, há expansão do potencial de violação. Muitas vezes esses conceitos se confundem, mas do ponto de vista jurídico, é fundamental estabelecer um conceito de dados pessoais, para dar concretude à tutela dos dados.

Nas leis de proteção de dados, o conceito de dado é mais restrito do que na literatura genérica, até mesmo no campo das teorias da informação. Dados "brutos" podem não ter significado, mas portam informações que, ao serem codificadas, possuem características importantes para a sociedade da informação. No campo jurídico e normativo, os dados são entendidos como um dos direitos que protegem a personalidade e o "pessoal" é um elemento do conteúdo, que trata de um tipo específico de informação. No General Data Protection Regulation - GDPR, que influenciou muitas leis de proteção de dados, "dados pessoais" significa qualquer informação que possa tratar de uma pessoa identificada ou identificável. É importante destrinchar o que isso significa. Trata-se de uma pessoa singular que, mesmo que não seja inicialmente identificada, possa estar ligada a um identificador, seja nome, número de identificação, dados de identificação ou outros; outros fatores, como identidade física, fisiológica, econômica, cultural também perpassam os dados dessa pessoa singular (Hoffmann-Riem, 2022).

A lei brasileira adotou um conceito amplo de dado pessoal, ao assumir, de forma preliminar, que todo dado é importante, em especial aqueles que tratam de determinadas informações da pessoa. Com isso, posicionou um conceito de dado pessoal expansionista, como qualquer informação relacionada a pessoa natural identificada ou identificável. É

importante revisar esse conceito, porque ele é um dos elementos centrais da Lei Geral de Proteção de Dados brasileira e estabelece os limites da tutela jurídica. Há duas possibilidades de conceito de dado pessoal para moldar uma normativa de dados pessoais: uma definição reducionista e outra expansionista.

Na versão reducionista, o conceito de dado pessoal se resume a informações relacionadas a pessoas identificadas e determinadas, que implicam num vínculo e direto e preciso da informação com a pessoa. Na versão adotada pela lei brasileira, há uma versão expansionista, que trata também das pessoas identificáveis - e indeterminadas, portanto - mesmo com vínculo indireto ou impreciso. Isso porque dados que pareçam irrelevantes em algum momento, e que inicialmente não façam referência a alguém diretamente, pode resultar em dados específicos, que identificam uma pessoa, ao serem cruzados com outras informações (Tepedino; De Teffé, 2020).

Na previsão da Lei Geral de Proteção de Dados, que estende o conceito para além da pessoa natural identificada, entende-se que há dado pessoal mesmo quando não houver presença imediata de identificadores diretos - ou indiretos - sobre um indivíduo, porque dados que podem conduzir à individuação da pessoa são interpretados como informação pessoal (Palmeira, 2020). Cabe a compreensão de que um dado, em si mesmo, não é perigoso. O perigo se refere à forma como o dado é utilizado, tratado e correlacionado com outras dados. É a partir dessa lógica que se entende que um dado não identificado pode se tornar uma informação potente sobre determinado indivíduo, quando em contato com outros dados.

Bioni (2019) assevera, por exemplo, que o vocabulário dos dados pessoais ganha contornos mais concretos de acordo com a utilização prática deles, em face das estratégias regulatórias adotadas em cada país. Destaca-se, além disso, que um dado pessoal não é isolado da análise contextual que o torna uma informação sobre determinada pessoa. E essa análise pode ser mais restrita, no conceito reducionista, ou mais flexível e ampla, no conceito expansionista que é adotado pela normativa brasileira.

O conceito de dados sensíveis, por outro lado, já é previsto no ordenamento jurídico brasileiro desde a Lei do Cadastro Positivo, de 2011, que foi o primeiro dispositivo a proibir a anotação de informações sensíveis para análise de crédito. A Lei Geral de Proteção de Dados trouxe um conteúdo ampliado para esse conceito, ao considerar tanto aspectos existenciais, quanto sociais, para esse tratamento jurídico. Os princípios da finalidade e da não discriminação são basilares para os dados sensíveis. O primeiro constitui a vedação da inclusão de qualquer informação, de natureza personalíssima, que extrapole a finalidade do tratamento de dados em questão. Entende-se, sobretudo no campo da Lei de Cadastro

Positivo, que as informações sensíveis de determinada pessoa não se relacionam, certamente, com a finalidade da análise de crédito, mas também há o objetivo de evitar qualquer viés discriminatório. O princípio da não discriminação conduz o tratamento de dados sensíveis e justifica a necessidade de uma tutela rigorosa. É a vedação do tratamento discriminatório que direciona os limites dos usos de dados sensíveis. Qualquer utilização de dados potencialmente lesiva, em face de sua possibilidade discriminatório, convoca regras restritivas de tratamento e constitui, em alguns casos, vedação ou limitação de uso (Mulholland, 2020).

A elaboração da categoria dos dados sensíveis, e da disciplina especificada aplicada a ela, não foi isenta de críticas. Uma dessas críticas tratava da impossibilidade de definir os efeitos do tratamento de forma antecipada, independentemente da natureza do dado. Mas essa crítica ignora a repercussão material e histórica das informações na vida dos indivíduos. Mesmo assim, afirmava-se que mesmo dados não qualificados como sensíveis, se submetidos a tratamento específico e em determinadas condições e contexto de agrupamento com outros dados, podem ser qualificados como sensíveis ou revelar aspectos sensíveis sobre determinada pessoa. A ideia seria de que um dado, em si, não é perigoso, mas o seu uso. Essa é a base do conceito de dado pessoal da lei brasileira, inclusive, mas entende-se que o percurso dos dados sensíveis é mais específico (Doneda, 2020).

O artigo 1º da LGPD sustenta a ideia de que essa é uma norma para proteger os direitos de liberdade e privacidade, mas também o livre desenvolvimento da personalidade da pessoa natural. Esse ponto é central, que se refere ao livre desenvolvimento da personalidade, porque promove a noção de que cada indivíduo tem o direito de eleger o seu modo de vida e de se desenvolver a partir do seu próprio projeto. Dessa maneira, a constituição da personalidade é livre, sem interferência de outrem, inclusive do Estado, já que se promove a autonomia individual no dispositivo jurídico (De Teffé, 2022).

Os dados contidos na categoria dos dados sensíveis expressam, no geral, um conteúdo relacionado à intimidade, à intimidade e à proteção da igualdade em sentido material, de informações que dizem respeito apenas à pessoa de direito. No sentido de desenvolver livremente a sua personalidade, a categoria também expressa o respeito e a proteção ao bojo de informações que integram a identidade pública do titular, mas que não deve ser utilizada de forma arbitrária, posto que a integração à esfera pública é uma das facetas da personalidade e constitui uma esfera de manifestação das convicções da pessoa (De Teffé, 2022).

A proibição da coleta e do tratamento dos dados muitas vezes não seria possível ou viável, porque há contextos nos quais coletar esses dados é necessário; muitos setores estariam comprometidos caso não pudessem utilizar essas informações, como setor de saúde e

organismos de pesquisa, por exemplo. Por isso mesmo, a consideração sobre os dados sensíveis varia de acordo ao regime adotado em cada país. A diferenciação conceitual dos dados sensíveis colabora com a necessidade de assumir que determinadas áreas são mais passíveis de utilização discriminatória, com maior potencial de danos aos titulares; portanto, cabe a cautela com essa categoria, mesmo para fins lícitos e legítimos (Doneda, 2020).

Nos termos da Lei Geral de Proteção de Dados, dado sensível é:

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018, art 5º inciso II)

Para além da previsão expressa dos dados sensíveis na Lei Geral de Proteção de Dados, entende-se que os dados sensíveis são uma espécie de dados pessoais que necessitam de uma proteção e tipologia diferente porque o conteúdo desses dados oferece maior vulnerabilidade ao titular. Ou seja, a proteção dos dados sensíveis não trata apenas de observar o conteúdo do dado, mas a potencialidade discriminatório do tratamento. Parte do princípio de que a utilização de certas informações é passível de maiores violações de direitos, então a limitação do tratamento incorre em uma proibição de que o uso gere discriminações ou abusos (Mulholland, 2020).

A própria criação da categoria dos dados sensíveis é fruto da observação sobre como há consequências diferentes do tratamento desse tipo de dado, em comparação com os demais. O impulso pragmático da construção jurídica dos dados sensíveis extrapola a privacidade, pois revela a proteção de um outro valor digno de tutela específica, que é o princípio da igualdade material. Não se trata certamente apenas do clássico direito ao isolamento, nesse caso, mas da observância da equidade em termos jurídicos. Os titulares de dados pessoais estão circunscritos a uma determinada configuração social, que envolve muitos tipos de desigualdades raciais, étnicas, religiosas e afins; portanto, a seleção desses dados sensíveis perpassa pela compreensão de que essas desigualdades não podem ser incorporadas pelo tratamento de dados pessoais (Doneda, 2020).

Mais do que isso, há que se refletir sobre as dinâmicas discriminatórias reais articuladas numa sociedade, para entender quais os dados devem ser incluídos nessa tutela especial. Os dados sensíveis observam a configuração social e política e como essa realidade social acarreta maior potencial lesivo para determinadas pessoas ou informações. No Brasil, os grupos mais vulneráveis socialmente e as minorias sociais são perseguidos e tem os seus direitos violados de diversas formas. No que se refere aos dados pessoais, sobretudo seus usos

em decisões automatizadas, as informações compiladas exprimem e treinam aplicações de maneira que o resultado do processamento de dados é enviesado e discriminatório (De Teffé, 2022).

Sem observar como as estruturas discriminatórias operam as aplicações e o processamento dos dados, a tutela dos dados sensíveis não tem a amplitude necessária para a complexidade do contexto. Nesse sentido, há que se observar não apenas a categoria dos dados sensíveis, mas os seus usos (Doneda, 2020). Há operações que representam maior potencial lesivo, porque a arquitetura das aplicações advém de pressupostos discriminatórios, muitas vezes. O Direito deve mobilizar reflexões para que a igualdade material seja efetivada, para romper com a utilização de características raciais, sexuais e de gênero para segregar e excluir pessoas (De Teffé, 2022). Cabem algumas notas acerca de quais usos representam maior potencial discriminatório.

O tratamento de dados sensíveis por empregadores, com usos para recrutamento, por exemplo, representam maior potencial lesivo, porque vieses raciais, sexuais e de gênero servirão para alimentar os sistemas que auxiliam nessas decisões. São críticos também os usos por companhias seguradoras, planos de saúde e governos, o que deve ampliar um cenário de violações a direitos, se as garantias de proteção aos dados pessoais sensíveis não forem observadas. Uma operação que trace um perfil do indivíduo com base em informações negativas pode levar a uma avaliação discriminatória da pessoa (Mulholland, 2020).

Dados de saúde também são críticos, em especial ao considerar planos de saúde, bancos e empregadores, porque podem gerar discriminações e escolhas com base em informações que são especiais, de exclusividade do titular de dados. Casos de perfilamento geraram tratamentos discriminatórios em diversos setores, com exemplos mais proeminentes nos Estados Unidos. Ao considerar as operações de perfilamento, que trata da formação de perfis baseados em dados, esse cenário é ainda mais crítico, o que torna o consentimento um instituto central para a não discriminação e autonomia individual. Para além do consentimento, a proibição da coleta por parte de determinados sujeitos - como empregadores - deve ser avaliada, optando-se pela exclusão da legitimidade de certas formas de coleta e tratamento.

No entendimento de Ana Frazão (2018), a inquietação especial com os dados sensíveis existe porque não apenas envolve a privacidade, mas proíbe que os dados sejam utilizados contra os titulares em operações escusas, que lhes restringiria de alguma forma no acesso a bens, serviços e direitos. Para ilustrar, ela cita o potencial dos dados biométricos ou impressões digitais para obter conhecimento sobre as características de um indivíduo, sejam

elas físicas, psicológicas ou comportamentais. Rodotà (2004) no artigo intitulado "Transformações do corpo", trata dos usos de dados biométricos e genéticos nessa era, que pode influenciar em uma série de operações de controle sobre os indivíduos, seja por parte do Estado ou de corporações. É esse potencial, de transformar o corpo em um instrumento de profunda vigilância e discriminação, que a tutela dos dados sensíveis protege o titular, mas não de forma estática; ou seja, um dado sensível pode ser dinâmico, de acordo com o uso que se faz dele. No que tange aos dados de saúde, a coleta e o tratamento desses dados é crítica porque é possível adquirir informações sobre a identidade da pessoa, mas também conteúdos preditivos. Com isso, protege-se mais do que a privacidade, mas uma dignidade geral da pessoa humana.

Frazão (2018) considera que há um fenômeno muito proeminente de publicidade comportamental, que visa a formação de perfis de consumo, que tem relação direta com a regulação do tratamento de dados pessoais, porque afeta a capacidade do indivíduo de tomar decisões, posto que a formação desses perfis muitas vezes induz o indivíduo a ações, com base em estudos preditivos, que afetam o exercício real da autonomia. Na seara do consumo e do trabalho, em especial, os riscos de utilização desses dados são enormes, em especial ao considerar os dados sensíveis. Destaca-se especialmente as violações, em esfera consumerista e trabalhistas, a empregados, consumidores e candidatos a vagas de emprego, mas o potencial lesivo desses dados extrapolam esses setores.

Por isso, Rodotà (2008) assevera a necessidade de posicionar dispositivos jurídicos estratégicos, que limitem a manipulação de dados pessoais e limite sua coleta ao mínimo necessário de acordo com finalidades legítimas, com base no princípio da necessidade e observância de outros princípios, como pertinência e proporcionalidade, para mitigar os danos. A coleta de dados pessoais se insere num contexto específico, então é preciso avaliar as mais diversas etapas de utilização desses dados, desde a obtenção até a sua finalidade. Categorizar dados como sensíveis não é o suficiente para barrar o seu uso, certamente, mas é um mecanismo de salvaguarda dos direitos dos titulares e, de forma mais ampla, dos direitos fundamentais.

O tratamento de dados sensíveis se insere num contexto global em que dados são utilizados de forma ampla, mas isso deve ser feito com cautela. Por natureza, há maiores restrições quanto à coleta dos dados sensíveis, não apenas pelo contexto, mas pelas associações possíveis entre um dado e outras informações que, conjuntas, podem adquirir potencial discriminatório. Por si só, uma informação é uma mera informação, mas em

conjunto com outras informações, e para agentes de tratamento específicos, esse uso pode lesar o titular dos dados e ferir o seu direito à igualdade material (Rodotà, 2008).

Rodotà (2004) ainda reflete sobre a possibilidade de coleta de dados em sistemas de identificação individual, ao invés de bancos de dados que contém informações diversas de uma multiplicidade de sujeitos, o que permitia tratar e analisar, de maneira centralizada, uma série de informações para tomar decisões. De qualquer maneira, aplica-se a compreensão teórica de que os dados sensíveis carecem de maior cuidado, porque há muitas experiências de violações registradas e grande potencial de ação lesiva, que fira os direitos fundamentais, a privacidade e o livre desenvolvimento da personalidade, ao promover, por meio do acesso, coleta ou tratamento de dados, efeitos discriminatórios. O que sustenta o tratamento dos dados pessoais sensíveis, e o tratamento de dados de maneira geral, embora se admita outras bases legais para tal, é o consentimento, como forte fundamento para a admissão do tratamento de dados. Dessa maneira, é fundamental compreender como a Lei Geral de Proteção de Dados definiu o tratamento, suas nuances para o tratamento de dados pessoais e de dados sensíveis, mas também suas lacunas e insuficiências.

3.2 O consentimento como base legal para tratar dados na LGPD

O consentimento é a primeira base para o tratamento de dados pessoais e é uma das fontes máximas de interpretação da lei geral de proteção de dados brasileira. Ele integrou a evolução da proteção de dados pessoais mundialmente, ao modificar a demanda regulatória e incluir uma concepção que considerasse a autonomia individual e o protagonismo do titular em âmbito regulatório. Como surgiu uma demanda para que o indivíduo tivesse controle dos seus dados, o consentimento entrou como técnica legislativa para garantir essa relação. Por conta desse protagonismo do consentimento nos dispositivos, há muitas reflexões e interpretações acerca da sua centralidade na LGPD.

Embora não seja a única hipótese para o tratamento de dados pessoais, nem mesmo superior às outras bases legais, há um centro gravitacional sobre esse instituto. Na Lei Geral de Proteção de Dados, ele é um dos instrumentos de tutela integral da pessoa humana, o que revela a preocupação legislativa com a participação do titular no gerenciamento de suas informações pessoais. A lei construiu, ainda, adjetivação - ou qualificadores - para o consentimento, para orientar regras específicas e reforçar o controle dos dados (Tepedino; De Teffé, 2020). As regras para o uso do consentimento estão presentes no art 7º da LGPD, mas o seu conceito foi previsto no art 5º, XII, que o define como uma manifestação livre,

informada e inequívoca por meio do qual o titular de dados pessoais concorda com o tratamento de seus dados, para determinada finalidade.

O consentimento é mencionado trinta e sete vezes na lei geral de proteção de dados brasileira. Além da sua representação quantitativa, ele parece ser o elemento central considerado para tratar dados, mesmo que haja outras bases legais. O consentimento parece não ter sido superado como paradigma, embora a sua operacionalização não seja suficiente para sustentar uma tutela qualificada da proteção dos dados pessoais. Seu uso é previsto no art 7º, inciso I, como hipótese para tratar dados, junto às outras nove bases legais para o tratamento. O consentimento é a regra, pois a sua dispensa ou inexigência só pode ocorrer em alguns casos. No que se refere aos dados públicos, cujo acesso é disponível, não é necessário consentimento, embora os controladores devam observar, mesmo nessas condições, garantia dos direitos dos titulares e a observância dos princípios que regem a lei.

A lei utiliza duas nomenclaturas diferentes sobre dados públicos, são elas: "dados pessoais de acesso público", no §3, e "dados tornados manifestamente públicos pelo titular", no §4º do seu art. 7. A primeira categoria representa uma informação pessoal de fácil acesso, disponível a todos. Um registro de propriedade de um imóvel, por exemplo, é uma informação pública, disponível em cartório. A lei permite o tratamento dessas informações sem a necessidade do consentimento, desde que siga princípios básicos, como a finalidade e a boa-fé, além do interesse público que justificou a disponibilidade desses dados (Brasil, 2018).

Se a informação é pública, ela pode ser utilizada, mas cabe ao controlador a interpretação do contexto de acesso dos dados. O tratamento posterior deve respeitar, e ser compatível, com o contexto que o originou, para proteger os titulares de violações, mesmo de dados disponíveis para todos. Os dados "manifestamente públicos pelo titular" seguem outra lógica, pois são dados que se tornaram públicos por uma ação do titular, pelo compartilhamento ativo deste, onde a informação não apenas é de sua autoria, mas divulgada por ele. É o caso, por exemplo, de uma informação divulgada pelo titular em redes sociais (Frahjof; Mangeth, 2020).

Há dois entendimentos sobre esse parágrafo e, na lei geral de proteção de dados, apenas um prevaleceu. O primeiro entendimento, que inclusive foi utilizado em ações civis, era de que essa informação poderia ser utilizada livremente, mesmo sem a correlação com alguma base legal, porque a única base legal adotada seria o consentimento, mas este estaria dispensado diante da publicidade do dado. O segundo defende que a publicização da informação pelo próprio titular dispensa a exigência do consentimento, mas a coleta e tratamento dessa informação manifestamente pública deveria ser baseada em uma das

hipóteses de tratamento previstas pela lei, esse é o entendimento dominante, positivado pelo art 7., §7º, incluído posteriormente.

Um dado pessoal nunca é irrelevante, mesmo público. Todo tratamento de dados pessoais deve observar os princípios, direitos e deveres estabelecidos pela norma geral de proteção. Dessa maneira, um processamento incompatível com o contexto de produção do dado é ilegítimo, embora seja difícil garantir a eficácia desse postulado, no sentido da fiscalização, uma vez que não há necessidade de obtenção do consentimento. O parágrafo 7 do art 7., inclusive, deve ser interpretado como sinônimo de que a finalidade do tratamento não pode ser discriminatória ou abusiva, além de ter um fim específico e limitado, sustentado por outras bases legais. O compartilhamento de dados pessoais entre controladores, independentemente da natureza do dado, segue a imperatividade do consentimento (Frahjof; Mangeth, 2020).

Segundo Bioni (2019), essa confusão decorre da cultura jurídico-legal nacional de interrelação direta da proteção dos dados pessoais com a privacidade, como se fossem sinônimos. Acredita-se, nessa concepção, que algumas informações devem receber maior proteção pela sua confidencialidade, o que dispensaria a preocupação em dados públicos, quase como se eles não fossem passíveis de proteção. A questão central não é apenas a natureza desses dados, nesse caso, mas a finalidade para a qual ele será utilizado ou o que justifica a sua disponibilização. A legalidade ou ilegalidade do tratamento tem relação com a compatibilidade da finalidade com o dado. Se houve publicização, deve-se considerar o ambiente de divulgação, para promover privacidade contextual. O uso indiscriminado não é permitido pela lei, nem mesmo dos dados públicos. Por fim, ele conclui:

> Portanto, as figuras de dados de acesso público e manifestamente público, além de estarem dentro do escopo de aplicação da LGPD, também estão sujeitas a um regime que impõe uma série de requisitos para o seu tratamento à luz do referencial da privacidade contextual. O caráter pedagógico dessa taxonomia é não deixar dúvidas de que tais tipos de dados não deixam de ser pessoais, rompendo com a chave binária do público privado. E, por fim, assegurar uma esfera de controle por parte dos titulares dos dados, ainda que não haja o seu consentimento para tanto. (Bioni, 2019, p. 344)

Examinar os qualificadores do consentimento é fundamental para compreender suas potencialidades e os seus limites no contexto de assimetria informacional. Dessa definição contida na LGPD, enfatiza-se que o consentimento deve ser livre, informado, inequívoco e para uma finalidade específica (Brasil, 2018). O adjetivo livre significa que o titular pode aceitar ou não a utilização dos seus dados, ou seja, não deve ser forçado a consentir. Há uma

vedação expressa ao tratamento de dados que impliquem em um vício de consentimento, qualquer situação ou intervenção que viciem essa condição devem ser examinadas.

Existe um problema sério nos casos concretos, posto que há assimetrias informacionais, e nos contratos, que muitas vezes obriga o titular dos dados a consentir ou não poderia usar determinado serviço ou aplicação. Se não há poder de barganha do cidadão, ou a possibilidade de acessar um serviço sem comprometer inteiramente os seus dados a contratos escusos, entende-se que há vulnerabilidade do titular. Essa assimetria de poder é um dos pontos críticos da lógica da era informacional, que reserva para as empresas, serviços e organizações a possibilidade de obrigar, silenciosamente, que o indivíduo consinta com o tratamento dos seus dados.

O consentimento esteve presente no direito privado como uma figura inclusa nos temas dos defeitos do negócio jurídico. Em diversas hipóteses, tutela-se a declaração de vontade da pessoa como um bem jurídico, que deve assegurar a liberdade e a consciência no fazer. Restada imperfeita a formação desse elemento, o negócio jurídico pode ser anulado por vício de consentimento. Sendo assim, a forma expressa do consentimento na LGPD transmite um diálogo com o Código Civil brasileiro, que tem elementos históricos da adjetivação que o consentimento possui no ordenamento jurídico do país, no que tange aos defeitos do negócio jurídico. O adjetivo livre, em especial, diz respeito às opções que o titular possui em relação ao dado coletável. Para garantir o exercício do livre-arbítrio no tratamento de dados, deve-se avaliar em que medida determinado serviço, operação e aplicação permitem ao titular dos dados consentir parcialmente, por exemplo. Na dinâmica do "tudo ou nada", que rege o funcionamento de muitas arquiteturas digitais, há uma assimetria de poder que impede o cidadão de calibrar as suas escolhas (Bioni, 2019).

Há operações e aplicativos atualmente, descritos por Bioni (2019) como painéis de privacidade, que buscam estabelecer políticas de privacidade com adesões parciais, o que muda completamente as permissões nos contratos de adesão. Essas ferramentas buscam permitir que o titular participe da tomadas de decisões dos seus dados de fato, com um leque de opções de confirmação ou recusa. O consentimento, nesse caso, foge à lógica binária e adquire mais nuances, porque o cidadão pode permitir autorizações fragmentadas para o tratamento dos seus dados, apenas no que considera razoável. Com o fatiamento do controle dos dados, o titular dos dados opta por algumas funcionalidades e, com isso, permite apenas a utilização dos dados necessários para essa aplicação.

Na prática, são configurações de privacidade personalizáveis, o que é um grande avanço para contrapor as estratégias escusas que fazem do consentimento livre uma obrigação implícita. Sobre a urgência de modificação dessas estratégias, Tepedino e de Teffé destacam:

> Sabe-se que não são todos os sujeitos que têm a habilidade de negociar ou a possibilidade concreta de rejeitar a condição imposta nos termos de serviços e políticas de privacidade das plataformas. Assim, ao invés de realmente concordar com o uso dos próprios dados, o que se verifica na prática é a obediência do titular à vontade das empresas, o que facilita práticas de controle e de uso indiscriminado de dados pessoais. Dessa forma, mostra-se necessário realizar mudanças significativas tanto na maneira pela qual o consentimento é implementado nos termos e políticas, quanto no desenho e arquitetura das plataformas. (Tepedino; De Teffé, 2020, p. 95)

O consentimento granular deve estar associado a outros mecanismos para que o titular dos dados possa exercer adequadamente o seu direito. Nesse sentido, não basta que o consentimento seja livre, ele precisa ter um espaço à parte das outras informações sobre determinada operação que o indivíduo deseja acessar. Não há consentimento livre se ele estiver acoplado a outras operações de tratamento. Ou seja, se determinado indivíduo consente com o uso dos seus dados para uma rede social, por exemplo, e essa rede social vende espaços publicitários para algumas empresas, os dados do indivíduo não pode ser armazenado ou utilizados como base para essas publicidades, posto que o cliente só consentiu com a operação da rede à qual forneceu os seus dados. Qualquer desvio dessa relação pode ser considerado como uma violação. Sobretudo no que se refere a esse tipo de publicidade comportamental, a cautela é importante para proteger o direito dos titulares de dados (Tepedino; De Teffé, 2020).

O vocábulo informado infere que o titular deve dispor das informações necessárias para avaliar em que medida o acesso, coleta e tratamento de dados realizado pelos agentes de tratamento corrobora, ou não, sua percepção sobre como seus dados devem ser tratados. A informação é fundamental para que o consentimento livre e consciente realmente seja efetivo, mas deve ser mais do que o simples ato de informar. Os responsáveis pelo tratamento de dados, para garantir a transparência na utilização dos dados dos titulares, devem evitar o vocabulário extremamente técnico, para diminuir a assimetria informacional entre as partes. É salutar que determinadas condições de popularização da linguagem técnica seja atendida para que, ao cumprir o requisito do acesso à informação, não reste uma outra armadilha: a opacidade. Acerca da relevância da informação para o combate às assimetrias informacionais, de Teffé e Viola afirmam:

> A informação é fator determinante para a expressão de um consentimento livre e consciente, direcionado a tratamento específico, para determinado agente e sob determinadas condições. Destaca-se, aqui, a importância dos princípios da transparência, adequação e finalidade para restringir tanto a generalidade na utilização dos dados quanto tratamentos opacos. Para diminuir a assimetria técnica e informacional existente entre as partes, exige-se que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados. (de Teffé; Viola, 2020, p. 9)

O Conselho Europeu de Proteção de Dados, órgão independente da União Europeia responsável por garantir a aplicação do Regulamento Geral de Proteção de Dados posicionou uma orientação acerca do consentimento e da opacidade, que contribui para a compreensão do que significa, de fato, consentimento informado, inclusive por enfrentar o mecanismo - consciente ou não - de assimetria informacional, que informa ao titular dos dados de forma ininteligível. No documento em questão, eles afirmam que os controladores devem usar uma linguagem clara e palpável, em todos os casos. A mensagem precisa ser entendida por qualquer pessoa, não apenas por especialistas e advogados. Toda a cadeia de informação complexa, como políticas de privacidade e linguagem jurídica, devem ser evitados no fornecimento de informações. O consentimento deve ser claro e distinto, de forma acessível. Essa é uma condição para que as pessoas tenham pleno acesso a informações relevantes; esse material não deve ser escrito em letras minúsculas com expressões técnicas, mas sim destacadas dos termos e condições gerais, para avaliação clara do titular (European Data Protection Board, 2020).

Nessa seara da opacidade, Mendes e Fonseca (2020) tratam das limitações cognitivas que o titular dos dados possui e que influencia em seu processo decisório. O paradigma do consentimento inclui uma avaliação acerca dos custos e benefícios envolvidos em consentir com os termos, em primeiro lugar. Uma vez minuto de informações amplas sobre o tratamento dos dados, o titular pode pesar e contrapor os riscos e os benefícios trazidos. A partir disso, toma a sua decisão. Tornou-se comum, como padrão procedimental, informar ao titular de dados sobre quais dados são coletados e como serão utilizados e, em seguida, permite-se que ele informe se aceita ou não os referidos usos, com base nas informações disponibilizadas.

Porém, os parâmetros por vezes ignoram as limitações cognitivas do titular, que podem dificultar a avaliação dos elementos fundamentais para consentir de forma adequada. É importante destacar que isso não significa que o titular de dados é leigo ou incapaz de decidir, mas da reflexão acerca do foco excessivo no consentimento, sem considerar a real capacidade

que o titular desses dados possui para compreender os riscos, sobretudo com a sobrecarga de termos técnicos e jurídicos que podem integrar os contratos (Mendes; Fonseca, 2020).

Numa reflexão semelhante, Bioni (2019) posiciona que a informação não é apenas a aproximação do indivíduo com a perspectiva, mas uma forma de autoproteção. Portanto, ela deve ser qualitativa, para preencher o vazio da assimetria informacional, especialmente para leigos. Isso não significa, no entanto, que é possível que o consumidor ou o titular de dados alcance o mesmo nível informativo do controlador. Não é necessário que ele saiba todas as minúcias das atividades de tratamento, especialmente se essas informações precisam ser sigilosas.

Mais do que isso, a própria arquitetura das aplicações implica numa avalanche de informações por detrás da lógica que a sustenta, o que inclui certa opacidade. Para manter alguns padrões de segurança da informação, as organizações podem suprimir informações, desde que estas não prejudiquem o direito do titular de dados de obter informações efetivamente relevantes e de seu interesse. Ou seja, a quantidade de informações deve ser o suficiente para que o titular saiba dos usos e dos riscos envolvidos no processo, sem sobrecarregá-lo. Ele conclui:

> O dever-direito de informação deve propiciar, portanto, ao usuário os elementos necessários para o início de um processo de tomada de decisão no que tange ao fluxo de seus dados. A prestação de uma informação clara, adequada e suficiente é o portal de entrada para capacitar o cidadão com o controle dos seus dados, sendo o próprio adimplemento (satisfatório) do dever-direito de informação. (Bioni, 2019, p. 247)

Apesar da centralidade da transparência que as entidades responsáveis pelo tratamento de dados devem ter, as pesquisas têm demonstrado que é necessária uma mudança geral na forma de pensar as políticas de privacidade, porque os indivíduos muitas vezes sequer leem as informações relevantes que lhes são apresentadas. Esse é um dos pontos críticos para a aplicação do consentimento como centro gravitacional de uma norma geral de tratamento de dados, porque se as informações não são inteligíveis ou até mesmo ignoradas pelo titular, esse consentimento resta viciado (Mendes; Fonseca, 2020).

Certamente uma parte dessa recusa em participar do processo decisório tem a ver com a complexidade e com o volume dos textos que explicam como os dados serão tratados, o que sobrecarrega a cognição dos titulares de dados, que ignoram o material disposto, pela excessividade das informações. Nesse sentido, é fundamental que o texto seja apresentado de forma separada, em linguagem acessível, mas também com uma estrutura que privilegie o

fácil entendimento. O consentimento fornecido, nesses casos, não expressa efetivamente a vontade do titular, o que faz com que a doutrina questione a valorização excessiva do consentimento para obter dados, posto que muitas vezes essa superestimação não implica em efetiva autonomia e proteção (Mendes; Fonseca, 2020).

A Lei Geral de Proteção de Dados brasileira, em seu artigo 9º, dispõe sobre consentimento informado, ao posicionar que o titular tem direito de acesso às informações, de maneira clara, sobre as finalidades do tratamento, a forma e duração do processo, informações acerca do controlador, informações acerca do eventual compartilhamento de dados realizado pelo controlador e as responsabilidades que os agentes de tratamento possuem perante o titular. Há uma base sólida que indica, no sentido do vocábulo informado, que deve haver compatibilidade entre o consentimento adquirido inicialmente e os usos reais dos dados. Sobre essa questão, de Teffé e Viola concluem:

> Na hipótese em que o consentimento é requerido, ele será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Quando o consentimento for necessário, havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações. (de Teffé; Viola, 2020, p. 10)

A terceira adjetivação do consentimento prevista pela LGPD trata do consentimento inequívoco, também entendida como uma expressão clara de que o titular de dados concorda com o tratamento, que pode ser analisado junto com a noção de finalidade determinada. O princípio da finalidade, como explora Bioni (2019) determinada que para o tratamento de dados ocorrer, ele deve ter um propósito objetivo, específico e explícito. Deve-se explicar a razão pela qual se utilizará um dado e como. O titular de dados não pode ser induzido a assinar um cheque em branco, o que insta a necessidade de que os responsáveis pelo tratamento de dados direcione o uso e o informe.

Um consentimento genérico não está de acordo com as políticas de proteção dos dados pessoais atualmente. Não se deve, na arquitetura atual, utilizar dados para "melhorar a experiência", porque essa política de privacidade genérica obriga o titular a consentir com os usos de seus dados de maneira desinformada (Bioni, 2019). Mendes e Fonseca (2020) explicam que a proteção de dados não é exclusivamente uma proteção dos dados em si, mas do titular de dados, que é quem arca com os riscos e eventuais prejuízos e lesões.

Por isso, o consentimento inequívoco segue uma finalidade determinada, para que não reste danos ao titular pela adesão a uma política de privacidade genérica, com carta branca para explorar indiscriminadamente as suas informações. Sobre a relevância desse instrumento, a doutrina conclui:

> A finalidade da coleta dos dados deve ser sempre previamente conhecida, seja qual for a base legal utilizada. Essa diretriz diz respeito à relação entre os dados colhidos e a finalidade perseguida pelo agente. Apresenta relação também com o princípio da utilização não abusiva e com a recomendação de eliminação ou transformação em dados anônimos das informações que não sejam mais necessárias. Defende-se que, a depender do tipo de informação, seria possível desmembrar o consentimento em algumas categorias, com requisitos menos ou mais rígidos, conforme a natureza dos interesses. Isso viria através da lógica do consentimento granular. (de Teffé; Viola, 2020, p. 11)

Uma problemática que envolve a finalidade determinada é o que Ruaro (2020) denomina como "problema de agregação", para a qual esse instrumento de compatibilidade serve. Ela divide esse problema em duas etapas, para tratar dos problemas estruturais que os indivíduos enfrentam para tomar decisões informadas e racionais sobre os seus dados. O primeiro problema é a quantidade imensa de entidades que coletam dados. Todos os dias os indivíduos precisam lidar com uma série de serviços e aplicações, com contratos de adesão extensos e complexos, que dificultam até mesmo a capacidade de avaliar os riscos.

Em face do volume significativo de operações para fornecer consentimento, a centralidade deste pode ser uma experiência impossível de ser realizada pelos indivíduos, porque a vida na economia da informação está permeada por serviços e aplicações que dependem da adesão dos titulares. O segundo problema, que envolve a finalidade, é a luta para que os indivíduos compreendam como seus dados podem ser agregados no futuro. Dados residuais considerados insignificantes no contexto da coleta, podem se tornar dados sensíveis se correlacionados com outros dados, o que dificulta para as pessoas avaliarem os possíveis danos futuros. A privacidade é uma questão de longo prazo (Ruaro, 2020).

A finalidade é o que permite analisar, regressivamente, se o tratamento de dados foi adequado com os objetivos propostos. Nesse sentido, a locução "finalidades determinadas" equilibra os adjetivos informado e livre, ainda que sejam noções separadas. São alguns pré-requisitos para os usos de dados pessoais, o que implica num processo de análise das etapas que devem ser observadas. Um consentimento inequívoco não pode advir de uma omissão, segundo uma interpretação doutrinária. As caixas pré-selecionadas, que configuram algumas aplicações, podem implicar um vício de consentimento, porque inação ou silêncio não é consentimento (Bioni, 2019).

O titular de dados deve visualizar e ter uma ação sobre o consentimento, de forma proativa, por meio da configuração do serviço. Essa é uma das interpretações cabíveis para o adjetivo, que tem relação direta com a maneira com que se configuram os serviços e produtos, por padrão. Em seu acesso inicial, por exemplo, o titular deve ser estimulado a configurar as funcionalidades que irá acessar, para consolidar uma ação inequívoca. Em um padrão de privacidade adequado, as operações, serviços e aplicações devem coletar a menor quantidade possível de dados e permitir ao titular a definição dos usos (Bioni, 2019).

O consentimento inequívoco não precisa ser por escrito, pois pode ser realizado de maneira que demonstre clara manifestação da vontade do titular. Reitera-se que manifestação da vontade não é omissão e o ideal é que as plataformas façam parte das mudanças para adequarem-se ao ambiente da proteção de dados, o que inclui construir arquiteturas que privilegiem a autodeterminação informativa, nos casos em que o consentimento for a base legal cabível. Os controladores de dados precisam promover um cenário de valorização da vontade do titular, ao invés de desenhar as suas plataformas para coletarem um consentimento viciado, com opções pré-definidas. Para privilegiar esse entendimento a lei dispôs que cabe ao controlador provar que o consentimento foi obtido de forma ativa, com observância do princípio da responsabilização (De Teffé; Viola, 2020).

Para um tipo de adjetivação auxiliar, que não qualifica o consentimento comum, mas uma hipótese de tratamento, cabe algumas análises. Trata-se da ideia de um consentimento específico e em destaque, nos casos em que o controlador pretende, de alguma forma, compartilhar dados pessoais com outros controladores. Esse tipo de consentimento ocorre em algumas situações, quando há terceiros que não mantêm relações direta com o titular, que realiza procedimentos para os quais o titular não consentiu, e que pretende de alguma forma utilizar esses dados. Sabe-se que há relações entre controladores, como redes sociais e empresas de publicidade. Por padrão, a transferência desses dados é vedada, exceto nos casos em que o terceiro - que não possui relação com o titular - adquirir essa autorização (Bioni, 2019).

Essa expressão também aparece em face da natureza dos dados coletados ou da vulnerabilidade do titular dos dados, a saber: dados sensíveis e dados de crianças e adolescentes. A última hipótese que carece de consentimento específico é a transferência internacional de dados para países que não têm um nível de proteção de dados compatível com o brasileiro. Nesse sentido, a LGPD seguiu a inspiração do GDPR, que exige a adequação do país a níveis adequados de proteção de dados pessoais, para transferir informações (Viola, 2019).

Dessa forma, há três possibilidades de requerimento taxativo do consentimento específico, pela natureza do dado, pela vulnerabilidade do titular e em razão de relação com outro país. A LGPD buscou estabelecer uma carga adicional de proteção do titular, por entender que esses cenários apresentam riscos singulares e a balança na era da informação pesa negativamente ao titular dos dados. Como há riscos altos no tratamento desses dados a priori, de certa maneira o cidadão confere o seu consentimento para assentir que concorda com os riscos elevados. Essa é uma questão particularmente crítica sobre a manifestação do consentimento que, embora seja fundamental para promover autonomia informacional, deixa a cargo do titular de dados muito riscos sobre as operações de tratamento. As hipóteses citadas acima, que carecem de consentimento especial, promove maior assertividade da participação do titular sobre o tratamento, para que ele revise movimentos específicos que serão feitos com os seus dados (Bioni, 2019).

Essa camada de proteção é interpretada pela doutrina de forma sistemática como uma forma de implicar o titular de dados no processo de controle dos seus dados, mas de forma que também responsabilize os responsáveis pelo tratamento de dados por esse processo. Ou seja, é preciso que as plataformas, serviços, empresas e aplicações adotem mecanismos que permitam a participação qualificada do titular, com elementos que operem sobre duas lógicas concomitantes: isolar o direito de informação e a declaração da vontade e assumir, na arquitetura, que essas duas instâncias conferem direitos distintos. O consentimento específico é uma coadunação do direito à informação junto à declaração de vontade, mas quem trata dados deve separar essas duas etapas, para permitir mais do que o consentimento trivial (Bioni, 2019).

Em termos práticos, isso significa, por exemplo, promover mecanismos de dupla verificação do consentimento, seja por meio de mensagens textuais ou imagens. Outra possibilidade é gerar etapas de informação e de declaração da vontade, nas quais o titular de dados precisa estar efetivamente atento para essa dinâmica. Bioni (2019) sugere a dupla verificação, primeiro com a concordância do titular dentro da plataforma ou aplicação e depois numa confirmação via e-mail. Independentemente da forma que essa dupla verificação tiver, o que isso implica é a necessidade de concepção diferenciada no que tange à proteção de dados pessoais, que envolve não apenas à autodeterminação informativa como um pólo fundamental da tutela dos dados, mas também a chamada à responsabilização dos agentes de tratamento.

Para posicionar essa defesa, cabe a apresentação das lições de dois autores que tratam da arquitetura da rede como forma de proteger os dados pessoais. O primeiro é Lawrence

Lessig (2000), que propôs a premissa de que o código é uma lei. Ele sugere uma perspectiva de regulação da rede na qual o próprio código é a etapa inicial de regulação. Entende-se código como a codificação, realizada por programadores, que faz determinada página, aplicação, serviço e plataforma funcionar. É o que fica por trás de uma série de serviços acessados nos meios digitais. O código é a concepção dessas aplicações. Com isso, todas essas aplicações acessadas, seja um site de loja online ou um aplicativo de banco, tem normas implicadas no próprio desenvolvimento da aplicação, que é anterior ao acesso do titular de dados que interage com a plataforma.

Esse código impõe as regras de uso, que projeta a arquitetura vista posteriormente pelo usuário. Antes da regulação legal operada pelas normas jurídicas, há regras impostas primariamente por meio do código, que permite, autoriza, bloqueia ou nega determinada performance nesse espaço (Lessig, 2000). Por isso, alguns espaços são mais reguláveis e propensos à proteção da privacidade e dos dados pessoais, enquanto outros ignoram ou consideram tais elementos acessoriamente.

A própria arquitetura da internet depende de uma série de agentes intermediários privados que subsidiam a relação entre remetentes e destinatários, seja entre um provedor e um usuário, um comprador e um vendedor e afins. Eles são os responsáveis por mediar a experiência da pessoa com os mais diversos ecossistemas online. No entanto, a economia da informação se tornou um fenômeno no qual entidades privadas poderosas coletam quantidades inigualáveis de informações, o que configura uma prática de hiper mediação. Embora na lógica atual seja fundamental o papel da intermediação, as tecnologias não devem ser utilizadas para exercer soberania de organizações específicas no que tange à coleta e uso dos dados pessoais. No modelo difundido atualmente, as condições contratuais que regulam a relação entre plataformas e usuários são promovidas unilateralmente, por meio de "Termos de uso", aplicados como condição para que o titular acesse o produto ou serviço, vinculados a outros contratos que regulam a relação, como políticas de privacidade e padrões da comunidade (Venturini et al., 2019).

Outra contribuição fundamental, que se relaciona com a discussão de Lessig sobre a arquitetura das redes, é a noção de privacidade por concepção idealizada por Ann Cavoukian no âmbito da Comissão de Informação e Privacidade de Ontário, no Canadá. É uma metodologia que se baseia na concepção de que os produtos e serviços devem facilitar o controle e a proteção dos dados dos cidadãos. Mais do que isso, a privacidade desde a concepção, é um processo que privilegia a privacidade desde os primeiros contornos da concepção de produtos, aplicações e serviços. É uma metodologia estruturada em sete

princípios, dentre eles, a ideia de proatividade e prevenção, em oposição à reação e remediação (Cavoukian, 2009).

O contrato de adesão, por exemplo, é uma das formas de experiência direta que o titular de dados tem com a arquitetura da rede, assim como as preferências de cookies que aparecem em muitas páginas acessadas na internet, dentre outros. Bioni expôs a padronização das relações entre plataformas e titulares de dados, por meio de políticas de privacidade repetidas, que pouco contribuem para que o cidadão exerça controle sobre os seus dados, pelo contrário. Essa estandardização dos instrumentos contratuais geram empecilhos para um ambiente equilibrado, porque ao cidadão cabe aderir, o que significa concordar com a exploração intensa dos seus dados, ou não, e deixar de usar as plataformas e serviços. Sobre o tema, ele argumenta:

> Essa dinâmica dos contratos de adesão assinala, sobretudo, a assimetria de forças das relações de consumo, na medida em que o seu elo mais forte fixa unilateralmente o programa contratual. Isso significa, em termos de proteção de dados pessoais, que será o fornecedor quem determinará os rumos do fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada (Bioni, 2019, p. 229)

A padronização e a unilateralidade significa que todo usuário que deseje acessar determinada plataforma terá as mesmas condições, mas a lógica do contrato de adesão é um reforço da impossibilidade de negociação, na qual só é possível aderir ou se retirar. Uma vez aceito o contrato, rege-se o princípio civilista de que as partes ficam obrigadas a cumprir o acordo, mesmo que o titular dos dados não o leia ou não o entenda completamente. Especificamente por isso, a Lei Geral de Proteção de Dados qualificou o consentimento, para enfatizar a responsabilidade das plataformas na promoção de um consentimento livre, informado, inequívoco e para uma finalidade determinada (Venturini et al., 2019).

Os Termos de Uso estabelecem regras para publicação e compartilhamento de conteúdo, assim como modalidades de coleta e processamento de dados. É mister enfatizar que eles regulam não apenas as relações de consumo, mas todas as formas de coleta e processamento de dados pessoais, o que incute implicações significativas no que tange aos direitos humanos. O ponto nevrálgico é a opacidade do consentimento nas relações que se definem de forma unilateral, porque os poderes maiores que intermediam a participação dos usuários em meios digitais operam por meio de instrumentos que deixam pouquíssima ou nenhuma escolha às pessoas. No cenário atual, em que há uma dependência dos acessos

digitais à vida humana, rejeitar ou estar fora desse ambiente dificilmente é uma possibilidade para os indivíduos (Venturini et al., 2019).

Os elementos podem ser projetados para permitir maior ou menor autonomia do usuário, maior ou menor compatibilidade com uma política de equilíbrio entre agentes de tratamento e titulares de dados. Ao assumir um modelo de regulação que considere o poder governamental, ou mesmo que posicione nos dispositivos legais os princípios e bases para o tratamento de dados, é preciso pensar no desenho da rede como parte da regulação, porque é a arquitetura da aplicação que controla o comportamento, em termos iniciais. Essa perspectiva de Lessig (2000) contrapõe a ideia de que não é possível governar ou regular o ciberespaço e a economia da informação digital.

Não há natureza ou essência das aplicações, há interesses discrepantes entre empresas que coletam e tratam dados e cidadãos comuns. Esses espaços foram construídos e podem, portanto, serem modificados para atender aos princípios que regem a tutela da proteção de dados pessoais, regular o código não significa barrar a criatividade e a inovação, mas é necessário pensar a concepção e o desenho das plataformas como um dos mecanismos de responsabilização coletiva, de maneira que o consentimento dos titulares não seja viciado (Lessig, 2000).

Um dos exemplos de coleta "mínima" em ambientes virtuais, que pode gerar sérios danos à proteção de dados dos titulares, é a política de cookies. Ela é informada por meio de uma pop-up, uma pequena janela que se abre na página quando o usuário acessa. O cookie é um arquivo de texto armazenado pelo navegador que funciona como uma identidade de navegação do usuário, pois permite memorizar dados e reconhecer hábitos de navegação, de forma que, ao ser utilizado como mecanismo de predição e vigilância, pode auxiliar no cruzamento de informações com outros dados de navegação (Tobbin; Cardin, 2021).

Existem diversas categorias de cookies e cada uma delas implica em formas diferentes do uso dos dados pessoais. Eles podem ser categorizados de acordo com a necessidade, a finalidade, o período de guarda das informações e até mesmo em função da entidade responsável por seu gerenciamento. Os cookies primários são aqueles utilizados pelo próprio site que o titular visita, ele não direciona nenhum tipo de ação do indivíduo para site de terceiros. No geral, eles incluem informações básicas, como credenciais de logins e idioma escolhido para visualização. Os cookies de terceiros são aqueles criados em um domínio diferente daquele que o titular visita, são domínios que incorporam elementos de outra página, como para a exibição de anúncios. Os cookies necessários são aqueles sem os quais a plataforma não consegue funcionar, eles são condicionais ao regulamento correto da página

ou do serviço. Nesse sentido, as informações rastreadas têm relação com a funcionalidade do serviço que a aplicação oferece e restringe-se a prestar corretamente o serviço requerido, sem atender a interesses do controlador, mas sim contemplando os interesses do titular (ANPD, 2022).

Os cookies não necessários são os mais perigosos do ponto de vista da proteção dos dados pessoais, porque eles existem para rastrear comportamentos de navegação do usuário, não para o mero funcionamento do site ou aplicação. Eles medem o desempenho da página, o que é importante em termos de diagnóstico interno, mas eles também rastreiam informações como o tempo de visualização de um usuário, a interação com informações correlacionadas ao site e até mesmo o acesso a aplicações de terceiros, o que permite aos controladores realizarem uma série de análises e modificações para induzir ou manipular a forma como o usuário se comporta diante do conteúdo veiculado (ANPD, 2022).

A distinção entre os cookies necessários e os não necessários são relevantes para discutir as bases legais que autorizam, e se ajustam, para o tratamento de dados. Em torno da finalidade, há três tipos de cookies: analíticos, de funcionalidade e de publicidade. Os analíticos ajudam a entender como os indivíduos utilizam o site, quais páginas visitam com mais frequência, como o site se comporta diante das ações que o indivíduo realiza, quais tipos de erros aparecem e afins. Os cookies de funcionalidade servem para registrar as preferências do usuário na plataforma e oferecer os serviços que o titular deseja, mas também pode incluir cookies de terceiros, como parte do desenvolvimento de funções não essenciais. Os cookies de publicidade coletam as informações para exibir anúncios. Eles registram hábitos de navegação, informações pesquisadas nas buscas, e coletas que permitem a construção de perfis e de exibição de anúncios personalizados de acordo à análise dos seus interesses. (ANPD, 2022).

Esses pequenos dados coletados, no geral, passam desapercebidos pelos titulares, sobretudo por serem apresentados como uma caixinha semelhante à de um anúncio, com as seguintes opções "aceitar", "rejeitar" ou "gerenciar preferências", embora o gerenciamento de preferências tenha algumas ressalvas. Os cookies são instrumentos de viabilização de páginas, podem oferecer insights às plataformas sobre desempenho, além de servir para o funcionamento básico das operações. O fato é que concordar com as condições de uso implica em algum nível de rastreamento de suas atividades, seja pelo próprio site ou por terceiros, porque muitos cookies servem para publicidade comportamental e são instalados dentro de um site, mas com domínios diversos, que rastreiam e coletam os dados para outras operações (Tobbin; Cardin, 2021).

Pelo potencial de rastreamento das atividades desenvolvidas pelos titulares de dados em meios virtuais, entende-se que é fundamental salvaguardá-los técnica e juridicamente dos impactos negativos que essa operação, que parece corriqueira e inofensiva, pode gerar para os direitos à informação e à transparência, assim como à privacidade dos titulares. Ressalta-se a transparência porque a política de cookies das plataformas muitas vezes ignora a necessidade de informações claras, precisas e inteligíveis sobre como esses dados são tratados. Sobretudo em situações nas quais há grande quantidade de dados coletados, para criar perfis comportamentais e anúncios publicitários para usuários, isso representa um sério risco à privacidade e violação dos direitos humanos. A observância dos princípios da transparência e da privacidade desde a concepção é fundamental em todo tipo de tecnologia que rastreia dados, inclusive em dispositivos móveis, ressalvadas às peculiaridades para cada dispositivo (ANPD, 2022).

Há um predomínio de modelos de negócios baseados em filtragens algorítmicas, que utilizam diversos mecanismos de coleta de dados e de direcionamento de publicidade, com base nesses dados residuais coletados. Um resíduo na economia de dados nunca é uma informação irrelevante. Essas práticas incluem o direcionamento de anúncios de produtos e serviços, de forma otimizada, para os titulares de dados como e-consumidores. Essas práticas utilizam técnicas de mapeamento em bolha, porque o comportamento de um indivíduo digitalmente é rastreado de forma massiva e permite aos analistas dos dados entenderem o caminho que este percorre até uma compra, a quais anúncios reage e afins (Magrani, 2019).

Os cookies são parte dessa logística porque representam as pegadas digitais que o titular deixa na navegação. Dessa maneira, as informações que as pessoas veem nas plataformas são fruto de edições invisíveis que operam para a customização da navegação, com o intuito tanto de vigiar quanto de construir uma experiência particular, para cada indivíduo, de acordo com os seus padrões algorítmicos. Diante dessa forma sofisticada de vigilância e predição, o consentimento tem sido ineficaz para barrar os abusos contidos nas políticas de privacidade, políticas de cookies e nos termos de uso das plataformas, o que gera graves violações de direitos, silenciosamente (Magrani, 2019).

Ao considerar a necessidade de transparência em relação à política de cookies, é fundamental observar como o consentimento pode ser alterado pela maneira como as plataformas desenham a informação sobre a coleta desses dados. Ao considerar uma norma de dados pessoais que exija o consentimento prévio e expresso, por exemplo, os usuários são bombardeados com uma série de avisos sobre cookies, mas de uma maneira maçante e

forçada, de maneira que muitas vezes eles aceitavam a política sem compreender as consequências dessa ação (Bioni, 2019).

Nesse sentido, não há grande poder no consentimento, uma vez que a sua operacionalização fica a cargo exclusivamente das plataformas que, de certa maneira, induzem a experiência do usuário para aceitar sem maiores investigações sobre o uso dos seus dados. A qualificação legislativa do consentimento, por si só, não é capaz de modificar a lógica que rege as plataformas. Ela deve direcionar padrões de aplicações, mas num diálogo e regulação contínuos, pois o titular de dados, diante de uma avalanche de informações e janelas em sua tela, pode optar por meramente aceitar e seguir em frente. Não é distante supor que tal problemática é uma vantagem para as organizações que tratam dados (Bioni, 2019).

A autoridade nacional de proteção de dados brasileira publicou um guia que discute as políticas de cookies e a LGPD, para direcionar as interpretações dos controladores para a questão e sobretudo para enfatizar como as arquiteturas das plataformas podem ser viciadas para obter consentimento forçado dos titulares. No que tange ao consentimento, que é o objeto central dessa pesquisa, a entidade entende que o indivíduo deve ter a opção de aceitar ou recusar a utilização de cookies, sem consequências negativas que possam prejudicar a manifestação da vontade do titular (ANPD, 2022).

Qualquer menção de condicionamento do uso ao aceite integral da política de cookies pode viciar o consentimento, mesmo que o elemento de manifestação da vontade deva ser avaliado nos casos concretos. Destaca-se que, para consentir, o titular deve ter alternativas reais e satisfatórias, que inclua informações claras, precisas e acessíveis, sem incorrer em uma situação de aceitar integralmente ou retirar-se da plataforma. Eles ainda relembram que o consentimento é inequívoco, o que não admite os mecanismos de cookies que interpretam a omissão como sinônimo de consentimento. Autorizações desenhadas para serem pré-selecionadas no momento da visualização do titular não são recomendadas, pois viciam o consentimento, assim como mecanismos de consentimento tácito (ANPD, 2022).

Em um posicionamento interessante, a ANPD observa que, segundo a Lei Geral de Proteção de Dados Pessoais brasileira, compete ao controlador comprovar que o consentimento respeita os parâmetros de proteção de dados, não à LGPD. Ela desaconselha o uso do consentimento como base legal para promover cookies estritamente necessários, porque não há manifestação real de autonomia nesse caso. O que há é o condicionamento da escolha diante da impossibilidade de recusar essa funcionalidade. Ela indica:

> Diante do que estabelecem esses requisitos legais, pode-se afirmar que não é apropriado utilizar a hipótese legal do consentimento nas hipóteses de cookies estritamente necessários. Isso porque, nestes casos, a coleta da informação é essencial para assegurar o funcionamento da página eletrônica ou para a adequada prestação do serviço, de modo que não há condições efetivas para uma manifestação livre do titular ou, ainda, para que se assegure a este a real possibilidade de escolher entre aceitar ou recusar o tratamento de seus dados pessoais (ANPD, 2022, p. 20)

Qualquer tratamento em que a coleta e uso dos dados seja estritamente necessário para cumprir obrigações legais, a hipótese do consentimento não é apropriada. As plataformas têm utilizado a política de cookies por meio da prática do consentimento e tem exigido o consentimento dos titulares aos cookies necessários na mesma pop-up que explicam e pedem autorização par os cookies não-necessários. A forma com que as plataformas concebem os seus códigos não é desinteressada ou ingênua. Num cenário assimétrico, essas práticas induzem a violações de direitos.

A arquitetura das aplicações deve ser concebida de forma proativa, com mecanismos que antecipem e previnam incidentes de privacidade antes que eles aconteçam. Implica em examinar os riscos preventivamente, ao invés de focar em remediar danos, como "efeitos colaterais". Essa prática requer um comprometimento em adotar altos padrões de privacidade, em especial inspirados numa série de indicações de alto nível das leis globais de regulação. Na ótica da privacidade por concepção, há o desenvolvimento de uma cultura de entendimento e de adoção dos princípios da privacidade, para equilibrar a balança desigual da assimetria entre organizações e titulares de dados. Testar as aplicações criadas, diagnosticar práticas fracas de privacidade e corrigir os impactos negativos estão entre as ações possíveis dentro dessa perspectiva (Cavoukian, 2009).

A tecnologia pode ser um braço da privacidade, uma facilitadora do controle dos titulares sobre as suas informações. Há tecnologias que privilegiam essa abordagem da privacidade por concepção e contribuem para um cenário que proteja não apenas o titular de dados, mas também os agentes de tratamento, uma vez que um ambiente de garantia da privacidade contribui para práticas de negócio éticas. Há mecanismos criptográficos que anonimizam dados pessoais ou quebra vínculos de identificação entre um dado e uma pessoa, assim como modelos de navegação anônima que impedem rastreamentos de titulares de dados. O ponto central, notadamente, é empoderar o titular de dados como centro gravitacional dessa tutela jurídica (Bioni, 2019).

Esses exemplos demonstram que revisar a arquitetura dos sistemas é uma forma de proteger os dados e urgente, posto que o consentimento tem suas lacunas diante do cenário de extração e utilização massiva de dados pessoais. É mister implementar práticas que equalizem

as assimetrias que o mercado informacional impõe aos titulares, a confidencialidade e o anonimato são estratégias interessantes, mas mecanismos de transparência e informação qualificada também devem ser implementados. As políticas de privacidade mais protegem as empresas da responsabilidade de fazer parte, qualitativamente, de um novo cenário de proteção. Não devem ser utilizadas como braço da violação dos direitos dos titulares que, nesse ambiente, pouco possuem escolha real. Num contexto de vigilância, predição e mineração de dados pessoais, as estéreis políticas de privacidade permitem às plataformas permanecerem numa posição assimétrica (Bioni, 2019).

Dentro da privacidade por concepção, há o princípio da privacidade por padrão que implica em seguir quatro etapas relevantes: determinar e seguir o propósito e a especificação do uso de dados, apenas no limite do que é relevante para a circunstância do tratamento; coletar informações pessoais de forma justa e limitada ao mínimo necessário; evitar a identificabilidade e a capacidade de correlação entre os dados coletados, de forma a minimizar o uso irrefreado de informações pessoais para propósitos escusos e modelos preditivos; reter os dados apenas até que os fins específicos propostos no início do tratamento sejam cumpridos.

O terceiro princípio posiciona a defesa da privacidade dentro do design das plataformas e das arquiteturas dos sistemas, não posteriormente às violações materiais de direitos. O resultado disso é considerar a privacidade como um componente essencial para o funcionamento dos sistemas, como um dado integrado a este, de forma holística. É uma forma qualificada de pensar as bases legais para o tratamento de dados, inclusive o consentimento, porque incute na etapa de programação a criatividade e a integração de princípios que regem o tratamento em cada nação. Em uma abordagem sistêmica, a privacidade define a forma como o sistema será concebido e é possível sanar eventuais lacunas, ao invés de gerir apenas os danos. Na etapa do design, inclusive, deve-se documentar possíveis riscos e formas de mitigação, assim como alternativas aos eventuais riscos e um programa de diagnósticos. Em termos gerais, o que o trabalho de Cavoukian (2009) aponta é a possibilidade de que o desenho das plataformas siga parâmetros protetivos quanto aos dados pessoais.

A autodeterminação informacional, e os qualificadores do consentimento, implicam em que os titulares de dados tenham controle sobre todo o ciclo de vida da coleta ao tratamento, não apenas na ação de concordar ou discordar. O que se busca é uma nuance ou granularidade do consentimento, com autorizações específicas, voluntárias e preferenciais do titular quanto às suas informações. Deve-se garantir o poder de barganha em um processo de tomada de decisão justo, posto que a economia dos dados propõe uma arena traiçoeira para os

indivíduos. A autonomia inclui a possibilidade de decidir como os seus dados serão utilizados, com preferências granulares, e controlar o ciclo de vida do dado, com informações de como estes são tratados. Do contrário, mesmo a concessão para uma finalidade determinada é um cheque em branco. Sobre essa questão, Mendes e Fonseca assinalam:

> No paradigma do consentimento, os ideais de autonomia e de empoderamento individual assumem, diversas vezes, contornos meramente formais. Desconsideram-se questões envolvendo o contexto em torno do consentimento e do tratamento em questão, tais como os perigos acerca da natureza dos dados envolvidos. Nesse cenário, o consentimento se torna um modo conveniente de viabilizar a coleta e o uso de dados sem, contudo, "confrontá-los com os valores centrais em jogo". Afinal, caso derive de uma decisão em que a livre vontade do titular dos dados é sensivelmente questionável, torna-se igualmente questionável a capacidade do consentimento em garantir esses ideais de autonomia e de empoderamento. (Mendes; Fonseca, 2020, p. 524)

Trata-se, portanto, de assumir que a capacidade de inferência e correlação trazida pelas novas tecnologias faz com que seja impossível, para o indivíduo, no momento da coleta, ter ciência completa das possíveis consequências dessa coleta no futuro ou mesmo gerencie plenamente o ciclo de vida do dado a partir do mero consentimento no momento da coleta. Há muitas incertezas quanto às possibilidades de agregar e cruzar dados. Nessa ampla cadeia da regulação, é mister considerar o ciclo de vida do dado como ponto crucial para a referência regulatória, de forma global: qual a finalidade para qual o dado foi coletado? Como informar adequadamente ao titular esses elementos? Que efeitos adversos foram oriundos das informações coletadas durante o tratamento?. A última questão é crucial, porque um dado pode afetar direitos do titular após o tratamento, em correlação com outras informações.

Destaca-se que, para isso, não é necessário limitar ou proibir o tratamento de dados ou renunciar ao consentimento. O consentimento é uma esfera de proteção significativa, que promove parte da autodeterminação informacional, mas há que se considerar a capacidade real de exercer esse direito frente ao contexto vigente. O consentimento individual prévio deve ser apenas um dos instrumentos de salvaguarda dos dados pessoais e do direito dos titulares, sobretudo. A contribuição de Barocas e Nissembaum (2014) critica a percepção de que o consentimento informado é um meio eficaz de autonomia dos indivíduos, de fazer escolhas, assumir e lidar com riscos, expressar preferências e resistir à exploração violenta das suas informações.

As autoras criticam essa perspectiva do consentimento como um *instrumento super-homem*, que pode determinar a autodeterminação informacional por si só. De fato, o consentimento é um mecanismo fundamental, sobretudo para a relação com plataformas

conscienciosas, que tratam os dados pessoais de maneira responsável. Ele pode significar, em muitos casos, a garantia da privacidade - como sinônimo de controle sobre as informações de si. No entanto, uma vez que os termos de uso e contratos de adesão se tornaram os principais instrumentos de uma gama de aplicações, o foco têm sido apenas conceber protocolos que demonstrem que os titulares de dados efetivamente consentiram com o seu uso (Barocas; Nissembaum, 2014).

Por si só, o consentimento tem, na configuração digital atual, pouca força, diferentemente do contexto do século passado, no quadro em que ele ascendeu. Embora seja ainda retratado como instrumento central, e figure na proteção de dados brasileira como base para o tratamento de dados, há muitos desafios concretos para a sua obtenção qualificada. Barocas e Nissembaum (2014) retratam alguns desses desafios. O primeiro é o paradoxo da transparência. A autonomia tem relação com uma compreensão sólida para efetuar uma escolha. O debate teórico e jurídico buscou a simplificação das políticas de privacidade como uma das soluções para a assimetria informacional de natureza técnica, pela ininteligibilidade do contrato para parte dos titulares.

Vários dispositivos jurídicos seguem a demarcação de que é preciso simplificar e tornar claro o entendimento. Esse é um instrumento interessante, ao mesmo tempo que, ao simplificar, retira-se a fidelidade da operação. Para tomar decisões que efetivamente permitam controle sobre os dados, os indivíduos precisam entender o tipo de informação recolhida, com quem é partilhado, quais as restrições e para que finalidade. Não é possível simplificar completamente essas informações, mas a sobrecarga da era dos grandes dados faz com que acompanhar esse processo seja enfadonho para muitos titulares (Barocas; Nissembaum, 2014).

Outros desafios são a indeterminação e a imprevisibilidade de uma operação. Nos mais diversos contatos típicos de coleta de dados, ao considerar o paradigma do big data, os dados se movem entre os bancos e entre os controladores de maneira imprevisível. Por isso Nissembaum (2011) defende o conceito de integridade contextual. Porque o potencial valor do dado nem sempre é visível no momento da recolha; ele pode valer, na economia da informação, muito mais. Por conta disso, ela acredita que a única forma de limitar essa imprevisibilidade é por meio da restrição dos destinatários e dos princípios de transmissão especificados.

Práticas de hiperextensão da finalidade do tratamento não são anômalas, são o sangue vital de muitas empresas que lucram com dados pessoais. Ao extrair informações de colaboração com terceiros, aumenta o campo de dados para lucrar ainda mais. Nesse sentido,

uma entidade responsável por tratar dados, que obteve o consentimento do titular para determinada operação, deve transparência sobre informações adicionais, não previstas, que conseguiu obter? Tudo depende do significado que "informado" possui dentro da doutrina e da norma jurídica (Barocas; Nissembaum, 2014).

As normas, portanto, devem observar essa integridade contextual, que significa observar se o fluxo do tratamento de dados foi apropriado com os interesses do titular; a utilização de informações para obter vantagem econômica e lucratividade contextual, uma vez distante dos benefícios para o titular dos dados, deve ser restrita. Observar a integridade contextual significa correlacionar o contexto da relação e as características do tratamento efetuado. Por exemplo: quais expectativas existem nesse tratamento? De maneira que o contexto define a violação, considerando os atores envolvidos, os tributos da informação e os princípios de transmissão (Nissembaum, 2011).

Nesse sentido, o consentimento não deve ser banido ou ignorado. Ele representa um dos instrumentos centrais de realização da autonomia individual e se tornou o paradigma central para a proteção dos dados em diversos países. Porém, os avanços tecnológicos desafiam institutos consolidados, porque apresentam desafios inéditos, sobretudo ao considerar os lucros que as organizações obtém pela violação, mesmo que discreta, dos direitos dos titulares em suas aplicações. Posicionar mecanismos de fiscalização e regulação ampla é fundamental para garantir que o consentimento não tenha mero contorno formal, mas seja um mecanismo que se ajuste às análises contextuais e, em diversos casos, ceda lugar a outras bases legais que podem garantir, ao mesmo tempo, os interesses dos agentes de tratamento, mas sobretudo a proteção do titular de dados.

CONSIDERAÇÕES FINAIS

A legislação da proteção de dados pessoais percorreu um longo caminho, complexo e evolutivo, moldado especialmente pelo histórico dos avanços tecnológicos, que impuseram novos desafios para o Direito. As diversas mudanças sociais associadas à tecnologia construíram um espaço crítico para que o âmbito legislativo refletisse acerca das medidas necessárias para enfrentar o cenário da economia da informação. Diversas fases representaram os contornos do consentimento como um elemento central para a proteção de dados pessoais, mesmo que de forma tímida, no início de sua evolução legislativa. Um dos marcos cruciais para esse instrumento de proteção foi a Diretiva de Proteção de Dados Pessoais da União Europeia, em 1995, embora a Lei de Proteção de Dados na Alemanha, em 1970, tenha sido o primeiro dispositivo de reconhecimento formal do consentimento para a proteção de dados pessoais. Foi a Diretiva Europeia, no entanto, que estabeleceu mais fortemente o consentimento como um princípio para o processamento de dados pessoais. Ela coloca o titular de dados no centro gravitacional da proteção, o que foi um passo importante à época.

Com a rápida evolução tecnológica, especialmente com a ascensão da internet e das mídias sociais, novos desafios surgiram para o consentimento na proteção de dados. Em pouco tempo, os dados se tornaram o objeto central da economia da informação e passaram a ser coletados de forma massiva; nenhum dado, desde então, é irrisório ou irrelevante. A complexidade das interações digitais e a coleta massiva de informações pessoais tornaram mais difícil para os usuários compreenderem e controlarem como seus dados são utilizados. Isso gerou um questionamento sobre a eficácia do consentimento como um mecanismo de proteção robusto.

O General Data Protection Regulation, que entrou em vigor em 2018, representou uma mudança de chave na proteção de dados pessoais, porque expandiu diretrizes que consideram a complexidade que a economia da informação adquiriu nas últimas décadas. Ele reforçou as diretrizes estabelecidas na Diretiva Europeia e impôs requisitos mais rígidos, além de introduzir a noção de consentimento claro, específico, informado e inequívoco como concepção e qualificadores do consentimento. Essa concepção influenciou fortemente a Lei Geral de Proteção de Dados brasileira.

No Brasil, a evolução do consentimento na proteção de dados pessoais reflete uma jornada marcada por mudanças legislativas e adaptações às demandas de uma sociedade cada vez mais digital. O histórico do consentimento pode ser compreendido através de marcos legais e movimentos sociais que influenciaram a forma como os dados pessoais são tratados e

protegidos no país. A Constituição Federal de 1988 foi um marco inicial na proteção dos direitos individuais no Brasil. Embora não tenha abordado especificamente a proteção de dados pessoais, consagrou princípios fundamentais, como o direito à privacidade, intimidade e inviolabilidade da vida privada, fornecendo a base para futuras regulamentações nesse sentido.

O Código de Defesa do Consumidor também contribuiu para o cenário de autonomia informacional, além de proteger a transparência e o direito à informação clara sobre produtos e serviços, o que estabelece uma base para o consentimento implícito. Isso se reflete na relação entre consumidor e fornecedor, onde a expectativa é que as empresas forneçam informações claras sobre como os dados serão utilizados, permitindo aos consumidores tomarem decisões informadas. O Marco Civil da Internet, estabelecido em 2014, foi um divisor de águas ao introduzir diretrizes para o tratamento de dados pessoais no ambiente online. A lei determinou a necessidade de consentimento explícito para a coleta, armazenamento e uso de dados pessoais, estabelecendo princípios para garantir a privacidade dos usuários da internet no Brasil.

Um marco significativo na história do consentimento na proteção de dados no Brasil foi a promulgação da Lei Geral de Proteção de Dados (LGPD) em 2018. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece diretrizes claras para o tratamento de dados pessoais, incluindo a necessidade de consentimento claro e explícito para a coleta e uso desses dados. Com a LGPD, o consentimento passou a ser um dos pilares centrais na proteção de dados pessoais no Brasil. A lei exige que as empresas obtenham o consentimento dos titulares dos dados de maneira clara e específica, informando sobre a finalidade e a extensão do uso dessas informações. Além disso, a LGPD estabeleceu direitos aos titulares, como acesso aos dados, correção de informações imprecisas e exclusão dos dados pessoais após o término da relação entre a empresa e o titular.

Apesar dos avanços, a implementação completa da LGPD enfrenta desafios, incluindo a adaptação das empresas às novas exigências, a necessidade de criar uma cultura de proteção de dados e garantir a conformidade com a legislação. A questão do consentimento permanece como um desafio, especialmente diante da complexidade das interações digitais e da necessidade de garantir um consentimento informado em um ambiente online em constante evolução. Em resumo, o histórico do consentimento na proteção de dados no Brasil demonstra uma trajetória de avanços legislativos significativos, especialmente com a promulgação da LGPD. O consentimento tornou-se um pilar central na proteção dos dados pessoais, refletindo

a preocupação crescente em garantir a privacidade e os direitos dos cidadãos brasileiros em um contexto digital em rápida transformação.

Apesar dos avanços regulatórios, persistem desafios significativos. A crescente assimetria informacional entre empresas e usuários, juntamente com a coleta massiva de dados, levanta questões sobre a eficácia do consentimento. A complexidade dos termos e condições, juntamente com a falta de transparência sobre o uso real dos dados, mina a capacidade dos indivíduos de conceder um consentimento genuinamente informado. Além disso, a globalização das atividades digitais e a necessidade de interoperabilidade entre diferentes sistemas de proteção de dados apresentam desafios adicionais. A necessidade de harmonização e cooperação internacional para garantir uma proteção eficaz dos dados pessoais continua sendo uma questão premente.

O consentimento na proteção de dados pessoais percorreu um caminho notável ao longo das décadas, desde suas origens éticas e legais até a consagração nos regulamentos de privacidade mais recentes, como o GDPR. No entanto, os desafios emergentes da era digital destacam a necessidade contínua de aprimorar e fortalecer as salvaguardas de proteção de dados, além de garantir que o consentimento permaneça relevante e eficaz diante da rápida evolução tecnológica e das mudanças sociais. A busca por um equilíbrio entre a inovação tecnológica e a proteção da privacidade dos indivíduos continua sendo um desafio crucial para a sociedade contemporânea.

No turbilhão da revolução digital, a proteção dos dados pessoais tornou-se uma preocupação central. A ascensão da era da informação trouxe consigo inúmeras vantagens, mas também desafios intrincados, especialmente no que diz respeito à privacidade e à proteção dos dados. Nesse contexto, o consentimento tem sido considerado como o principal pilar para salvaguardar a privacidade do indivíduo. No entanto, a crescente assimetria informacional impõe desafios significativos à eficácia do consentimento como protetor de dados.

O consentimento, embora seja uma peça fundamental na regulamentação de privacidade de dados, tem enfrentado limitações significativas, especialmente no contexto da era digital. O consentimento implica que um indivíduo, ao concordar com os termos e condições estabelecidos por uma entidade que coleta seus dados, está ciente e consente com o uso dessas informações. No entanto, na prática, essa premissa tem sido desafiada pela complexidade das relações digitais e pela assimetria de poder entre os indivíduos e as corporações que coletam e processam dados.

A assimetria informacional é uma realidade incontornável na era digital, onde as corporações detêm uma quantidade desproporcional de conhecimento e poder em relação aos indivíduos. Isso cria um desequilíbrio na negociação do consentimento, pois os termos e condições muitas vezes são apresentados em contratos extensos e complexos, dificultando a compreensão completa por parte dos usuários. Além disso, a falta de opções reais para os usuários, além de concordar com os termos ou abandonar o serviço, limita ainda mais a capacidade de exercer um consentimento informado e livre de coerção.

A personalização e a prática das “bolhas de interesse” de conteúdo têm sido estratégias-chave das empresas para coletar dados pessoais. Essas práticas, embora proporcionem uma experiência mais personalizada, também levantam questões éticas, uma vez que muitas vezes extrapolam os limites do que um indivíduo está disposto a compartilhar. A coleta passiva de dados, muitas vezes sem o conhecimento explícito do usuário, também questiona a validade do consentimento, já que este deveria ser baseado em uma escolha informada e consciente.

A falta de transparência nos processos de coleta, uso e compartilhamento de dados também mina a eficácia do consentimento como protetor de dados. Os indivíduos frequentemente se deparam com práticas obscuras, onde não têm clareza sobre como suas informações serão utilizadas. Os acordos de consentimento frequentemente escondem os verdadeiros propósitos para os quais os dados serão empregados, deixando os usuários vulneráveis à exploração de seus dados pessoais.

É crucial repensar o paradigma de proteção de dados na era da assimetria informacional. Enquanto o consentimento permanece uma ferramenta importante, sua eficácia isolada é limitada diante da complexidade e das disparidades de poder existentes. Uma abordagem multifacetada se faz necessária, envolvendo não apenas o consentimento informado, mas também a transparência, a responsabilidade das empresas, a regulamentação mais estrita e a conscientização dos usuários sobre seus direitos e o valor de seus dados. A transparência deve ser promovida como um princípio fundamental na coleta e no processamento de dados. As empresas devem ser obrigadas a fornecer informações claras e compreensíveis sobre como os dados são coletados, utilizados e compartilhados. Além disso, regulamentações mais rígidas são necessárias para garantir que o consentimento seja verdadeiramente informado, em uma linguagem acessível para a maioria das pessoas.

A responsabilidade das empresas na proteção dos dados dos usuários deve ser reforçada. Elas devem ser incentivadas a adotar medidas proativas de segurança e privacidade, além de serem responsabilizadas por práticas inadequadas de coleta e uso de

dados. Isso pode ser alcançado por meio de políticas de privacidade robustas, auditorias independentes e penalidades mais severas para violações de dados. A educação e a conscientização dos usuários também desempenham um papel fundamental na proteção dos dados na era digital. Os indivíduos devem ser capacitados com conhecimento sobre seus direitos de privacidade e o valor de seus dados pessoais. Iniciativas de educação pública e campanhas de conscientização são essenciais para capacitar os usuários a tomarem decisões informadas sobre o compartilhamento de seus dados.

Muitos usuários não compreendem completamente como seus dados serão utilizados após darem o consentimento. As políticas de privacidade frequentemente são extensas e repletas de terminologia técnica, dificultando a compreensão real do escopo e das implicações do consentimento concedido. O consentimento é muitas vezes obtido para um propósito específico, porém, a evolução tecnológica permite que os dados sejam utilizados de formas não previstas inicialmente. Isso levanta questões sobre o consentimento concedido para um propósito específico e o uso futuro que pode não estar alinhado com as expectativas iniciais dos usuários. O poder econômico e tecnológico das organizações frequentemente coloca os usuários em uma posição desigual quando se trata de negociar termos de consentimento. A falta de alternativas viáveis pode forçar os usuários a aceitarem termos que não estão de acordo com suas preferências, minando a capacidade de consentir de forma livre e informada.

Em síntese, a insuficiência do consentimento como protetor de dados na era da assimetria informacional é evidente diante das complexidades e desafios do cenário digital atual. É imperativo adotar uma abordagem mais holística e abrangente, que não apenas valorize o consentimento informado, mas também promova a transparência, responsabilidade corporativa, regulamentação eficaz e conscientização dos usuários. Somente através de esforços colaborativos e uma mudança significativa no paradigma de proteção de dados será possível enfrentar os desafios emergentes e preservar a privacidade na era digital. Além do consentimento, uma série de medidas complementares e abordagens mais abrangentes são essenciais para proteger os dados pessoais na era digital. A evolução tecnológica e a complexidade das interações online demandam uma abordagem multifacetada que vai além do simples consentimento. Vamos explorar algumas dessas medidas:

O conceito e a prática de privacidade por padrão desempenha um papel fundamental na proteção dos dados pessoais na era digital. Desenhar a arquitetura das aplicações de maneira ética e com proteção ao titular de dados é uma das estratégias basilares para modificar a cultura de remediação nessa área. As organizações devem incorporar princípios éticos desde o início da concepção de sistemas, para permitir que os indivíduos tenham maior

controle sobre suas informações pessoais desde o primeiro momento até o final do tratamento. A privacidade por padrão busca oferecer opções claras aos indivíduos, de forma qualificada. Deve servir para aumentar a compreensão dos usuários sobre o tratamento, ao invés de nublar os processos de tratamento dos dados.

A natureza complexa e muitas vezes opaca dos termos e condições apresentados aos usuários torna o consentimento pouco significativo. Muitas vezes, as empresas utilizam contratos extensos e linguagem complexa, dificultando a compreensão real dos usuários sobre como seus dados serão utilizados. A assimetria informacional entre empresas e usuários é um obstáculo fundamental para o consentimento eficaz. As corporações detêm um poder desproporcional na coleta e no uso dos dados, enquanto os usuários frequentemente não têm o conhecimento ou a capacidade de avaliar completamente as consequências do consentimento que estão concedendo. Por isso, é fundamental ir além do simples consentimento. Reformas legislativas e novas concepções regulatórias devem ir além do consentimento individual, mas posicionar mecanismos reais de responsabilização das empresas pelo uso dos dados. Destaca-se a importância de regulamentações mais estritas que exijam uma linguagem mais clara nos termos de serviço, além de impor penalidades mais significativas para violações de privacidade.

No campo da responsabilização, destaca-se a importância que as organizações que tratam dados possuem na promoção de um ambiente mais adequado para a proteção dos titulares de dados. Deve-se demarcar algumas dessas responsabilidades, sobretudo no sentido de compartilhar o dever de cuidado, para além do papel do titular em proteger os seus próprios dados. Tal tarefa é notadamente impossível diante do desequilíbrio de poder na era da informação. Uma das principais responsabilidades das organizações é promover a transparência em suas práticas de coleta e uso de dados. Isso implica fornecer informações claras e acessíveis sobre como os dados são coletados, processados e compartilhados. Comunicar de maneira clara e compreensível os propósitos para os quais os dados são utilizados é essencial para reduzir a assimetria informacional e promover a confiança dos usuários.

As organizações têm a responsabilidade de garantir que o consentimento dos usuários para a coleta e o processamento de dados seja verdadeiramente informado. Isso implica oferecer escolhas claras e específicas aos usuários, permitindo que decidam livremente como desejam que seus dados sejam utilizados. O consentimento deve ser obtido de maneira ética, evitando práticas enganosas ou coercitivas. É responsabilidade das organizações minimizar a coleta excessiva de dados pessoais e proteger as informações dos usuários contra acessos não

autorizados. Isso envolve adotar medidas de segurança robustas, como criptografia, anonimização e controle de acesso, garantindo a integridade e confidencialidade dos dados.

Além de cumprir as regulamentações existentes, as organizações têm a responsabilidade ética de ir além, implementando políticas e práticas que promovam a proteção da privacidade, mesmo em situações em que a lei não seja explícita. Isso inclui adotar uma abordagem proativa para garantir a privacidade dos usuários e demonstrar responsabilidade corporativa no tratamento dos dados pessoais. As organizações devem prestar contas por suas práticas de privacidade e proteção de dados. Isso implica ser transparente sobre como os dados são utilizados, permitindo auditorias independentes e relatando prontamente qualquer violação de dados ou incidentes de segurança. A responsabilidade e a transparência demonstram o compromisso das organizações em agir de forma ética e proteger a privacidade dos usuários.

Em síntese, as organizações enfrentam uma responsabilidade crucial diante da assimetria informacional. Ao promover a transparência, garantir consentimento informado, proteger os dados, educar os usuários e agir de maneira ética e responsável, as organizações podem reduzir a disparidade de conhecimento e fortalecer a confiança dos usuários, contribuindo para uma relação mais equitativa e ética no tratamento dos dados pessoais. Essa abordagem não apenas atende às exigências legais, mas também respeita os direitos fundamentais dos indivíduos em um mundo cada vez mais digitalizado.

Por isso, esse trabalho conclui que, embora o consentimento seja um componente importante na proteção de dados pessoais, seus limites estão intrinsecamente ligados à complexidade das interações digitais e à assimetria informacional. Superar esses desafios exige uma abordagem mais ampla, que envolva não apenas o consentimento, mas também medidas de transparência, educação, regulamentação eficaz e responsabilidade corporativa para garantir uma proteção de dados mais robusta e eficaz.

Ir além do consentimento na proteção de dados pessoais requer uma abordagem holística que englobe transparência, educação, segurança por design, responsabilidade corporativa, regulamentações sólidas, minimização de dados e cooperação global. É uma interconexão de medidas que se complementam, visando não apenas empoderar os usuários, mas também responsabilizar as empresas e as autoridades reguladoras para assegurar a privacidade e a proteção dos dados pessoais na era digital em constante evolução. Essas estratégias combinadas formam um panorama mais amplo e eficaz para enfrentar os desafios emergentes e preservar a privacidade individual.

REFERÊNCIAS

ANPD. **Guia orientativo - cookies e proteção de dados pessoais**. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2022.

BAROCAS, S.; NISSEMBAUM, H. Big Data's End Run around Anonymity and Consent. In: BAROCAS, Solon et al. **Privacy, Big Data, and the Public Good**. New York: Cambridge University Press, 2014, p. 44-75. Disponível em: https://doi.org/10.1017/cbo9781107590205.004. Acesso em: 8 nov. 2023.

BARROSO, L.R. A viagem redonda: habeas data, direitos constitucionais e as provas ilícitas. **Revista de Direito Administrativo**, 213, Rio de Janeiro, p. 149-163, jul/set 1998.

BESSA, L.R. **Nova lei do cadastro positivo**. Correio Braziliense, Brasília, 5 ago 2019.

BIONI, B. **De 2010 a 2018**: a discussão brasileira sobre uma lei geral de proteção de dados. 2 jul 2018. Disponível em: https://brunobioni.com.br/blog/2018/07/02/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados/. Acesso em: 10 jul 2023.

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

BIONI, B. **Xeque-Mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. GPoPAIUSP, Jul. 2016. Disponível em: https://www.academia.edu/28752561/Xeque_Mate_o_tripé_de_proteção_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 28 jul. 2023.

BIONI, B.; SILVA, P.G.F.; MARTINS, P.B.L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, Brasília, v. 1, p. 8-19, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/issue/view/39/46. Acesso em: 31 jul 2023.

BOFF, S.O.; FORTES, V.B.; FREITAS, C.O.A. **Proteção de Dados e Privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BORGESIUS, F J.Z. et al. Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. **European Data Protection Law Review**, v. 3, n. 3, p. 353-368, 2017. Disponível em: https://doi.org/10.21552/edpl/2017/3/9. Acesso em: 31 jul. 2023.

BOTELHO, M. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a lei geral de proteção de dados pessoais. **Argumenta Journal Law**, Jacarezinho – PR, Brasil, n. 32, 2020, p. 191-207.

BRASIL. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, 5 out. 1988. Disponível em: https://legis.senado.leg.br/norma/579494. Acesso em: 31 jul. 2023.

BRASIL. Lei Complementar nº 166, de 8 de abril de 2019. Lei Complementar nº 166 de 08/04/2019. Diário Oficial da União, 9 abr. 2019. Disponível em: https://legis.senado.leg.br/norma/30892420. Acesso em: 31 jul. 2023.

BRASIL. Lei nº 12.414, de 9 de julho de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 31 jul 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 31 jul 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 jul 2023.

BRASIL. Lei nº 8078, de 11 de setembro de 1990. Lei nº 8.078 de 11/09/1990. Diário Oficial da União - Suplemento, 12 set. 1990. Disponível em: https://legis.senado.leg.br/norma/549954. Acesso em: 31 jul. 2023.

BRASIL. Lei nº 9507, de 12 de novembro de 1997. Lei nº 9.507 de 12/11/1997. Diário Oficial da União, 13 nov. 1997. Disponível em: https://legis.senado.leg.br/norma/551383. Acesso em: 31 jul. 2023.

CALDERON, M.P. A evolução do direito de acesso à informação até a culminância na lei nº 12.527/2011. **Revista Brasileira de Ciências Policiais**, Brasília, v. 4, n. 2, p. 25-47, jul/dez 2013.

CAVOUKIAN, A. **Privacy by design**: the 7 foundational principles. Canada, Ontario: Information and Privacy Commission, 2009. Disponível em: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. Acesso em: 25 nov 2023.

COELHO, A.C.B. **A lei geral de proteção de dados pessoais brasileira como meio de efetivação dos direitos da personalidade**. 2019. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/14305/1/ACBC05052019.pdf. Acesso em: 28 jun 2023.

COHEN, M. F. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação**, v. 31, n. 3, p. 26-36, set. 2002. Disponível em: https://doi.org/10.1590/s0100-19652002000300003. Acesso em: 31 jul. 2023.

DA ROSA, T.H.; FERRARI, G.M.R. PRIVACIDADE, INTIMIDADE E PROTEÇÃO DE DADOS PESSOAIS (aspectos brasileiros). **Argumenta Journal Law**, Jacarezinho - PR, n. 21, p. 137-166, fev. 2015. ISSN 2317-3882. Disponível em: <https://seer.uenp.edu.br/index.php/argumenta/article/view/495>. Acesso em: 31 jul. 2023. doi:http://dx.doi.org/10.35356/argumenta.v0i21.495.

DE TEFFÉ, C. S.; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1-38, 9 maio 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 31 jul. 2023.

DONEDA, D. **Da privacidade à proteção de dados pessoais**: fundamentos da lei geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 05/2020 on consent under Regulation 2016/679**. 4 mai 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 22 set 2023.

FACCHINI NETO, E.; DEMOLINER, K.S. DIREITO À PRIVACIDADE NA ERA DIGITAL – UMA RELEITURA DO ART. XII DA DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS (DUDH) NA SOCIEDADE DO ESPETÁCULO. **REVISTA INTERNACIONAL CONSINTER DE DIREITO**, v. 9, n. 9, p. 119-140, 18 dez. 2019. Disponível em: https://doi.org/10.19135/revista.consinter.00009.06. Acesso em: 31 jul. 2023.

FRAJHOF, Isabella Z.; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. In: MULHOLLAND, Caitlin (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020.

FRAZÃO, Ana. **Nova LGPD**: o tratamento dos dados pessoais sensíveis. 26 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 3 ago. 2023.

GIL, A.C. **Como elaborar projetos de pesquisa**. 4ª ed. São Paulo: Atlas, 2002.

HILL, K. How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did. **Forbes**, 16 fev 2012. Disponível em: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=78e57e366668 Acesso em 10 jun 2023.

HOFFMANN-RIEM, W. BIG DATA E INTELIGÊNCIA ARTIFICIAL: desafios para o Direito. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S. l.], v. 6, n. 2, p. 431–506, 2020. DOI: 10.21783/rei.v6i2.484. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/484. Acesso em: 31 jul. 2023.

HOFFMANN-RIEM, W. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 2 ed. Rio de Janeiro: Forense, 2022.

LAKATOS, E.M.; MARCONI, M.A. **Fundamentos da metodologia científica**. 5 ed. São Paulo: Atlas, 2003.

LESSIG, Lawrence. Code: And other laws of cyberspace. New York: Basic Books, 2000.

LIMA, C. C. Garantia da privacidade e dados pessoais à luz do Marco Civil da Internet. In: SALOMÃO LEITE, G.; LEMOS, R. (orgs.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 148-164.

LISBOA, R.S. Direito na sociedade da informação. **Revista dos Tribunais**, São Paulo, v. 95, n. 847, p. 78-95, maio 2006.

MAGRANI, E. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019.

MANTOVANI, A.C. **O CONSENTIMENTO NA DISCIPLINA DA PROTEÇÃO DOS DADOS PESSOAIS**: uma análise dos seus fundamentos e elementos. 2019. Dissertação de mestrado (Pós Graduação em Direito) — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019.

MARTINS, R. M.; GUARIENTO, D.B. **EC torna a proteção de dados pessoais um direito fundamental**. Migalhas, 18 fev. 2022. Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/359941/ec-torna-a-protecao-de-dados-pessoais-um-direito-fundamental. Acesso em: 6 fev. 2024.

MAXIMILIANO, C. **Hermenêutica e aplicação do direito**. 21 ed. Rio de Janeiro: Forense, 2017.

MAYER-SCHÖNBERGER, V. Generational Development of Data Protection in Europe. In **The Handbook of Information and Computer Ethics**, John Wiley & sons, pp. 219-241, 2008.

MENDES, L. S. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 12, n. 39, p. 185–216, 2019. DOI: 10.30899/dfj.v12i39.655. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 31 jul. 2023.

MENDES, L. S.; FONSECA, G. C. S. da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S. l.], v. 6, n. 2, p. 507–533, 2020. DOI: 10.21783/rei.v6i2.521. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 25 nov. 2023.

MENDES, L.S. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**, São Paulo: Ed. RT, nov. 2019, p. 35-56.

MENDES, L.S. O diálogo entre o Marco Civil da Internet eo Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 25, n. 106, p. 37-69, jul./ago. 2016.

MENDES, L.S. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 20, n. 79, jul/set, p. 42-82, 2011.

MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor**. Imprenta: São Paulo, Saraiva, 2014.

MENDES, L.S. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. 2008. **Repositório Institucional da UnB**, [s. l.], 2008. Disponível em: http://repositorio.unb.br/handle/10482/4782. Acesso em: 31 jul. 2023.

MODESTO, J.A. BREVES CONSIDERAÇÕES ACERCA DA MONETIZAÇÃO DE DADOS PESSOAIS NA ECONOMIA INFORMACIONAL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. **Revista de Direito, Governança e Novas Tecnologias**, v. 6, n. 1, p. 37, 26 ago. 2020. Disponível em: https://doi.org/10.26668/indexlawjournals/2526-0049/2020.v6i1.6558. Acesso em: 31 jul. 2023.

MONTEIRO, R.L. et al. **Lei Geral de Proteção de Dados e GDPR**: histórico, análise e impactos. Baptista Luz Advogados, 2019. Disponível em: https://baptistaluz.com.br/wp-content/uploads/sites/99/2019/01/RD-DataProtection-ProvF.pdf Acesso em: 31 jul. 2023.

MONTEIRO, R.L. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?. Instituto Igarapé, Artigo Estratégico 39. Dezembro, 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 10 jul 2023.

MONTORO, A.F. **Introdução à Ciência do Direito**. 29ª ed. São Paulo: RT, 2011.

MOTA, I. D.; ABAGGE, Y.R.; KNOERR, F.G. A LEI GERAL DE PROTEÇÃO DE DADOS: OS DADOS PESSOAIS PODEM SER CONSIDERADOS DIREITOS DA PERSONALIDADE?. **ECONOMIC ANALYSIS OF LAW REVIEW**, v. 10, p. 278-302, 2019.

MULHOLLAND, C. O tratamento de dados pessoais sensíveis. In: MULHOLLAND, C. (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. p. 121-156.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus,** v. 140, n. 4, p. 32-48, out. 2011. Disponível em: https://doi.org/10.1162/daed_a_00113. Acesso em: 25 nov. 2023.

OLIVA, A.C.; PESSOA, F.M.G. Bancos de Dados e a Proteção do Consumidor Brasileiro: o Panóptico Pós-Moderno. **Prim Facie**, [S. l.], v. 15, n. 28, p. 01–43, 2016. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/primafacie/article/view/27684. Acesso em: 31 jul. 2023.

PALMEIRA, M. M. A segurança e as boas práticas no tratamento de dados pessoais. In: MULHOLLAND, C. (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020, p. 319-342.

PERES, M.M.; SIMÃO FILHO, A. Credit scoring e a proteção de dados pessoais. **Direito e Desenvolvimento**, João Pessoa, v. 12, n. 1, p. 49-63, jan/jun 2021.

PEZZI, A.P.J. **A necessidade de proteção dos dados pessoais nos arquivos de consumo**: em busca da concretização do direito à privacidade. 2007. Universidade do Vale do Rio do Sinos, [s. l.], 2007. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/2400. Acesso em: 31 jul. 2023.

PINHEIRO, P.P. **Direito digital**. 7ª ed. São Paulo: Saraiva Educação, 2021.

REMEDIO, J. A.; REMEDIO, T. P.; REMEDIO, D. P. Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018): o consentimento do titular dos dados para o tratamento de seus dados pessoais. In: **I - Encontro Virtual do CONPEDI - Direito, Governança e Novas Tecnologias II**. Florianópolis: CONPEDI, 2020. v. 1. p. 75-92.

RODOTÁ, S. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Transformações do corpo. **Revista trimestral de direito civil**, v. 5, n. 19, p. 65–107, jul./set., 2004.

RUARO, R. L. ALGUMAS REFLEXÕES EM TORNO DO RGPD COM ALUSÕES A LGPD: um exercício interpretativo. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 14, n. 42, p. 219–249, 2020. DOI: 10.30899/dfj.v14i42.760. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/760. Acesso em: 25 nov. 2023.

SAITO, V. H. Desafios contemporâneos para a tutela dos direitos à privacidade e aos dados pessoais. **Res Severa Verum Gaudium**, Porto Alegre, v. 5, n. 2, 2021. Disponível em: https://seer.ufrgs.br/index.php/resseveraverumgaudium/article/view/110379. Acesso em: 31 jul. 2023.

SARLET, I.W. PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NA CONSTITUIÇÃO FEDERAL BRASILEIRA DE 1988. **Revista Brasileira de Direitos**

Fundamentais & Justiça, v. 14, n. 42, p. 179-218, 10 ago. 2020. Disponível em: https://doi.org/10.30899/dfj.v14i42.875. Acesso em: 31 jul. 2023.

SARTORI, E.C.M. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na Internet. **Revista de Direito Civil Contemporâneo**, vol. 9, out/dez 2016.

SCHELEDER, A.F.P; NOSCHANG, P.G. **Um ensaio sobre os direitos digitais de cidadania como nova categoria dos direitos de personalidade**. Balcão do Consumidor [recurso eletrônico]: coletânea cidadania, mediação e conciliação. Passo Fundo: Ed. Universidade de Passo Fundo, 2018. Disponível em: <https://www.upf.br/_uploads/Conteudo/Balc%c3%a3o%20do%20Consumidor/2019/cidadania_mediacao_e_conciliacao.pdf#page=9>. Acesso em: 15 jun. 2023.

SOARES, P.S.C. **A questão do consentimento na Lei Geral de Proteção de Dados**. 11 maio 2019. Disponível em: https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados. Acesso em: 31 jul. 2023.

SOUZA, C.A. LEMOS, R. **Marco civil da internet**: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda, 2016.

TEPEDINO, G. **Temas de direito civil**. 3ª ed. Rio de Janeiro: Renovar, 2004.

TEPEDINO, G.; DE TEFFÉ, C.S. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83-116, 2020. Disponível em: https://doi.org/10.33242/rbdc.2020.03.005. Acesso em: 28 jul. 2023.

TOBBIN, R.A.; CARDIN, V.S.G. Política de cookies e a “crise do consentimento”: Lei Geral de Proteção de Dados e a autodeterminação informativa. **Revista da Faculdade de Direito**, n. 47, p. 241-262, 31 dez. 2021. Disponível em: https://doi.org/10.22456/0104-6594.113663. Acesso em: 25 nov. 2023.

VENTURINI, J. et al. **Terms of service and human rights: an analysis of online platform contracts**. Rio de Janeiro: Revan, 2016.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193, 15 dez. 1890. Disponível em: https://doi.org/10.2307/1321160. Acesso em: 31 jul. 2023.

ZANATTA, R. A proteção de dados entre leis, códigos e programação: os limites do Marco Civil da Internet. In: DE LUCCA, N.; SIMÃO FILHO, A.; PEREIRA DE LIMA, C.R. (orgs.). **Direito e Internet III: Marco Civil da Internet**. São Paulo: Quartier Latin, 2015, p. 447-470.

ZANATTA, R. **Perfilização, discriminação e direitos**: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. 2019. DOI: http://dx.doi.org/10.13140/RG.2.2.33647.28328.

ZUBOFF, S. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021.