UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

Camila Fiamoncini Oliveira

Dados pessoais disponíveis publicamente e a prática de *data scraping*:
uma análise dos parâmetros legais impostos pela
Lei Geral de Proteção de Dados Pessoais

Florianópolis, SC
2022

Camila Fiamoncini Oliveira

Dados pessoais disponíveis publicamente e a prática de *data scraping*:
uma análise dos parâmetros legais impostos pela
Lei Geral de Proteção de Dados Pessoais

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador:
Prof.(a) Liz Beatriz Sass, Dr(a).

Florianópolis, SC
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Oliveira, Camila Fiamoncini
Dados pessoais disponíveis publicamente e a prática de data scraping : uma análise dos parâmetros legais impostos pela Lei Geral de Proteção de Dados Pessoais / Camila Fiamoncini Oliveira ; orientador, Liz Beatriz Sass, 2022.
80 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2022.

Inclui referências.

1. Direito. 2. Dados Pessoais Disponíveis Publicamente. 3. Lei Geral de Proteção de Dados Pessoais. 4. LGPD. 5. Data Scraping. I. Sass, Liz Beatriz. II. Universidade Federal de Santa Catarina. Graduação em Direito. III. Título.

Camila Fiamoncini Oliveira

Dados pessoais disponíveis publicamente e a prática de *data scraping*:
uma análise dos parâmetros legais impostos pela
Lei Geral de Proteção de Dados Pessoais

Este Trabalho Conclusão de Curso foi julgado adequado para obtenção do Título de Bacharel em Direito e aprovado em sua forma final pelo Curso de Graduação em Direito da Universidade Federal de Santa Catarina.

Florianópolis/SC, 15 de março de 2022.

Prof. Luiz Henrique Cademartori, Dr.
Coordenador do Curso de Graduação em Direito

Banca Examinadora:

Prof.(a) Liz Beatriz Sass, Dr(a).
Orientador - UFSC

Prof.(a) Angela Maria Rosso, Dr(a).
Avaliador - UFSC

Prof.(a) Tobias Pereira Klen, Dr(a).
Avaliador - UFSC

AGRADECIMENTOS

São muitas as pessoas e motivos para os quais posso dedicar meus agradecimentos e, em especial, minha gratidão. Sendo que para realizar tal tarefa poderia consagrar dias e até meses recordando de todos os indivíduos que, de alguma forma, colaboraram para que eu tivesse a oportunidade de cursar Direito na Universidade Federal de Santa Catarina e para que eu trilhasse este caminho do modo que o fiz. Contudo, para não tornar esta importante parte do Trabalho de Conclusão de Curso demasiadamente longa, contentar-me-ei com as principais menções, sem, de forma alguma, retirar de minha recordação os demais indivíduos que, por ventura, não tenha aqui citado.

Primeiramente, dedico meus agradecimentos e minha gratidão aos meus pais, Clarice e Márcio, e à toda minha família, pelos constantes aprendizados que contribuíram para que eu me transformasse na pessoa que sou, e pela dedicação em oferecer elementos que me estimulassem a não conter esforços para ser cada vez melhor, também no âmbito profissional, mas em todos os outros aspectos da vida.

Ao meu irmão, Felipe, por ser exemplo para mim, pelo suporte e parceira de uma vida, por ter sido família em Florianópolis, e por sempre proporcionar aprendizados durante nossa convivência. Ao meu namorado, Lucas, pelo apoio durante a realização desta pesquisa, pelo afeto, amparo e caminhos que trilhamos ao lado um do outro.

Aos amigos, Pedro, Lucas, Rhuann, Johann, André, Be e Gio, pela cumplicidade durante as aulas na graduação, à Dri e à Gabi, pelo companheirismo desde o início da faculdade, à Lury pela amizade sincera e pela sinergia como dupla no Escritório Modelo de Assistência Jurídica (EMAJ), e à Ju, pela amizade e parceria incondicional. Obrigada a todos por terem dado à Florianópolis os ares de casa.

À empresa júnior Locus Iuris, por ter me proporcionado vislumbrar novas possibilidades, pelo imensurável desenvolvimento técnico e pessoal em 2 anos e meio de experiência ao longo da minha graduação e pelas pessoas que fizeram parte dessa trajetória, em especial, Tobias, Amanda, Rafael e Ana Berti.

À UFSC, pela oportunidade de trilhar minha graduação em ambiente de acolhimento, de dedicação e de qualidade.

Ao escritório Lopes Advogados, pela oportunidade de atuar com consultoria

jurídica voltada à proteção de dados, despertando a paixão que hoje nutro pela área; por acreditar no desenvolvimento de profissionais através da experiência construída na prática, filosofia que construiu uma equipe singular, líder e inspiradora; e por fugir do óbvio.

Por fim, à minha orientadora Liz Beatriz Sass, pelo suporte técnico e emocional, pela empatia, pela delicadeza e pela disponibilidade durante todo o processo de elaboração desta pesquisa; e à banca avaliadora, Tobias Pereira Klen e Angela Maria Rosso, por terem aceitado o convite para colaborar em um tema áspero e pouco explorado e por constituírem, todos, exemplos de profissionais, nos quais me espelho e guardo profundo respeito.

OLIVEIRA, Camila Fiamoncini. **Dados pessoais disponíveis publicamente e a prática de *data scraping***: uma análise dos parâmetros legais impostos pela Lei Geral de Proteção de Dados Pessoais. 2022. 80f. Trabalho de Conclusão de Curso (Graduação) – Curso de Graduação em Direito, Universidade Federal de Santa Catarina, Florianópolis/SC, 2022.

Orientador: Prof.(a) Liz Beatriz Sass, Dr(a).

RESUMO

Dentro dos cenários de tratamento de dados pessoais que se desenham atualmente, principalmente decorrentes do contexto do Big Data, o *data scraping* adquire pertinência por ser um método que automatiza a coleta de dados da *Web,* o que inclui dados pessoais*.* Por conseguinte, questionamentos sobre as implicações da Lei n. 13.709/2018 (Lei Geral Proteção de Dados Pessoais - LGPD) sobre tal prática ganham relevância e atualidade. Diante disso, por meio do método dedutivo, a presente pesquisa busca delimitar quais os parâmetros impostos pela LGPD para o tratamento de dados pessoais disponíveis publicamente, categoria mais suscetível à prática do *data scraping* devido à sua ampla acessibilidade. Inicialmente, faz-se uma abordagem da evolução conceitual e do contexto legislativo em torno das ideias sobre privacidade e proteção de dados pessoais, buscando, inclusive, diferenciá-las. Em seguida, conceitua-se o *data scraping*, levantando os riscos da prática para a proteção de dados pessoais e para a privacidade; delimita-se o que se insere na concepção de dado pessoal de acesso público e dado pessoal tornado manifestamente público pelo titular, que conjuntamente são denominados nesta pesquisa como dados pessoais disponíveis publicamente; e ainda, aprofunda-se nos requisitos gerais e específicos - estes últimos previstos nos §§3º, 4º e 7º do art. 7º da LGPD - que devem ser observados no tratamento de dados pessoais disponíveis publicamente. Com base nessas premissas, a parte final da pesquisa concentra-se no estudo do requisito que impõe a necessidade de indicar uma base legal ao tratamento de dados pessoais, e de que forma essa exigência aplica-se à prática do *data scraping* voltada aos dados pessoais disponíveis publicamente*.* Para tanto, propõe-se a compreensão das hipóteses dos §§ 3º, 4º e 7º do art 7º da Lei como bases legais autônomas, e subsidiariamente, destaca-se o legítimo interesse e, principalmente, os parâmetros que tal hipótese autorizativa exige caso seja utilizada como fundamento legal*.* Por fim, apresenta-se a teoria da privacidade contextual como referencial teórico complementar, para vislumbrar um equilíbrio entre as novas formas de tratamento de dados pessoais decorrentes dos avanços da tecnologia e a garantia de controle ao titular sobre seus dados pessoais, bem como para ampliar a concepção da autodeterminação informacional, transpondo alguns estigmas tradicionais atrelados a este conceito.

Palavras-chave: Dados Pessoais Disponíveis Publicamente**.** Lei Geral de Proteção de Dados Pessoais. LGPD. *Data Scraping*.

ABSTRACT

Considering the personal data processing scenarios that are currently designed, mainly arising from the context of Big Data, data scraping acquires relevance as a method that allows to automate the collection of data from Web, which includes personal data. Therefore, questions about the implications of Law n. 13.709/2018 (General Personal Data Protection Law - LGPD) on such practice gain relevance and topicality. For this reason, the present research aims to delimit the parameters imposed by LGPD for the publicly available personal data processing, since this data category – publicly available personal data - is highly susceptible to the practice of data scraping due to its wide accessibility. First, an approach is made to the conceptual evolution and legislative context around the ideas about privacy and personal data protection, concluding what are the conceptual differences between both aceptions. Then, the concept of data scraping is presented, as well as the risks of the practice for privacy and personal data protection; the concept of publicly accessible personal data and personal data made manifestly public by the data subject are defined, which together are referred to, in this research, as publicly available personal data; and also, it is presented the general and specific parameters - the latter provided by §§3, 4 and 7 of article 7 of LGPD - which must be fulfilled in order to publicly available personal data processing be lawful. Based on these premises, the final part of the research focuses on the study of the parameter that imposes the need to indicate a legal basis for the personal data processing, and how this requirement applies to the practice of data scraping of publicly available personal data. In conclusion, the research proposes to understand the hypotheses of §§ 3, 4 and 7 of article 7 of LGPD as autonomous legal basis, and alternatively, proposes to analyses the legitimate interest and, mainly, the parameters that such authorizing hypothesis requires to be indicated as a legal basis. Finally, the theory of contextual privacy is presented as a complementary theoretical reference, to visualize a balance between the new ways of processing personal data - resulting from advances in technology - and the guarantee of control to the data subject over his personal data, as well as to expand the conception of informational self-determination, since the theory transposes some traditional stigmas linked to this concept.

Keywords: Publicly Available Personal Data. General Law for the Protection of Personal Data. LGPD. Data Scraping.

LISTA DE SIGLAS

CDC	-	Código de Defesa do Consumidor
CNIL	-	*Commission Nationale de l'Informatique et des Libertés*
EC	-	Emenda Constitucional
EDPS	-	*European Data Protection Supervisor*
GDPR	-	*General Data Protection Regulation*
ICO	-	*Information Commissioner's Office*
IP	-	Internet Protocol
LAI	-	Lei de Acesso à Informação
LGPD	-	Lei Geral de Proteção de Dados Pessoais
MCI	-	Marco Civil da Internet
OAIC	-	*Office of the Australian Information Commissioner*
PI	-	*Privacy Internacional*
RGPD	-	Regulamento Geral de Proteção de Dados
STF	-	Supremo Tribunal Federal
STJ	-	Supremo Tribunal de Justiça
TIC	-	Tecnologias da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

O avanço das tecnologias de informação e comunicação tem gerado implicações diretas no escalonamento da capacidade de processamento de dados em relação aos aspectos de velocidade, volume e variedade, características intrínsecas ao moderno conceito de *Big Data*. Essa revolução tecnológica proporcionou incontáveis benefícios, como o desenvolvimento de melhores estratégias na prevenção à fraude, aprimoramento das pesquisas acadêmicas, gestão mais eficaz de políticas públicas no âmbito do Poder Público, entre outros.

Por consequência, o objeto do processamento de dados também passa a abranger os dados pessoais, isto é, as informações que dizem respeito a uma pessoa física capazes de torná-la identificada ou identificável. Em especial, integram este contexto os dados pessoais *disponíveis publicamente*, já que se encontram mais acessíveis que outros na *World Wide Web.*

Como exemplos de modelos de negócios que focam no processamento de dados pessoais, tem-se os *data brokers*, que dão insumos para uma cadeia de empresas que utilizam da publicidade online direcionada, da avaliação dos hábitos de navegação dos consumidores, da avaliação para concessão de crédito, entre outras finalidades.

Nesta esfera destaca-se o *data scraping*, tendo sido definido nesta pesquisa como uma técnica automatizada de coleta de dados na *Web* através de “bots” ou agentes de software. Essa prática tem ganho um papel importante, pois é um dos possíveis meios de coletar dados e possibilitar a criação de uma base de dados, por meio da qual buscar-se-á estruturar informações relevantes e padrões de conhecimentos.

Diante dos desafios impostos pelas novas tecnologias que originam novas formas de tratamento de dados pessoais, em paralelo à promulgação de legislações acerca do tema; suscitam-se discussões e questionamentos sobre como se dará a aplicação da LGPD neste contexto de processamento ágil e intenso de dados pessoais que ocorre na atualidade, o que inclui o *data scraping*. Esses questionamentos vão desde como observar os princípios, os fundamentos e as garantias previstas aos titulares de dados em um contexto em que o mesmo banco de dados pessoais pode ser utilizado para diferentes propósitos ou em um meio em que o tratamento de dados encontra obstáculos triviais, tais como viabilizar a prestação de informação ao titular; até a questão de como informar as finalidades do tratamento ao titular de dados pessoais quando uma disponibilização de um dado pessoal em uma rede social, por exemplo, pode abrir incontáveis possibilidades de tratamento posterior, sendo de alta dificuldade a limitação de propósitos.

Evidente que não se pretende elucidar tais problemáticas em todos seus detalhamentos e contornos. Todavia, diante da atualidade e relevância do tema, busca-se nesta pesquisa, através do método dedutivo, responder quais são os parâmetros estabelecidos pela LGPD para a prática de *data scraping* voltada a dados pessoais disponíveis publicamente, isto é, os aspectos basilares a serem observados para que a prática seja considerada lícita e adequada.

Para tanto, no primeiro capítulo, traça-se (i) o contexto de surgimento do direito à privacidade e à proteção de dados pessoais e da evolução dessas duas acepções, a fim de conceber como se conectam - tendo sido resultado de evoluções conceituais interligadas - e como se diferenciam entre si; (ii) o cenário normativo nacional sobre a proteção de dados pessoais, anterior à LGPD; e, por fim, (iii) o contexto de promulgação da LGPD e os conceitos insculpidos pela legislação, fundamentais para o desenvolvimento da presente pesquisa.

No segundo capítulo, afunila-se mais o objeto da pesquisa ao delinear (i) o conceito de *data scraping* e os riscos que a prática apresenta para o direito à privacidade e à proteção de dados pessoais; (ii) o conceito de dados de acesso público e dados tornados manifestamente públicos pelo titular, que, em conjunto, são tratados aqui como dados disponíveis publicamente; e (iii) os requisitos gerais - com exceção do requisito de indicação da base legal, a ser tratado no terceiro capítulo - e específicos para o tratamento de dados disponíveis publicamente, sendo estes últimos delimitados pelas disposições dos §§3º, 4º e 7º do art. 7º da LGPD.

No terceiro capítulo, considerando a bagagem conceitual e a delimitação dos requisitos para o tratamento de dados pessoais disponíveis publicamente, aborda-se (i) o requisito geral que impõe a fundamentação do tratamento em uma base legal. Para tanto, (i.1) leva-se em conta a compreensão das hipóteses dos §§ 3º, 4º e 7º do art. 7º da LGPD como bases legais autônomas, e propõe-se alguns níveis de avaliação para que se aproxime de uma base legal mais adequada para a prática de *data scraping* voltada a dados disponíveis publicamente; ainda, (i.2) subsidiariamente, analisa-se o legítimo interesse como possível base legal e os parâmetros que esta hipótese autorizativa exige, principalmente devido ao fato de ser a base legal mais abrangente, que gera maiores dúvidas em sua aplicação e que apresenta-se, em circunstâncias específicas, como possibilidade ao consentimento. Por fim, busca-se (ii) propor a teoria da privacidade contextual como um referencial teórico relevante para se conceber um equilíbrio entre as novas tecnologias, que deram ensejo a uma realidade de processamento intensivo de dados, com a proteção dos dados pessoais e a garantia do controle ao titular sobre suas informações, através da observância da chamada integridade contextual.

2 EVOLUÇÃO CONCEITUAL E LEGISLATIVA DA PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

Considerando a correlação direta e muitas vezes a confusão conceitual em torno das suas concepções, é relevante para o desenvolvimento da presente pesquisa uma abordagem sobre o contexto histórico e legislativo do surgimento das ideias sobre a privacidade e a proteção de dados na sociedade, bem como sua evolução.

Para Rodotà (2008, p. 15), o direito à privacidade, atualmente, pode ser compreendido como “o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular”.

Bioni (2019, p. 66) por sua vez, afirma que a proteção aos dados pessoais não se confunde com o direito à privacidade, já que o primeiro ultrapassa a esfera do último e penetra as esferas de outros direitos da personalidade, tendo em vista que os dados pessoais guardam relação com várias espécies de direitos da personalidade.

Ainda que os conceitos esboçados atualmente por conceituados juristas não sejam sempre homogêneos, a presente pesquisa inicia apresentando essas duas acepções, uma do direito de privacidade e outra da proteção de dados, para frisar que estes conceitos decorrem de uma trajetória histórica, tecnológica e legislativa que contribuiu para que se chegasse ao entendimento contemporâneo sobre a temática.

Por isso, a primeira parte desta pesquisa propõe-se a explorar e reunir informações relevantes sobre o surgimento do direito de privacidade e da proteção de dados pessoais, e, assim, partir para a análise dessas influências no Brasil até a promulgação e a entrada em vigor da Lei n. 13.709, de 14 de agosto de 2018 (BRASIL, 2018), intitulada de Lei Geral de Proteção de Dados Pessoais (LGPD). Ainda, após traçada essa trajetória, tratar-se-á sobre os principais conceitos e disposições trazidas pela LGPD, visto seu papel basilar para o desenvolvimento da presente pesquisa.

2.1 CONTEXTO HISTÓRICO E LEGISLATIVO DO DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS

Inicia-se tratando do direito à privacidade e à proteção de dados no mesmo capítulo, tendo em vista a estreita correlação entre ambas as acepções. Tal conexão, como se buscará demonstrar, reflete-se nos contextos histórico e legislativo do nascimento e desenvolvimento desses direitos.

Portanto, para se compreender o surgimento do direito à proteção de dados pessoais, é imprescindível analisar o surgimento da ideia de privacidade e a sua evolução conceitual.

Assim, tratar-se-á, inicialmente, do direito à privacidade, em seguida, das gerações de leis relativas à proteção de dados pessoais para, por fim, delimitar as similaridades e diferenças entre os dois conceitos. Essa diferenciação conceitual é relevante para desenvolvimento da pesquisa e para compreensão do porquê os dados pessoais, mesmo aqueles de acesso público, devem ser tutelados pela proteção de dados pessoais.

2.1.1 Evolução do direito à privacidade

Como um marco primordial sobre a discussão do tema da privacidade (FORTES, 2017, p. 272), tem-se o artigo dos norte-americanos Samuel Warren e Louis D. Brandeis, The Right to Privacy, publicado no ano de 1890, na Revista de Direito da Universidade de Harvard (WARREN; BRANDEIS, 1890).

Ao vislumbrar as possíveis consequências danosas à vida privada dos indivíduos frente à evolução da tecnologia, tal como as técnicas no campo da fotografia que permitiam a geração de fotos instantâneas, os autores preocuparam-se em investigar quais seriam as bases jurídicas que poderiam garantir a defesa da privacidade diante destes eventos, qual a natureza deste direito que se pretendia defender e seus limites (RUARO; MOLINARO, 2017, p. 16).

Contudo, conforme adverte Doneda (2021, p. 126), a referida obra não deve ser vista de modo isolado, desconsiderando o fato desta ser parte de “um contexto bem mais amplo no qual a sociedade norte-americana e o sistema capitalista se encontravam”.

Por esse motivo, importante esclarecer que apesar da tradução literal que dá título à obra parecer evocar o direito à privacidade como sinônimo ao chamado “the right to privacy”, a concepção deste último está de modo mais íntimo relacionado a um direito geral de personalidade, que atrai para si características mais abrangentes e regula diversos cenários distintos (DONEDA, 2021, p. 127).

A lógica argumentativa utilizada pelos juristas Warren e Brandeis é que, assim como poder-se-ia proteger as emoções externalizadas através de músicas, igual proteção mereceriam aquelas emoções, sentimentos, pensamentos expressos por

outros meios. A diferença é que “o que estaria a se proteger não era o princípio da propriedade privada, mas, sim, a inviolabilidade pessoal” (RUARO; MOLINARO, 2017, p. 18).

A proteção do chamado “right to privacy” respalda-se não mais no direito de propriedade, rechaçando a ideia da privacidade como um direito derivado daquele, mas nos direitos da personalidade e na própria dignidade da pessoa humana (RUARO; MOLINARO 2017, p. 16). Assim, torna-se possível reconhecer um direito à privacidade por si só, como uma das espécies dos direitos individuais garantidos ao homem (FORTES, 2017, p. 274).

A obra de Warren e Brandeis posicionou a privacidade sob um novo ângulo de análise e compreensão e abriu horizontes para o alcance do patamar de direito constitucionalmente reconhecido (DONEDA, 2021, p. 128).

A partir de então, o reconhecimento do direito à privacidade passa a ganhar cada vez mais espaço, inclusive no âmbito do direito internacional, sendo que, após a Segunda Guerra Mundial, diversos documentos passam a mencioná-lo tais como a Declaração Americana dos Direitos do Homem, que consistiu no primeiro instrumento a tratar sobre o direito à privacidade, resultante da IX Conferência Internacional Americana, que ocorreu em Bogotá em 1948. Tendo como objetivo a proteção de direitos essenciais da pessoa humana (FERREIRA; PINHEIRO; MARQUES, 2021, p. 158), restou estabelecido, em seu artigo V, o direito do indivíduo à proteção da lei contra ataques abusivos à honra, reputação e vida particular e familiar.

No mesmo sentido, a Declaração Universal dos Direitos Humanos, no mesmo ano de 1948, em seu artigo 12, resguarda o direito à privacidade ao prever a proteção do indivíduo contra interferências em sua vida privada, família, lar e correspondência, assim como de ataques à sua honra ou reputação (ONU, 1948).

No contexto europeu, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, aprovada em Roma, no ano de 1950, demonstrou os reflexos e as preocupações decorrentes do término da Segunda Guerra Mundial, porque limitou, conforme seu artigo 8º[1], a proteção da vida privada

[1] “1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.” (COUNCIL OF EUROPE, 1950).

com exceções pontuais vinculadas à proteção da democracia, segurança pública ou nacional (FORTES, 2017, p. 277).

Todos esses instrumentos jurídicos possuem um ponto em comum no contexto de surgimento e admissão do direito à privacidade, pois buscam garantir o respeito à vida privada do indivíduo. Dessa forma, fica evidente que o reconhecimento da privacidade como um direito fundamental sucedeu de um movimento internacional.

No entanto, o avanço da tecnologia, o desenvolvimento das técnicas de processamento de dados e a trivialização do computador como um equipamento básico nos lares de considerável parte da população, descortinou maiores preocupações acerca da privacidade. Isso porque o armazenamento e a avaliação de dados relacionados aos indivíduos tornaram-se processos facilitados, despertando interesses de diversos setores que vislumbraram o valor da coleta e utilização de dados pessoais de terceiros. Situações como as descritas acima, intensificadas pela realidade das Tecnologias da Informação e Comunicação (TIC) mas não restritas somente a esse contexto, abriram margem para a insegurança dos dados pessoais coletados e reforçaram uma falta de transparência quanto à sua utilização (RODRIGUEZ; RUARO, 2010, p. 183).

Assim, frente às TICs, a proteção jurídica tradicional concedida à privacidade até então se mostrou insuficiente para abarcar todas as possíveis repercussões derivadas desta sociedade da informação (RODRIGUEZ; RUARO, 2010, p. 183).

Conclui-se, portanto, que a privacidade extrapolou a esfera tradicional do seu conceito - vinculada ao direito de não sofrer interferências alheias no âmbito privado - para desdobrar-se também em torno da informação e, em especial, a pessoal (DONEDA, 2021, p. 177), viabilizando espaço para o surgimento do direito à proteção de dados pessoais como um direito autônomo.

2.1.2 Gerações das leis relativas à proteção de dados pessoais

Buscou-se, à priori, tratar do contexto e evolução do direito à privacidade por estar intrinsecamente ligado à evolução da concepção do direito à proteção dos dados pessoais, de modo que o surgimento do último, conforme pretende-se demonstrar a seguir, conecta-se ao primeiro como uma espécie de continuação, traçando, todavia, características próprias e atuais a esta disciplina (DONEDA, 2021, p. 177).

Assim, para fins didáticos, parte da doutrina adota uma classificação

estruturada em quatro gerações que se refere à evolução de paradigmas das leis relativas à proteção de dados pessoais.

Ao debruçar-se sobre o estudo das gerações das leis é possível observar como o regime jurídico da proteção de dados pessoais, que inicialmente surge de uma ideia de derivação da privacidade, vai ganhando espaço como um direito autônomo.

Nesse sentido, a primeira geração de leis que buscam a salvaguarda dos dados pessoais surgiu na década de 1970. Alguns exemplos são destacados por Doneda no seguinte trecho (DONEDA, 2021, p. 179):

> Entre as precursoras, a já mencionada Lei do *Land* alemão de Hesse, em 1970; a primeira lei nacional de proteção de dados que foi, na Suécia, o Estatuto para bancos de dados de 1973 – *Data Legen*, ou *Datalag* (que por sua vez também criava um inspetor para o uso de dados pessoais – o Dataispektionen), além do *Privacy Act* norte-americano em 1974.

As referidas legislações eram reflexo da experiência do *National Data Center* e outros casos similares. O *National Data Center* foi objeto de um projeto de lei nos Estados Unidos, cuja proposta consistia na construção de uma base de dados centralizada no país, e que, em 1960, não foi aprovado pelo Congresso americano, tendo em vista justamente a preocupação acerca dos riscos à privacidade que sua concretização poderia acarretar (TAVARES, 2022, p. 9-10), além do excessivo crescimento de poder do governo diante do controle desta base de dados (DONEDA, 2021, p. 166).

Por conseguinte, as chamadas leis de primeira geração de proteção de dados pessoais tinham como núcleo central a proteção dos dados pessoais em face dos perigos da coleta irrestrita de informações, que era predominantemente realizada pelo Estado.

Tais legislações baseavam-se, por exemplo, em uma lógica regulatória de concessão de autorizações para a criação de bancos de dados e no controle dos mesmos por órgãos públicos (DONEDA, 2021, p. 180). Focalizava-se, portanto, na esfera governamental e na previsão de normas rígidas que barrassem o uso da tecnologia, a fim de garantir que a figura do Estado não coibisse a liberdade do cidadão através da vigilância excessiva (BIONI, 2019, p. 114).

Diante da ampliação do processamento de dados para além da esfera governamental e do crescimento destes centros de processamento, a insuficiência das leis de primeira geração e a inviabilidade de manutenção da estrutura jurídica de

concessões e regras rígidas, adotada inicialmente, impôs a necessidade de um novo arranjo quanto à proteção dos dados pessoais (DONEDA, 2021, p. 181).

Por volta da segunda metade da década de 70, passa-se por uma mudança de paradigma em relação às legislações de proteção de dados, partindo-se para as chamadas leis de segunda geração, as quais dão enfoque na autonomia do próprio titular de dados para ingerência de seus dados pessoais e ainda ampliam sua área de aplicação para a esfera privada (BIONI, 2019, p. 115). Como exemplos deste modelo cita-se a lei francesa de proteção de dados pessoais de 1978 (*Informatique at Libértes*), a lei austríaca de 18 de outubro de 1978 (*Datenschutzgesetz*) e as constituições portuguesa e espanhola que se direcionam neste sentido, apesar de terem promulgado leis específicas mais tarde (DONEDA, 2021, p. 169).

Ao invés de voltar-se para o fenômeno tecnológico em si, como objeto que necessita de regulação e até certa coibição, as leis de segunda geração fundamentam-se no direito à privacidade e proteção de dados pessoais como uma liberdade negativa a ser exercida pelo próprio cidadão, e, por conseguinte, buscam conceder recursos para que este constate a utilização indevida de seus dados pessoais e exija tutela (DONEDA, 2021, p. 181).

A segunda geração das leis também apresentava suas fragilidades, o que motivou uma nova abordagem, dando origem à terceira geração das leis acerca da proteção de dados pessoais. Conforme Doneda (2021, p. 182):

> Estas leis **(de segunda geração - Grifo do Autor)** 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.

Diante dessa problemática, a terceira geração de leis sobre a temática manteve o foco no cidadão, mas alargou o escopo de tutela dos dados pessoais. Aqui

alcança-se o ápice da terminologia: autodeterminação informacional[2] (DONEDA, 2021, p. 182-183).

A autodeterminação informacional, portanto, consistiria no direito de controle do titular sobre o trânsito de dados pessoais, como resultado da conjugação da (i) concepção da privacidade como liberdade negativa do titular não sofrer interferência alheia e (ii) da concepção moderna, que engloba a proteção de dados pessoais por todo seu fluxo, e que impõe proteção dinâmica durante todo o ciclo de vida do dado pessoal - o que inclui deveres aos agentes de tratamento (VAINZOF, 2019, p. 27).

Isso decorre do entendimento do tratamento de dados pessoais como um processo, que não se limita ao momento de escolha do titular pela disponibilização de informações, mas sim que abrange todo um percurso de processamento e utilização do dado. Ao longo deste percurso algumas garantias devem ser respeitadas, como o dever de informação (DONEDA, 2021, p. 183).

De outra parte, deu-se protagonismo ao indivíduo ao buscar assegurar sua participação em cada movimento dos seus dados pessoais, muito fundamentado no consentimento. Todavia, essa estratégia também apresentou fragilidades (BIONI, 2019, p. 116).

A diferença entre a chamada quarta geração de leis e a terceira reside no reconhecimento da relação desigual que se opera entre o cidadão e as entidades que coletam e processam seus dados, tanto no âmbito público como na esfera privada, e na posição de vulnerabilidade do titular destas informações.

Exploram-se, sob essa perspectiva, proposições normativas alternativas que não deixassem apenas sob as mãos do indivíduo a escolha sobre o processamento de dados pessoais, como no caso de impor limites ao tratamento que independem da vontade do titular, relativizando-se a centralidade do consentimento (BIONI, 2019, p. 116-117).

Ainda assim, observa-se que o protagonismo do consentimento permaneceu como traço marcante da abordagem regulatória, inclusive, tendo sido objeto de distribuição de qualificadores, como livre, informado, inequívoco, específico e/ou

---

[2] A autodeterminação informacional foi inicialmente reconhecida em decisão da Corte Constitucional alemã no julgamento do caso da Lei do Censo de 1983, que pretendia coletar e tratar diversos dados pessoais da população, a princípio, para propósitos de mensurar estatísticas espaciais e geográficas da população. Todavia, na Lei constava a possibilidade de compartilhamento e cruzamento de informações com outros registros públicos, além de que as finalidades eram vagas e amplas, não deixando claro como os dados seriam, de fato, tratados após coleta. (BIONI, 2019, p. 101-103).

explícito. Seu protagonismo tanto continua sendo marcante que desenha, segundo Bioni, um paradigma de autodeterminação informacional quase como sinônimo de consentimento. Essa perspectiva tem efeitos na própria aplicação das normas a respeito da proteção de dados, que tem seguido tal norte regulatório (BIONI, 2019, p. 117).

A partir dessa análise, conclui-se que, frente aos mais diversos contextos que a sociedade da informação descortina, foi necessário o reconhecimento e a ampliação da proteção dos dados pessoais do indivíduo, para que se ajustasse aos cenários enfrentados em cada período geracional.

2.1.3 Convergências e diferenciações relevantes entre a privacidade e a proteção de dados pessoais

A proteção de dados foi ampliando os horizontes do direito à privacidade, porém, as duas acepções não necessariamente se confundem.

Para Rodotà (2008) o direito da privacidade atualmente perpassa não somente ou de modo predominante o direito de estar só, mas principalmente o direito de obter maior controle sobre o fornecimento e utilização de informações pessoais:

> Frente aos novos desafios, é cada vez mais claro que o sentido de isolamento predominante na doutrina do direito à privacidade do tempo de Brandeis e Warren está superado. Neste novo panorama, a privacidade deixa de ser um meio de garantir o isolamento de alguns para cumprir também uma outra função, que é reagir contra políticas de discriminação baseadas em opiniões e opções religiosas, políticas e sexuais, bem como de toda sorte de informações privadas. (RODOTÀ, 2008, p. 117).

O direito à privacidade passa a ampliar suas facetas e passa a preocupar-se com a esfera que diz respeito à proteção de dados pessoais e às responsabilidades que da última decorrem para o próprio titular e para os agentes que processam dados pessoais.

Do mesmo modo, para Doneda (2021, p. 139) a privacidade adota cada vez mais uma construção em torno dos dados pessoais, o que fica evidente a partir da evolução normativa acerca do tema.

Contudo, deve-se destacar que a proteção de dados pessoais, ainda que se conecte à privacidade, não está limitada por esta, pois faz referência a diversas

garantias fundamentais do ordenamento jurídico pátrio (DONEDA, 2006, p. 235).

No mesmo sentido, Bioni (2019, p. 93) estabelece algumas diferenças entre as duas acepções que particularmente interessam a presente pesquisa. O direito à privacidade estrutura-se historicamente por meio do binômio público e privado, tendo como foco a delimitação do que está na esfera privada e o que está se desempenhando publicamente.

A proteção da privacidade permite a existência de refúgio ao indivíduo para se afastar do espaço público, a fim de que ele tenha a opção de manter preservadas informações de sua esfera privada. Desse modo, o titular tem a opção de realizar uma revelação seletiva de informações pessoais. É neste sentido que se concebe a privacidade como direito de estar só e protegido de interferências alheias, tratando-se de uma liberdade negativa (BIONI, 2019, p. 94).

Porém, modernamente, a privacidade ganha nova dimensão, pois a tutela do direito de privacidade perpassa um controle das informações pessoais e há de ser construído, tratando-se de uma proteção dinâmica (BIONI, 2019, p. 97).

Ainda assim, a proteção de dados pessoais não pode resumir-se à mera evolução da privacidade. Ela adquire autonomia pois deixa de ser conduzida pela lógica dicotômica do público e privado. Basta que uma informação esteja atrelada a uma pessoa física, independente do seu caráter público ou privado, para que nasça o direito à proteção dos dados pessoais (BIONI, 2019, p. 98).

Isso significa dizer que mesmo que o titular tenha escolhido divulgar sua informação para o público, ainda existem deveres que impõem limitações ao tratamento destes dados pessoais. Não é porque a informação pessoal não encontra-se na esfera privada do indivíduo - tendo sido publicizada, por exemplo - que ela não merecerá tutela jurídica.

Logo, a despeito das divergências conceituais, o direito à privacidade e o direito à inviolabilidade dos dados pessoais conectam-se tanto quando se debruça sobre suas conceituações, como quando se analisa a evolução histórica de cada uma dessas acepções (FORTES, 2017, p. 279). E é fato que, conforme Bioni (2019, p. 99-101), na sociedade da informação atual, a proteção dos dados pessoais alcança papel tão abrangente e fundamental que passa a adentrar em várias outras esferas, além da que se refere à privacidade, não cabendo mais ser reduzida simplesmente a uma derivação desta.

2.2 DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Por meio do avanço das novas tecnologias, as formas de violações do direito à privacidade foram alteradas e ampliadas, de modo que a concepção de privacidade também necessitou ser compreendida através de novos ângulos e perspectivas. É neste momento que a ideia de proteção de dados pessoais começa a se avolumar.

Movimento semelhante ocorre no Brasil, isto é, a privacidade precedeu a proteção de dados pessoais. Enquanto a primeira detinha previsão expressa na Constituição Federal; a segunda, somente mais tarde, foi reconhecida como direito fundamental. Concomitantemente, busca-se demonstrar que a discussão acerca da proteção de dados pessoais já está há tempos na pauta nacional, visto o diverso número de legislações infraconstitucionais que tangenciam o tema. Contudo, é evidente que após a promulgação da LGPD tornou-se possível falar em, de fato, uma estruturação do sistema de proteção de dados no Brasil. Dado este fato, passa-se a apresentação dos conceitos primordiais estatuídos neste diploma normativo.

2.2.1 Proteção de dados pessoais como direito fundamental e legislações tangenciais e pertinentes à privacidade e à proteção de dados pessoais no Brasil

Apesar da Carta Magna não se utilizar do termo privacidade, faz menção à inviolabilidade da intimidade e da vida privada, prevendo-a como direito fundamental em seu art 5º, inciso X (BRASIL, 1988). Por sua vez, até a recentíssima promulgação da Emenda Constitucional nº 115, de 11 de fevereiro de 2022, a proteção de dados pessoais, nestes exatos termos, não se encontrava expressa na Constituição Federal. Contudo, garantias que perpassam a proteção de dados pessoais já anteriormente encontravam amparo no inciso XII, cujo objeto consiste na inviolabilidade da correspondência, comunicações telegráficas, de dados e das comunicações telefônicas (BRASIL, 1988).

A rigor, uma interpretação inicial, diante da leitura da Constituição Brasileira, poderia justificar o entendimento de que a proteção de dados pessoais mereceria resguardo constitucional quanto à sua “comunicação”, com base no inciso XII do art. 5º, que prevê a inviolabilidade das comunicações de dados (DONEDA, 2021, p. 269-

270). Neste sentido, inclusive, houve decisão do Supremo Tribunal Federal (STF), no RE 418.416/SC[3] (BRASIL, 2006, p. 74), de relatoria do Ministro Sepúlveda Pertence, que reconheceu a inexistência, com fundamento em garantias constitucionais, da proteção dos dados em si, mas apenas da sua comunicação.

Todavia, para Doneda (2021, p. 271), trata-se de interpretação temerosa, vez que haveria uma lacuna entre a garantia constitucional à privacidade e a proteção de informações pessoais, que sob perspectiva da corrente citada, deteria tutela mais sutil. Tal lacuna abre brechas para gerar uma exoneração dos agentes frente à uma ofensa à privacidade ou a outros direitos fundamentais, quando originada de uma utilização excessiva ou imoderada dos dados pessoais de um indivíduo.

A limitação à proteção dos dados pessoais apenas quando da sua comunicação e interceptação ocasionava brechas e distanciava-se da complexidade e amplitude dos fenômenos cada vez mais crescentes vinculados ao processamento e coleta de dados, impulsionados pela sociedade da informação (DONEDA, 2021, p. 271).

Assim, já era possível o reconhecimento do direito fundamental da proteção de dados pessoais frente à uma interpretação sistemática da Carta Magna, e principalmente, com fundamento em um dos postulados basilares do sistema jurídico brasileiro: a dignidade da pessoa humana. Ruaro e Molinaro (2017, p. 23) afirmam que:

> A dignidade da pessoa humana é fonte primária que apresenta as diretrizes do ordenamento jurídico dos Estados de Direito, representando vetor interpretativo e indicativo, e em se tratando do direito brasileiro, apresenta-se como um dos fundamentos do próprio Estado de Direito.

Com a proteção constitucional ao princípio da dignidade da pessoa humana, consagrada no art. 1º, III, da Carta Magna, protege-se prontamente todos os direitos da personalidade, sendo que especialmente restaram positivadas as tutelas ao direito de liberdade de expressão (art. 5º, inc. IX), informação (art. 5º, inc. XV), privacidade (art. 5º, inc. X) e violação de correspondência (art. 5º, inc. XII) (RUARO; MAÑAS; MOLINARO, 2017, p. 25).

Contudo, também se protegem outros direitos que amparam o princípio da dignidade da pessoa humana e que não necessariamente estão expressos no texto

[3] A decisão (RE 418.416/SC, de 2006) cita a obra de Ferraz Jr. (1993, p. 447).

constitucional. Isso porque, conforme Ruaro e Molinaro (2017, p. 26), para se garantir amplo respeito ao princípio constitucional da dignidade, é necessário conceder proteção ampla à pessoa humana nos mais diversos aspectos, inclusive aquele que concerne à proteção de dados pessoais, tendo em vista os riscos intrínsecos vinculados à inexistência de tutela robusta das informações que digam respeito ao indivíduo:

> No que concerne à identificação dos direitos da personalidade na Carta Política vigente, é fundamental salientar o apontamento feito por Gustavo Tepedino, no sentido de que não seria necessário que os direitos da personalidade fossem representados em um único direito subjetivo, ou ainda que fossem classificados múltiplos direitos da personalidade. A técnica mais apropriada seria a de, isto sim, proteger amplamente a pessoa humana em todos os seus aspectos. Destarte, pode-se afirmar que a dignidade seria o fundamento da República, configurando verdadeira cláusula geral de tutela e promoção da pessoa humana. Nesta seara, ressalta-se, ainda, o atual entendimento de que os direitos fundamentais – que visam, juridicamente, a limitar o poder estatal, proibindo a interferência no plano individual dos cidadãos e, ao mesmo tempo, exigindo uma prestação estatal efetiva para a proteção desses direitos – são autoaplicáveis no território brasileiro e, portanto, o simples fato de inexistência de legislação específica que trate do direito à proteção de dados pessoais não pode constituir óbice para que se perfectibilize a sua defesa. (RUARO; MOLINARO, 2017, p. 26).

No Brasil, portanto, a proteção de dados pessoais já teria sustentáculo na garantia constitucional da dignidade da pessoa humana, e ainda, nos próprios direitos fundamentais à intimidade, vida privada, sigilo das comunicações e à informação (RUARO; MOLINARO, 2017, p. 26).

Não obstante a possibilidade de se contemplar a proteção de dados pessoais como um direito com bases na dignidade da pessoa humana, mesmo que não expresso na Constituição Federal, vale-se destacar que, em 10 de fevereiro de 2022, em sessão solene, o Congresso Nacional protagonizou o momento de promulgação da Emenda Constitucional 115 (BRASIL, 2022), que incluiu a proteção de dados pessoais na categoria de direitos e garantias fundamentais constantes do artigo 5º da Constituição Federal. Trata-se de um marco civilizatório que culmina na materialização dos entendimentos acima demonstrados, os quais concluem que, de fato, a proteção de dados trata-se de um direito autônomo e fundamental, agora constituindo-se cláusula pétrea (RODAS, 2022).

Nas palavras do ministro do Superior Tribunal de Justiça (STJ) Ricardo Villas

Bôas Cueva:

> Trata-se de um marco civilizatório, que coloca o Brasil no mesmo patamar de proteção de direitos fundamentais que a Europa. Agora se completa a arquitetura legislativa da proteção de dados no Brasil. A positivação do direito fundamental à proteção de dados é fundamental para aprofundar a tutela da autodeterminação informativa no país, pois a LGPD tem caráter marcadamente instrumental. (RODAS, 2022, tela 2).

Anteriormente à LGPD e à promulgação da EC 115, contudo, a fim de possibilitar e regulamentar a tutela destes direitos relativos à proteção de dados, observa-se na legislação pátria, inicialmente, uma proteção fragmentada e com enfoques específicos como as previsões acerca do Código de Defesa do Consumidor, da ação de *habeas data*, - da Lei de Acesso à Informação, entre outras. Ao invés de um sistema integrado e norteado pelos princípios constitucionais, de modo a contemplar uma integral tutela através da proteção de dados pessoais, as previsões de cada segmento guiam-se pela lógica de seus próprios ramos (DONEDA, 2021, p. 45).

Para Doneda (2021, p. 45), é possível analisar alguns dos motivos pelos quais essa configuração se estruturou, visto que diante do perfil social do país, existe a priorização de outros problemas estruturais que antecedem a preocupação quanto à proteção de dados pessoais. A própria percepção da relevância de uma proteção aos dados pessoais não se desenvolve de maneira homogênea na sociedade de perfil desigual como é a brasileira, sendo que é necessária a satisfação de outros problemas básicos previamente.

Assim, para uma análise mais completa acerca do ordenamento jurídico brasileiro quanto às disposições sobre proteção de dados pessoais, é necessário não somente debruçar-se sobre a Lei n. 13.709/2018 (BRASIL, 2018), mas também sobre as demais previsões de normativas que, apesar de esparsas, cumpriram e cumprem a função de amparar diversos cenários conectados à privacidade e à proteção de dados pessoais. São elas: (i) leis estaduais anteriores à Constituição Federal (ii) ação de habeas data, (iii) o Código de Defesa do Consumidor, (iv) a Lei de Arquivos Públicos, (v) a Lei de Acesso à Informação, (vi) a Lei do Cadastro Positivo e (vi) o Marco Civil da Internet.

Primeiramente, faz-se notar que anteriormente à própria Constituição Federal, já existiam legislações estaduais, como a Lei estadual do Rio de Janeiro nº 824 de 28

de dezembro de 1984, que tratava de direitos do indivíduo frente a seus dados - como a garantia de conhecer suas informações pessoais contidas em banco de dados - e dispunha sobre o princípio da finalidade - através da proteção contra a utilização de informações pessoais para fins diversos daqueles para os quais foram obtidas - e do consentimento informado - prevendo a possibilidade de uso dos dados para fins diversos dos informados desde que houvesse consentimento expresso da parte diretamente interessada (DONEDA, 2021, p. 280).

No mesmo sentido discorre a Lei Estadual de São Paulo nº 5.702, de 5 de junho de 1987 (SÃO PAULO, 1987, Art. 12), prevendo o direito de acesso do indivíduo e o de retificação, assim como reconhecendo certa natureza sensível à algumas categorias de dados pessoais, em seu artigo 12, ao proibir a colocação de dados referentes à origens raciais, opiniões políticas, filosóficas ou religiosas, orientações sexuais e filiação sindical ou partidária.

Com a promulgação da Constituição da República Federativa do Brasil em 1988 (BRASIL, 1988), resta concebido pelo legislador brasileiro o instituto do *habeas data*, que ganha especial destaque devido a recente saída de algumas sociedades de regimes militares na década, no intuito de evitar o uso autoritário de informações pessoais (DONEDA, 2021, p. 278). Consagrado pelo art 5º inciso LXXII, e regulamentado pela Lei 9.507/97, o instrumento do *habeas data* serve para promover o conhecimento, retificação e esclarecimento sobre dado ou informação do impetrante que conste em banco de dados de caráter público, detendo, inclusive, prioridade de tramitação frente a outras ações, com exceção do *habeas corpus* e mandado de segurança (TEPEDINO; FRAZÃO; OLIVA, 2019).

O Código de Defesa do Consumidor (CDC), que marcou profundamente o ordenamento brasileiro, também dispôs acerca de direitos e garantias para o indivíduo sobre suas informações pessoais presentes em banco de dados e cadastros. Diante da busca pelo equilíbrio na desigual relação de consumidor e fornecedor, o CDC também observou o problema da utilização abusiva das informações sobre consumidores e estabeleceu limites ao uso da informação (DONEDA, 2021, p. 276).

A referida normativa, na seção VI do capítulo V em seu artigo 43[4], garante o direito de acesso e de retificação ao consumidor e estabelece prazo máximo de

[4] "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes." (BRASIL, 1990, Art. 43).

retenção dessas informações. Dessas disposições é possível extrair o princípio da qualidade dos dados, da transparência e, até mesmo, do esquecimento (TEPEDINO; FRAZÃO; OLIVA, 2019). Seu escopo, por óbvio, limitou-se às relações de consumo e não poderia adquirir força de um sistema geral de proteção e dados pessoais. Contudo, para Doneda (2021, p. 276-277), suas disposições não deixam de ser úteis como guias interpretativos para outros cenários.

A Lei de Arquivos Públicos, Lei nº 8.159, de 8 de janeiro de 1991, também buscou proteger o direito de acesso à informação do cidadão. Ainda que suas previsões sobre acesso e sigilo estejam revogadas pela Lei de Acesso à Informação, estabeleciam que arquivos sigilosos, ou seja, arquivos que poderiam violar a intimidade ou a vida privada, deveriam estar submetidos a regras específicas (TEPEDINO; FRAZÃO; OLIVA, 2019).

A Lei de Acesso à Informação, Lei nº 12.527/2011 (BRASIL, 2011a), por sua vez, colabora no panorama nacional da proteção de dados ao amparar o direito de acesso, qualidade da informação, sigilo, e, em especial, ao diversificar as categorias das informações entre ultrassecreta, secreta e reservada (TEPEDINO; FRAZÃO; OLIVA, 2019). Exige, ainda, o consentimento para divulgação das informações privadas e estipula responsabilização civil no caso de uso indevido destas informações.

A Lei de Cadastro Positivo - Lei 12.414, de 9 de junho de 2011 (BRASIL, 2011b) - tem como objetivo a formação de um banco de dados com informações de adimplemento para a formação de histórico de crédito, e sua menção deve-se aos limites estabelecidos pelo legislador quanto ao tratamento de dados que envolvem a construção deste histórico de crédito. Para Tepedino; Frazão e Oliva (2019, p. 28), “a proposta dessa lei é permitir que o mercado identifique os bons pagadores e, com isso, reduza a taxa de juros, sem descuidar, porém, da proteção dos dados pessoais”.

Algumas destas disposições são: proibição do uso excessivo de informações de adimplemento (BRASIL, 2011, Art. 3º, §3º, I); proibição do uso de informações sensíveis, isto é, aquelas relativas à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (BRASIL, 2011b, Art. 3º, §3º, II); dever de informação para com o cadastrado - como o dever de comunicação ao cadastrado em até 30 dias após abertura do cadastro (BRASIL, 2011b, Art 4º, §4º, I); e garantia de direitos ao cadastrado em relação as suas informações constantes no banco de dados - como o de cancelamento do

cadastro, o de acessar gratuitamente suas informações, o de solicitar à revisão de decisão tomada de modo exclusivamente automatizado.

Ainda, a legislação fortalece o princípio da finalidade, conforme disposição do art. 7º, ao prever de modo mais rígido as finalidades pelas quais tais informações poderão ser utilizadas, sendo três as suas hipóteses: para análise de risco de crédito, para subsidiar concessão ou extensão de crédito e para realização de venda ou transações que impliquem risco financeiro ao consulente.

O Marco Civil da Internet (MCI) - Lei nº 12.965, de 3 de abril de 2014 - busca nortear o processo de aplicação da internet e ganha, no contexto histórico, extrema relevância quanto à matéria, vez que reconhece a proteção de dados pessoais e a privacidade como um princípio do uso da internet no Brasil, apresentando enfoque nos usuários e preocupação com a tutela dos direitos fundamentais. De fato, foi através do Marco Civil da Internet que a palavra privacidade passou a constar no ordenamento brasileiro. Tal previsão, contudo, não trouxe grandes inovações frente ao fato de que a garantia à vida privada e íntima já havia sido consagrada na Constituição Federal de 1988 (MACIEL, 2019, l. 286 de 3.283-p).

O MCI estabeleceu garantias de direitos aos usuários: como o direito à exclusão definitiva dos dados mediante requerimento do usuário ou ao término da relação entre as partes, o de não fornecimento a terceiros de seus dados pessoais, incluindo registros de conexão, de acesso à aplicações de internet, o de ser informado de modo claro e acessível sobre tratamento e proteção de seus dados pessoais; e, ainda, o princípio da finalidade, pois proíbe utilização dos dados para finalidade diversas das informadas em contrato de prestação de serviços ou termos de uso de aplicações de internet (BIONI, 2019, p. 130-131).

Tais princípios e orientações podem ser observados em outras legislações ao redor do mundo na época, com destaque para a Diretiva 16/95 da União Europeia, e seriam, mais tarde, abordados na Lei Geral de Proteção de Dados Pessoais (MACIEL, 2019, l. 311 de 3.283-p).

Resta demonstrado, portanto, que a proteção de dados pessoais no Brasil não é tema novo nas legislações pátrias, mas sim objeto de preocupação há décadas; e que, ainda que fragmentadas por diferentes ramos do direito, alguns alicerces da proteção de dados pessoais, já caminharam, mesmo que a passos tímidos, para alcançar garantias e positivação no ordenamento brasileiro.

Não deixava de ser necessário, entretanto, uma lei própria e exclusiva sobre

o tema, pois, como visto, tais previsões não davam conta de formar e organizar um sistema integral de proteção de dados pessoais. Inclusive, a necessidade de uma lei específica sobre a matéria foi prevista no próprio Marco Civil da Internet, em seu art. 3º, inciso III (TEPEDINO; FRAZÃO; OLIVA, 2019, p. 28).

Com isto posto, parte-se, com maior noção acerca de como o tema está positivado nas normas brasileiras, para uma análise mais minuciosa acerca da Lei Geral de Proteção de Dados Pessoais.

2.2.2 Promulgação e principais conceitos insculpidos na Lei Geral de Proteção de Dados Pessoais

O caminho percorrido até a chegada do marco normativo da proteção de dados pessoais no Brasil regressa décadas atrás. A perspectiva de uma normativa que discipline a matéria ganha estímulo em meados de 2000, devido a participação do Brasil em negociações internas do Mercosul, que pressionavam no sentido da construção de uma norma comum aos países do bloco (BIONI, RIELLI, 2021, p. 21). Ao fim, não foi concretizada uma regulação única para os países do grupo, porém o movimento deflagrou estímulos para internalizar a questão.

É possível afirmar que a materialização desta ideia começou a dar seus passos por iniciativa da Secretaria de Assuntos Legislativos em conjunto com o Departamento de Proteção e Defesa do Consumidor, ambos do Ministério da Justiça. Em 2010, uma minuta do Anteprojeto de Lei de Proteção de Dados foi submetida à consulta pública (BIONI, RIELLI, 2021, p. 21). No intervalo de 2011 a 2015, outras legislações pertinentes ao tema foram promulgadas, como a Lei do Cadastro Positivo, a Lei de Acesso à informação, e o Marco Civil da Internet.

Neste mesmo período, houveram outras duas proposições de projeto de lei para regulação da proteção de dados pessoais: o Projeto de Lei 4060/201233, proposto pelo então Deputado Federal Milton Monti; e o Projeto de Lei 330/201334, de autoria do então senador Antônio Carlos Valadares.

Na Europa, entre 2012 e 2016 foi discutido e aprovado o Regulamento Geral de Proteção de Dados (RGPD ou, na sigla em inglês, GDPR), enquanto no Brasil, em 28 de janeiro de 2015, o Ministério da Justiça realizou uma segunda consulta pública sobre sua nova versão do Anteprojeto (BIONI, RIELLI, 2021, p. 24).

Para Bioni e Rielli (2021), ao citar o que Doneda chamou de conjunção astral, houveram quatro fatores preponderantes para aprovação da lei:

> Vividas duas “fases” de diálogo multissetorial para a construção de um texto para a LGPD, no final de 2017 ainda não havia perspectiva concreta de aprovação da lei. Foi preciso o que Doneda chama de “conjunção astral” para que isso fosse, de fato, possível. Resumidamente, essa conjuntura favorável pode ser atribuída a, pelo menos, quatro fatores de destaque, que ocorreram paralelamente no Brasil e no mundo e concorreram para a formação de um cenário fortemente propício à aprovação de uma lei geral de proteção de dados brasileira. Foram eles: **i) o escândalo Cambridge Analytica, que precipitou um debate por vezes restrito a círculos específicos para a grande mídia e o grande público; ii) a entrada em vigor, em maio de 2018, do Regulamento Geral de Proteção de Dados (RGPD) europeu, que acirrou a necessidade de maior segurança jurídica quanto ao tratamento de dados no Brasil; iii) o desejo expresso do Brasil ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável.** (grifo nosso). (BIONI; RIELLI (2021, p. 32).

Tais fatores encerraram na aprovação do projeto na Câmara, no envio do Projeto de Lei ao Senado, cujo conteúdo também restou aprovado com modificações textuais somente. Enviado à sanção presidencial, para o fim do momento de conjunção astral, alguns órgãos públicos reuniram-se para propor vetos à lei, em decorrências dos impactos que a LGPD poderia representar para seus setores. O projeto recebe a sanção presidencial com vetos, retirando do texto da lei, por exemplo, a previsão de criação de uma Autoridade Nacional de Proteção de Dados com autonomia e independência administrativa, para, mais tarde, através da Medida Provisória 869/2018, estabelecer a estrutura da autoridade para um modelo subordinado à Presidência da República (OBSERVATÓRIO, 2022).

Com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), o Brasil passa a integrar o rol dos países que possuem um sistema jurídico e institucional para regular o uso de dados pessoais, ao invés de regramentos dispersos e não necessariamente coesos. Segundo Bioni e Rielli (2021, p. 60):

> Antes disso, o Brasil contava somente com leis setoriais sobre proteção de dados. Era uma verdadeira colcha de retalhos que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava

> insegurança para que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios, bem como desestimulava formulação de políticas públicas e parcerias público-privada. Além disso, nenhuma das leis setoriais existentes haviam sido desenhadas nem eram vocacionadas para lidar com o fenômeno altamente complexo de uma economia e sociedade cada vez mais movida por dados. É a lei geral que fornecerá organicamente o conjunto completo de direitos e deveres de todos os atores desse ecossistema, conferindo segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados.

Constata-se, portanto, o papel que desempenhou a promulgação da LGPD, tanto para proteger e garantir direitos aos indivíduos titulares de suas informações pessoais, como para esclarecer as responsabilidades e limites dentro do sistema de atores que de alguma forma tratam dados pessoais, promovendo segurança jurídica para ambos os grupos.

Tendo sua discussão ocorrido em momento similar ao da discussão do Regulamento Geral de Proteção de Dados europeu, a LGPD sem dúvidas inspirou-se na normativa e importou seus principais alicerces. Todos os princípios insculpidos pela GDPR constam também da LGPD, sendo que a última ainda estabeleceu os seguintes: segurança, prevenção e não discriminação. Da mesma forma, existe consonância entre as legislações no que diz respeito aos direitos dos titulares de dados pessoais, como os de acesso, notificação, retificação e cancelamento de seus dados (BIONI; MENDES, 2021, p. 377).

A concatenação entre os ditames das duas normas é relevante, pois é devido às similaridades existentes entre ambas, que torna-se possível utilizar as orientações das autoridades de proteção de dados dos países sob a incidência da GDPR como guias interpretativos, pelo menos para os pontos poucos desenvolvidos pela Autoridade de Proteção de Dados brasileira, pela doutrina ou jurisprudência pátria (COTS; OLIVEIRA, 2018, p. 11).

Pois bem, os principais conceitos abordados pela LGPD também merecem maiores explicações e ponderações, vez que serão de fundamental papel para o desenvolvimento da presente pesquisa.

A LGPD estabelece regras para o tratamento de dados pessoais, seja este realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, buscando proteger os direitos fundamentais de privacidade, liberdade e o livre desenvolvimento da pessoa natural. O termo “proteger” por si só demonstra como o

legislador enxergou a dinâmica desigual na relação entre o titular e o responsável por tratar seus dados pessoais, na qual a vulnerabilidade evidentemente fica no polo dos titulareS (COTS; OLIVEIRA, 2018, p. 59).

A lei tem caráter principiológico, define indicadores para auferir o cumprimento dos deveres dos agentes e une-se a termos técnicos para delimitar os conceitos dos quais trata (PINHEIRO, 2020, p. 17-18). Sua estrutura divide-se em dez capítulos que determinam limites ao tratamento de dados pessoais, responsabilidades e obrigações aos agentes de tratamento, bem como direitos aos titulares dos dados pessoais.

Como seus fundamentos (BRASIL, 2018, art. 2º) a LGPD traz: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, honra e a imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Para entender os horizontes nos quais a lei é aplicável, primeiramente, vale esclarecer até onde se estende o conceito de dado pessoal, tratamento de dados pessoais, agentes de tratamento e titulares de dados.

Dado pessoal, conforme o artigo 5º, inciso I, da LGPD (BRASIL, 2018), é qualquer “informação relacionada a pessoa natural identificada ou identificável”. Portanto, a concepção de dado pessoal ultrapassa os tradicionais nomes, endereços e número de cadastro de pessoa física; e incluem toda informação que pode identificar um indivíduo, não necessariamente de modo direto ou mediante análise de apenas um dado individualmente. Uma informação que não identifica diretamente, mas que pode identificar um indivíduo de maneira indireta, é considerada dado pessoal. Alguns exemplos seriam: características físicas, número de identificação de um funcionário em uma empresa, número de *Internet Protocol* (IP).

A aplicação da LGPD não alcança, contudo, o tratamento de dados anonimizados, nos termos de seu art. 12 (BRASIL, 2018, art. 12), já que essencialmente esta categoria de dados não permite que o titular a eles vinculado seja identificado, “considerando a utilização de meios técnicos razoáveis e disponíveis na

ocasião de seu tratamento”[5] (BRASIL, 2018, art. 5º, XI). No caso dos dados anonimizados que ainda podem ter o processo de anonimização revertido com esforços razoáveis, ou utilizando exclusivamente meios próprios o tratamento é diverso (BRASIL, 2018, art. 12). Isso porque, por ainda guardarem a capacidade de serem relacionados ao titular daquela informação, continuam sob a proteção da Lei Geral de Proteção de Dados, pois os direitos fundamentais do titular, neste caso, ainda merecerão tutela e os dados deste titular ainda merecerão os devidos cuidados estabelecidos pela lei em questão.

Evidente que a diferenciação prática entre o dado anonimizado e aquele que poderá ser objeto de reversão não é tarefa simples e, nesse sentido, adquire grande valia a previsão da Lei no sentido de que poderá a Autoridade Nacional de Proteção de Dados estabelecer padrões e técnicas para anonimização de dados (COTS; OLIVEIRA, 2018, p. 142), visto que tais orientações servirão de guia para balizar melhor os limites desta seara que ainda não tem caminhos tão definidos quanto se gostariam.

Ainda, dentro do gênero “dados pessoais”, existe uma espécie que são os chamados dados sensíveis. Estes contemplam informações com potencial de gerar riscos consideráveis e expressivos frente aos direitos fundamentais do indivíduo, sendo revestidos de um regime especial, que buscou promover maior proteção, segurança e limites ao seu tratamento (MACIEL, 2019, l. 593 de 3.283). Deste modo, considera-se sensível, conforme art. 5º inciso II da LGPD:

> [...] o 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, II).

Por sua vez, o conceito de tratamento, conforme dispõe o artigo 5º, inciso X, consiste em “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação,

---

[5] “Art. 5º - Para os fins desta Lei, considera-se: XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;” (BRASIL, 2018, art. 5º, XI).

transferência, difusão ou extração” (BRASIL, 2018, Art. 5º, X), ou seja, qualquer operação realizada com o dado pessoal é considerada tratamento.

Além disso, a Lei Geral de Proteção de Dados Pessoais, visando a proteção dos direitos fundamentais dos titulares de dados pessoais, estabelece deveres e obrigações a serem observados pelos agentes de tratamento. Os agentes de tratamento são aqueles responsáveis por tratar os dados pessoais ou por, no mínimo, determinar este tratamento, e dividem-se em controladores e operadores.

É controlador, com fulcro no art. 5º, inciso VI da Lei, “toda pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018, Art. 5º, VI), e o operador, segundo art. 5º, inciso VII, é aquela “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (BRASIL, 2018, Art. 5º, VII). Portanto, o operador segue as determinações do controlador, não possuindo ampla ingerência sobre o tratamento de dados do titular, cujas finalidades e propósitos são traçadas pelo controlador. Cabe ao controlador, por sua vez, determinar os limites para o operador atuar, e tomar medidas para garantir que os dados estejam sendo tratados conforme as informações expostas ao titular.

Naturalmente, recaem para o controlador a maior parte das obrigações legais, uma vez que é ele quem possui relação direta com o titular dos dados pessoais (MACIEL, 2019, l. 1.259). E para o operador recaem obrigações acessórias decorrentes de contrato firmado com controlador ou ainda decorrente do próprio texto legal.

Conforme o art. 37 da LGPD, ambos os agentes de tratamento devem guardar registro das atividades de tratamento que realizam. O relatório de impacto à proteção de dados pessoais poderá ser requerido pela ANPD ao controlador, quando houver adoção da base legal do legítimo interesse – art. 10, §3º - ou em outra situação que a Autoridade considerar necessária - art. 38.

Por fim, o titular de dados pessoais será sempre uma pessoa física, natural. Dados de pessoas jurídicas, por exemplo, não são considerados dados pessoais, claro que se deve atentar aos casos de dados dos representantes legais de pessoas jurídicas, pois nesse caso trata-se de uma pessoa natural - o representante da pessoa jurídica (MACIEL, 2019, l. 894 de 3.283). Para os titulares de dados pessoais é garantida uma série de direitos que pode ser exercida mediante solicitação ao controlador, como o direito de, nos termos do art. 18 da LGPD: a) confirmar existência

de tratamento; b) acessar seus dados; c) corrigir dados incompletos, inexatos ou desatualizados; d) anonimizar, bloquear ou eliminar dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; e) exigir a portabilidade dos dados a outro fornecedor de serviços ou produto; f) eliminar os dados pessoais tratados com base no consentimento, exceto nas hipóteses previstas no art. 16 da lei; g) ter informações sobre com quem o controlador realizou o compartilhamento de dados pessoais; h) ter informações sobre a possibilidade de não fornecer consentimento e as consequências da negativa; i) revogar o consentimento.

Um dos requisitos para tratar dados pessoais de qualquer titular é a determinação da base legal para cada tratamento realizado. Conforme a LGPD, para qualquer tratamento de dados pessoais é necessária uma justificativa legal, quer dizer, é preciso que o tratamento encaixe-se em alguma das hipóteses permissivas previstas na legislação, as chamadas bases legais.

A exigência de uma base legal para o tratamento de dados, pode, a priori, parecer um impedimento burocrático, porém existem 10 possíveis bases legais que abrangem diferentes e amplos cenários, previstas no art. 7º da lei para amparar qualquer operação envolvendo dados pessoais (MACIEL, 2019, l. 601). Desse modo, abaixo são arroladas as hipóteses de base legal previstas na legislação:

1) Cumprimento de obrigação legal ou regulatória: está prevista no art. 7º, inciso II, e abrange os casos de tratamento de dados pessoais em função da existência de uma obrigação legal ou regulatória a ser cumprida (BRASIL, 2018, Art. 7º, II). É o caso do tratamento de dados de um funcionário em função da obrigação legal de assinatura da sua carteira de trabalho ou o caso de armazenamento de dados como o número de IP pelo período de seis meses para cumprimento de obrigação disposta no Marco Civil da Internet. Nestes exemplos, o consentimento do titular não é necessário para haver o tratamento de dados, o que, entretanto, não exclui o dever do responsável de informar ao titular as finalidades do tratamento e de prestar as demais informações exigidas perante à lei.

2) Tratamento de dados necessários à execução de políticas públicas: está prevista no art. 7º, inciso III, e concede à administração pública a permissão para tratar dados pessoais dos cidadãos. Alguns exemplos seriam: tratar dados com a finalidade de operacionalizar os benefícios do Bolsa Família ou a Política de Erradicação do trabalho infantil.

3) Tratamento para estudos realizados por órgãos de pesquisa: o inciso VI do

art. 7º prevê que deve ser garantida, sempre que possível, a anonimização de dados pessoais. Pressuposto da base legal em questão é que o responsável pelo tratamento - deve ser um órgão de pesquisa, definido no art. 5º, inciso XVIII, como:

> [...] órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. (BRASIL, 2018, Art. 5º, XVIII).

4) Tratamento de dados necessário para execução de contrato ou dos procedimentos preliminares a ele do qual seja parte o titular: previsto no art. 7º - inciso V. Inclusive, não seria lógico ou adequado requerer consentimento do titular em apartado, sendo que o mesmo tem interesse em assinar o contrato e contratar alguma espécie de serviço. Da mesma forma ocorre quando já está em andamento a execução do contrato. De qualquer modo, as demais obrigações que decorrem dos fundamentos e princípios da LGPD permanecem, evidentemente.

5) Exercício regular de direitos em processo de caráter judicial, administrativo ou arbitral: de acordo com o art 7º, inciso VI, admite-se o tratamento de dados pessoais para este fim, não sendo necessária a coleta de consentimento da parte adversa, o que seria incoerente. Dentro da hipótese ainda se encaixam as atividades como gestão, análise e utilização de dados realizadas pelo Poder Judiciário para conferir prestação jurisdicional (MACIEL, 2019, l. 726 de 3283).

6) Proteção da vida ou da incolumidade física do titular ou terceiro: disposto no inciso VII, do art. 7º, é outra hipótese em que se permite o tratamento de dados. Ora, inequívoco que em eventual conflito com o direito à privacidade, à proteção da vida do titular deverá prevalecer. Em caso de um acidente de trânsito em que é necessário ter acesso ao documento da vítima, não será necessário, outras vezes, nem mesmo possível, obter seu consentimento para tanto. A proteção da vida representa direito tão valioso que o tratamento também será possível em caso de se estar protegendo a vida de terceiro (MACIEL, 2019, l. 735-736 de 3.283).

7) Tutela da saúde: Relacionado ao direito à vida, também pode-se tratar dados para a tutela da saúde, limitando-se a arguição desta base legal, contudo, para os profissionais da área da saúde ou por entidades sanitárias - art. 7º, inciso VIII.

8) Proteção do crédito: base legal que inova em relação às previstas pela GDPR e outras legislações internacionais é a proteção do crédito, hipótese que

buscou não criar conflitos com a Lei do Cadastro Positivo e os serviços de proteção ao crédito. Portanto, não seria necessário consentimento prévio do titular para abertura de cadastro em banco de dados com informações sobre adimplemento de indivíduos e pessoas jurídicas, para realizar anotações no cadastro, para compartilhar estas informações com outros bancos de dados ou para fornecer a pontuação de crédito concluída através do exame das informações de adimplemento armazenadas (MACIEL, 2019, l. 775 de 3 283). São assegurados expressamente ao titular o direito de exclusão e o respeito ao princípio da finalidade, além de, naturalmente, todos os direitos e obrigações dos controladores previstos na LGPD (MACIEL, 2019, l. 785-786 de 3.283).

Para uma completa análise do rol de bases legais do art. 7º, é necessário analisar o consentimento e o legítimo interesse, previsto no inciso I e inciso IX do dispositivo, respectivamente. Aprofundar-se-á na análise dessas hipóteses autorizativas pois, por sua relevância e maior esfera de aplicabilidade, reclamam maior detalhamento.

O consentimento é a autorização expressa dada pelo titular ao controlador para o tratamento de seus dados pessoais (MACIEL, 2019, l. 631 de 3.283). Contudo, para ser válido ele precisa atender alguns requisitos legais, devendo sua manifestação ser: a) livre, b) informada, c) inequívoca e d) para uma finalidade determinada (BRASIL, 2018, Art. 5º, XII).

Por esse motivo, torna-se de extrema onerosidade a coleta de consentimento - base legal prevista no art. 7º, inciso I - no caso do tratamento que pode ser validado através de alguma das outras bases legais dentre o rol previsto no art. 7º (MACIEL, 2019, p. 28).

Autorizações genéricas são nulas pois não cumprem a necessidade do consentimento ser concedido para fins determinados apenas. Caixas de seleção pré marcadas também não são consideradas válidas pois enfraquecem a ideia da manifestação livre (MACIEL, 2019, l. 639 de 3.283). Ainda, pode o consentimento a qualquer tempo ser objeto de revogação, com fulcro no art. 18, inciso IX da LGPD. (BRASIL, 2018, Art. 18, IX).

Desse modo, ao requerer do titular o consentimento para realizar um tratamento de dados pessoais, o agente precisa verificar e tomar as devidas medidas para que o consentimento fornecido atenda todos os requisitos de validade, vez que cabe ao controlador o ônus da prova de que este foi obtido em conformidade com os

ditames legais, conforme art 8º, §2º. Pautando-se o tratamento de dados pessoais na base legal do consentimento, o titular adquire maior controle sobre seus dados pessoais pois decidem se estes serão ou não objeto de tratamento.

Se o consentimento, entretanto, contiver vício em alguns dos seus pressupostos, o mesmo será inválido e o tratamento realizado deverá ser considerado ilícito, conforme o que se conclui do disposto no art. 8º, §3º da Lei Geral de Proteção de Dados Pessoais (GROSSI, 2020, p. 24).

Vale-se mencionar a condenação do Google ao pagamento de 50 milhões de Euros como multa fixada pela *Commission Nationale de l'Informatique et des Libertés (CNIL)*, Autoridade de Proteção de Dados francesa. Conforme Oliveira (2019, n.p.), a CNIL ponderou que a empresa exigiu:

> - Consentimento geral para todos os serviços: não especificou quais dos diversos serviços de suas múltiplas plataformas (YouTube, PlayStore, Google Home e etc.) estariam envolvidos nas operações de coleta de dados e personalização de anúncios, fazendo com que o consentimento não fosse nem específico e nem inequívoco.
> - Deixou algumas opções de concordância com a exibição de anúncios em caixas pré-validadas;

É relevante tal decisão inclusive como guia interpretativo para aplicação da matéria no Brasil, visto, as similaridades entre o Regulamento Geral de Proteção de Dados e a Lei Geral de Proteção de Dados Pessoais. Para Grossi (2020, p. 25):

> Como as regras para um consentimento válido à luz do GDPR são muito semelhantes aos da LGPD, essa decisão da Autoridade francesa pode ser tida como paradigma apto a fornecer a compreensão do que seja um consentimento inválido/nulo segundo a legislação brasileira.

A análise de decisões como essa cumprem o papel de promover maior objetividade a concepções gerais que trazem consigo certa subjetividade, colaborando para construção doutrinária no país e para maior segurança jurídica para os agentes de tratamento, quando da adoção do consentimento como base legal.

Possivelmente a mais abrangente e subjetiva dentre as 10 bases legais, o legítimo interesse necessita de maiores orientações e definições da ANPD, para que sua aplicação seja mais clara e objetiva. Atualmente o texto legal, em seu art. 10, *caput*, incisos I e II, determina que a base legal poderá ser utilizada para finalidades legítimas, consideradas a partir de situações concretas, e deixa em aberto as

hipóteses em que poderia ser adotada, especificando dois casos, mas somente a título exemplificativo: a) apoio e promoção de atividades do controlador e b) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as suas legítimas expectativas e os direitos e liberdades fundamentais.

A especificidade relacionada a essa base legal é o chamado relatório de impacto à proteção de dados pessoais, que poderá ser solicitado pela ANPD, inclusive, quando o tratamento se fundar no legítimo interesse, com fulcro no art. 10, §3º da LGPD.

De qualquer modo, subsistem ao controlador todos os deveres e obrigações, nos termos da lei, como o cumprimento dos princípios da finalidade, necessidade, segurança e transparência. Levando em conta a maleabilidade desta base legal, para não se tornar uma espécie de carta branca servindo de justificativa para qualquer tratamento que não se encaixe nas demais bases legais, é que torna-se fundamental que o responsável pelo tratamento dos dados identifique de modo claro a finalidade, demonstre a necessidade e faça um sopesamento da “imprescindibilidade do uso desses dados em face das liberdades fundamentais e da expectativa do titular acerca da operação” (RODRIGUES; ROCHA, 2021, p. 59).

Para Leonardi (2019, p. 71), a inexistência de um rol taxativo para o instituto se justifica pelo fato de que quanto mais rígidas as restrições ao tratamento de dados pessoais, em especial na matéria do legítimo interesse, maiores os desafios para inovação, podendo incorrer na limitação da inovação no país. Assim, a abrangência deixada pela lei tem o objetivo de não esgotar ou limitar as hipóteses de aplicação da base legal, para que a cada novo cenário que o avanço da tecnologia originar, a adoção do instituto seja analisada caso a caso.

Para Bioni (2021, p. 79-80), a edição da lei deverá passar por um processo de aculturação:

> A edição de uma lei é apenas o primeiro passo na formação de uma cultura de proteção de dados pessoais no Brasil. Tomando como exemplo a edição do Código de Defesa do Consumidor na década de 90, demorou certo tempo para que o cidadão, órgãos de fiscalização e os próprios agentes econômicos fizessem a “lei pegar”. Após quase 4 (quatro) décadas, é possível dizer que a lei pegou e trouxe “civilidade” ao mercado de consumo com produtos e serviços mais seguros. As organizações que enxergaram no novo marco regulatório uma oportunidade em agregar valor e reputação aos seus produtos, até hoje colhem os frutos e usam isso no seu plano de comunicação. As organizações que vierem a estabelecer processos de governança

> de dados, investindo em capital humano e não só tecnológico, tudo isso como parte da sua missão institucional, se anteciparão e capitalizarão em cima do processo da formação de uma cultura de proteção de dados pessoais ainda a ser formada no Brasil.

Assim, apresentados brevemente alguns dos principais conceitos dispostos na LGPD, é possível avançar na análise do problema da presente pesquisa, para apresentar como a LGPD e a prática de raspagem de dados - *data scraping* - estão relacionadas, e quais, perante esta normativa, são os parâmetros para esta prática voltada aos dados pessoais disponíveis publicamente, a fim de que sejam cumpridos os ditames do sistema brasileiro da proteção de dados pessoais.

3 DADOS PESSOAIS DISPONÍVEIS PUBLICAMENTE E *DATA SCRAPING*

Como buscou-se demonstrar no primeiro capítulo da presente pesquisa, o desenvolvimento das tecnologias da informação elevou o grau de preocupação com a privacidade das informações e dados pessoais. Nesse cenário, composto pelo significativo quantitativo e disponibilidade de dados decorrente dos avanços das tecnologias de processamento, coleta e análise dos mesmos, localiza-se o fenômeno conhecido como *Big Data* (AZAMBUJA; GRANVILLE; SARMENTO, 2019).

É dentro desta perspectiva, ante a possibilidade de processamento de grandes volumes de dados, que se desenvolveram e ganharam foco algumas técnicas de processamento de dados, dentre elas: a mineração de dados e o *data scraping,* que, como será demonstrado, guardam estreita relação.

A questão que é pertinente à proteção de dados pessoais e à privacidade é a que se refere ao *data scraping* cujo objetivo é a "raspagem" de dados pessoais, e especialmente para esta pesquisa, os dados disponíveis publicamente.

3.1 CONCEITO DE *DATA SCRAPING* E SEUS IMPACTOS NA PROTEÇÃO DE DADOS PESSOAIS

A mineração de dados - *data mining* - é o processo por meio do qual dados são transformados em informações úteis e valiosas, através de técnica informática de combinação de dados e estatística. O objetivo da técnica é, através da ordenação e transformação de informações a partir de um banco de dados, a extração de inteligência significativa e padrões de conhecimento (MENDES, 2014, p. 109-110).

A estruturação de dados em informações relevantes e valiosas, partindo-se de um banco de dados, é o ponto em que a mineração de dados, que possui por si só amplo espectro de aplicação, conecta-se à prática de *data scraping*[6]*.* Para que se construa um banco de dados através do qual se realizará uma ordenação, é provável que se passe por um momento de “raspagem” de dados, isto é, de recolhimento, para o passo inicial de formação de um banco de dados.

O *data scraping* pode ser amplamente definido como uma técnica pela qual

6 “Note that there are two related terms: Web crawling and web scraping. Since our interest is in data mining, which requires extraction of data from crawled web pages, the discussion in this paper is directly related to web scraping.” (KASPA *et al.*, 2018. p. 50).

se utiliza um “agente de software” ou “bot” para coletar, analisar e organizar dados da web de maneira automatizada (LIU, 2020, p. 28), ou seja, trata-se de coleta de dados por meio de um programa de computador que extrai e realiza uma transferência de dados (HIRSCHEY, 2014, p. 897). A atividade de extrair, de forma automatizada, dados da *World Wide Web* pode também ser denominada de *web scraping* (SELLARS, 2018, p. 373). Em tal processo, o “software agent” ou “bot” imita a interação de navegação entre servidores da Web e humano, acessando os sites conforme necessário, analisando seu conteúdo, e por fim, encontrando e extraindo dados de interesse (LOURENÇO, 2013, p. 789).

O *data scraping* tem incontáveis aplicações e benefícios e pode ser utilizado para ajudar a identificar e extrair dados para análise, agregar informações de diferentes fontes, encontrar ofertas e descontos em serviços online, mapear redes inexploradas de servidores e sites, entre outros (SELLARS, 2018, p. 373-374). Dada a ampla esfera de aplicabilidade, a técnica foi adotada largamente (SELLARS, 2018, p. 373-374), tendo como objeto, inclusive, o processamento de dados pessoais, o que inclui aqueles disponíveis publicamente, em especial.

Contudo, quando o objeto do processamento tem como foco dados pessoais, surgem importantes questionamentos e preocupações quanto à esfera da privacidade dos indivíduos e proteção desses dados.

Isso porque, a depender do contexto, o *data mining*, bastante vinculada ao *data scraping*, pode expor o titular de dados a prejuízos como: (i) classificação potencialmente discriminatória, o que pode acarretar práticas que violam o princípio fundamental da igualdade; (ii) descumprimento do princípio da finalidade, pela falta de clareza da comunicação ou pela ausência de comunicação da finalidade em questão ao titular; (iii) transformação de dados pessoais em informações de caráter altamente sensível; e (iv) criação de perfis para tomada de decisões que podem afetar negativamente o titular (MENDES, 2014, p. 111).

Além dos já citados, o data scraping de dados acessíveis publicamente, em especial, também geram: (i) sentimentos de ansiedade e desconforto, ao saber que, por exemplo, fotos de mídias sociais estão sendo colhidas e analisadas; e (ii) prejuízos para o titular que pode ser vítima de chantagem, roubo de identidade, discriminação e fraude (XIAO, 2021, p. 707).

A utilização de dados disponíveis publicamente para processamento não compatível com o propósito pelo qual o dado foi disponibilizado também é um

preocupante prejuízo e risco aos direitos dos titulares de dados (XIAO, 2021, p. 707). Como exemplo, é possível citar a análise de *tweets* públicos por parte de pesquisadores da área da psicologia a fim de identificar problemas de saúde mental (REYNOLDS, 2020). Pois bem, trata-se de um tratamento secundário, cuja finalidade não tem relação com aquela que motivou a divulgação, visto que os usuários não tinham a expectativa de participarem de pesquisa sobre diagnóstico de problemas vinculados à saúde mental, mas sim de compartilhar suas ideias e pensamentos com o público (XIAO, 2021, p. 707).

Com isto posto, é possível concluir que os citados prejuízos e danos aos quais são expostos os titulares de dados através de técnicas de processamento, não se limitam a dados disponíveis publicamente ou a dados pessoais disponíveis em meio *online* somente (XIAO, 2021, p. 706). Porém, é evidente que os potenciais prejuízos são enormemente intensificados por estes dois fatores, visto que os dados pessoais disponíveis publicamente são dados de amplo acesso (MILANEZ, 2021, p. 422) e dados disponíveis em meio virtual, como procurou-se expor, são mais vulneráveis ao crescente avanço da tecnologia e ao massivo processamento que ocorre em ambiente *online*.

Por fim, o panorama atual que se construiu a partir desse intenso processamento de dados, que incluem dados pessoais disponíveis publicamente, é evidente: as informações referentes à pessoa física identificada ou identificável são submetidas a técnicas de processamento massivo cada vez mais apuradas, diante de uma exploração econômica agressiva em busca de crescimento exponencial (MILANEZ, 2021, p. 421).

Como consequência desta realidade houve o surgimento de diversos agentes que trabalham tão somente na coleta, processamento, venda e compartilhamento de dados, os denominados *data brokers*, os quais coletam informações sobre consumidores de variadas fontes online, combinando-as, a fim de predizer comportamentos e extrair inferências para propósitos de atividades de *marketing*, prevenção de fraudes, entre outros (MILANEZ, 2021, p. 422).

A questão é que, ante esse modelo e estratégia movidos a dados, torna-se bastante complexo e de alta dificuldade o monitoramento até mesmo de forma parcial dos usos e “reusos” que são empregados aos dados pessoais disponíveis publicamente (MILANEZ, 2021, p. 422). A opacidade sobre como os dados são tratados gera preocupações (CAMARA; RODRIGUES, 2019, p. 73).

Conforme Mayer-Schönberger e Cukier (2014. p. 107-109) o tratamento dos dados pessoais não pode ser vislumbrado como algo estático, pois mesmo após cumprido a finalidade primária de um tratamento, o dado segue tendo valor. Conforme Laura Schertel Mendes e Gabriel Campos Soares da Fonseca, com as tecnologias que se utilizam do Big Data, é real a possibilidade de extração de informações para fins deslocados daqueles que ensejaram a coleta desses dados, prática que inclusive pode gerar efeitos sob o próprio regime democrático (MENDES; FONSECA, 2021, p.99):

> A partir do posterior processamento, cruzamento e análise de grandes bancos de dados, pode-se gerar novas formas de valor político-econômico com o condão de impactar difusamente toda a sociedade e afetar sensivelmente o próprio regime democrático, tal como observado nos escândalos eleitorais envolvendo a Cambridge Analytica[7].

Pois bem, o tratamento posterior de dados pessoais, quer dizer, aquele que é realizado para finalidades diversas da original, inclusive através de técnicas de *data scraping,* é uma realidade que, como visto, carrega diversos potenciais prejuízos para os titulares de dados pessoais. É justamente por isso que a Lei Geral de Proteção de Dados estabelece algumas disposições a fim de impor certos parâmetros legais a estas práticas envolvendo dados pessoais disponíveis publicamente. Assim, busca-se aproximar de um equilíbrio entre uma sociedade marcada pelo *data-driven economy* e os direitos fundamentais do indivíduo, em especial a proteção de dados pessoais.

Para Doneda (2021, p. 24), trata-se de encontrar instrumentos que equilibrem a atividade de tratamento com parâmetros que possibilitem ao cidadão um efetivo controle em relação aos seus dados pessoais:

> A utilização de dados pessoais não é, em si, um problema. Na verdade, ela torna possíveis várias atividades, desde o planejamento administrativo até a ação humanitária, passando pela pesquisa de mercado e por mais um número infindável de áreas. Ocorre que a atividade do tratamento de dados pessoais requer instrumentos que a harmonize com os parâmetros de proteção da pessoa humana presentes nos direitos fundamentais e funcionalizados por

[7]Cambridge Analytica foi uma empresa privada que se utilizava de mineração e análise de dados para realizar e aprimorar comunicação estratégica para processos eleitorais. O caso polêmico envolvendo a empresa diz respeito à coleta e compartilhamento de dados pessoais dos usuários do Facebook que utilizaram um aplicativo e tiveram seus dados coletados e utilizados sem o devido consentimento. Apesar de que os dados estavam restritos ao tratamento para fins acadêmicos, eles poderiam ter sido utilizados para campanhas eleitorais como a que elegeu Donald Trump (WAKKA, 2019).

> instrumentos regulatórios que possibilitem aos cidadãos um efetivo controle em relação aos seus dados pessoais, garantindo o acesso, a veracidade, a segurança, o conhecimento da finalidade para a qual serão utilizados, entre tantas outras garantias que se fazem cada vez mais necessárias. (DONEDA, 2021, p. 24).

Em seguida, a fim de delimitar quais são estes parâmetros no âmbito da LGPD frente à técnica de *data scraping* apresentada neste tópico da pesquisa, aprofundar-se-á, primeiramente, nas categorias de dados disponíveis publicamente e seus conceitos, para estabelecer o que se enquadra na esfera de dados disponíveis publicamente e, por conseguinte, quais parâmetros deverão ser observados no que diz respeito a esta categoria de dados.

3.2 CONCEITO DE DADOS DE ACESSO PÚBLICO E DADOS TORNADOS MANIFESTAMENTE PÚBLICOS PELO TITULAR

Na cultura jurídica nacional a proteção de dados pessoais e o direito à privacidade ainda vislumbram-se quase como sinônimos. A consulta pública do anteprojeto de lei demonstrou tal aspecto ao servir de palco para debates quanto às repercussões no tratamento de dados de caráter público e de dados que expressam informações privadas (BIONI, 2019, p. 268).

Contudo, a privacidade e a proteção de dados pessoais, apesar de conectadas em suas trajetórias legislativas, guardam substanciais diferenças entre si, conforme pretendeu-se demonstrar no capítulo anterior. Tanto é assim, que o direito à proteção de dados resguarda, inclusive, informações pessoais que deixaram de ser privadas e se tornaram públicas. Portanto, uma crucial diferença entre ambos os conceitos se demonstra no fato de que, mesmo se não houver privacidade quanto à uma informação pessoal, a proteção de dados pessoais subsiste e deve ser resguardada (QUEIROZ, 2019, p. 19).

A legislação procura apartar a dicotomia entre o público e o privado, isto é, afastar a ideia de concessão de proteção à informação a depender do seu grau de confidencialidade (BIONI, 2019, p. 269). O fato do dado estar acessível publicamente ou expressar informação privada não é relevante para caracterização do mesmo como pessoal - relativos à pessoa física identificada ou identificável -, sendo que ambos

serão objeto de proteção pela Lei Geral de Proteção de Dados Pessoais. Supera-se, assim, a interpretação comum de que os dados de fontes públicas são de livre circulação e poderiam ser utilizados por qualquer agente de tratamento, para quaisquer usos e finalidades (MATTIUZZO; FAVARO, 2021, p. 408).

Considerando que as práticas de *data scraping*, em geral, afunilam-se na coleta e tratamento de dados pessoais acessíveis publicamente, o presente capítulo se destina justamente a entender o que se compreende do conceito de dados acessíveis publicamente que, conforme os §§ 3º e 4º do art. 7º, subdividem-se em duas categorias.

A fim de delinear os horizontes do problema que se busca responder é necessário realizar, inicialmente, uma diferenciação entre dados públicos e dados acessíveis publicamente. Para isso, utilizar-se-á primeiramente, com base na teoria do diálogo das fontes[8], outras legislações dispostas no ordenamento jurídico pátrio para alcançar uma delimitação mais clara destes conceitos.

O conceito de dado acessível ao público, traçado pelo art. 2º, II, do Decreto nº 8.777/2016, que institui a Política de Dados Abertos do Poder Executivo Federal, assemelha-se à ideia de dado público, ou seja, trata-se do dado gerado ou acumulado pelo Governo que não esteja sob sigilo ou restrição de acesso. De outro lado, os dados acessíveis publicamente guardam semelhança com a definição de dado aberto[9] prevista no art. 2º, III, do Decreto 8.777/2016, que é o dado estruturado em formato aberto, o qual permite o livre acesso e posterior tratamento.

Assim, enquanto o dado público tem como qualificador a natureza pública - estar sob guarda ou ter sido gerado pelo Governo - o dado acessível publicamente tem como qualificador a sua acessibilidade, devido ao ambiente de acesso público em que se encontra (TAVARES, 2022, p. 62).

Portanto, sob uma análise de coerência-sistemática do ordenamento jurídico, o dado pessoal de acesso público assemelhar-se-ia ao conceito de dado aberto, nos termos do art. 2º, inciso III, do Decreto 8777/2016, com o qualificador pessoal.

---

[8] A teoria do diálogo das fontes propõe uma abordagem que visa à intersecção e complementação das normas. Ao invés de enfocar em apenas um norma, passa-se a adotar um raciocínio de coordenação por meio do qual deve haver harmonia em um ambiente normativo plúrimo. Propõe uma influência recíproca entre as normas, ou seja, um diálogo. (AMARAL; MAIMONE, 2020)

[9] "Art. 2º Para os fins deste Decreto, entende-se por: III - dados abertos - dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte;" (BRASIL, 2016, art. 2º, III)

Delimitada essa diferenciação, em harmonia com os outros conceitos das legislações atinentes ao tema, vale se debruçar sobre as duas categorias de dados disponíveis publicamente dispostas pela LGPD. São elas: *(i) os dados de acesso público*, com previsão no art. 7º, §3º e §7º, e *(ii) os dados pessoais tornados manifestamente públicos pelo titular*, conforme art. 7º, §4º e §7º.

Suas diferenças não são meramente teóricas, já que o enquadramento entre uma ou outra categoria de dado pessoal - neste caso, dado pessoal de acesso público ou dado pessoal tornado manifestamente público pelo titular - repercute nos requisitos e exigências para o tratamento do mesmo.

Apesar do conceito de dados pessoais de acesso público não possuir previsão expressa na LGPD, é possível delimitá-lo com base em uma análise de coerência-sistemática do sistema normativo-jurídico. Não obstante, o conceito de dado pessoal público e dado pessoal de acesso público não se confundem. Isso porque é possível que um dado pessoal tenha natureza pública, sendo mantido e gerido pelo Poder Público, mas, ainda assim, não esteja acessível ao público, pois seu acesso dependerá, em certas ocasiões, de provocação para ser obtido ou estará sob sigilo.

As duas possíveis dimensões da transparência pública resumem como o dado pessoal sob manutenção ou gestão do Poder Público não necessariamente será de livre acesso. A transparência ativa trata, partindo-se do teor da Lei de Acesso à Informação, da obrigatoriedade de órgãos e entidades públicas divulgarem informações de interesse geral ou coletivo por iniciativa própria, salvo as informações sob sigilo. Já a transparência passiva determina a obrigatoriedade de prestar informações de interesse geral ou coletivo quando demandado pela sociedade (CONTROLADORIA GERAL DA UNIÃO, 2013, p. 14-17). Desse modo, em hipótese de transparência passiva, o dado pessoal que se encontra sob gestão do Poder Público, mesmo que de interesse coletivo ou geral, inicialmente não é de livre acesso, e por isso, não pode ser considerado um dado pessoal de acesso público, até que sua disponibilização tenha sido solicitada e atendida.

A categorização das informações proposta na Lei de Acesso à Informação (LAI) também interfere na acessibilidade de dados pessoais públicos. Informações pessoais que à priori eram de acesso público, ou seja, eram de livre acesso, podem ser classificadas como sigilosas em razão de sua imprescindibilidade para a

segurança da sociedade e do Estado[10]. Conforme a LAI, a depender da classificação entre reservada, secreta ou ultrassecreta da informação, esta deverá ser mantida por 5, 15 ou até 25 anos em sigilo (CONTROLADORIA GERAL DA UNIÃO, 2013, p. 31), deixando, por óbvio, de ser de livre acesso e se enquadrar como dado pessoal de acesso público.

Ainda que não se confunda com dado pessoal público[11], a definição de dado pessoal de acesso público tem alcance abrangente, abarcando quaisquer dados pessoais que tenham sido objeto de divulgação de terceiro - não o próprio titular - e que se encontrem disponíveis para o público geral, isto é, sejam de livre acesso. Assim, para enquadramento nesta categoria de dados é necessário a observância dos seguintes critérios: (i) a publicidade ampla do dado, ou seja, seu livre acesso pelo público geral, e (ii) a divulgação do dado por terceiros que não o próprio titular (TAVARES, 2022, p. 71).

A segunda categoria trata-se dos *dados pessoais tornados manifestamente públicos pelo próprio titular*. Para compreensão da abrangência deste conceito e consequentemente do alcance da hipótese de dispensa do consentimento prevista no art. 7º, §4º da Lei[12], mostra-se didática a separação e análise individual proposta por Giovana Tavares entre os dois requisitos que se encontram implícitos no vocábulo: *tornado* [..] *pelo titular* e *manifestamente público* (TAVARES, 2022, p. 74).

O primeiro elemento da definição - *tornado* [...] *pelo titular* - refere-se, por óbvio, à obrigatoriedade da divulgação ter sido realizada por iniciativa do próprio

---

10 "Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam: I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais; III - pôr em risco a vida, a segurança ou a saúde da população; IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País; V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas; VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações." (BRASIL, 2011).

11 "Entendemos por dados pessoais públicos as informações identificadas ou identificáveis que estejam em posse do Poder Público. Em relação ao acesso por terceiros, tais informações podem estar em duas situações: ou o acesso será livre ou será restrito. A restrição pode se dar por diversas razões, por exemplo, pela classificação da informação como ultrassecreta, secreta ou reservada, nos termos da Lei de Acesso à Informação (Lei 12.527/2011, doravante "LAI"), ou em razão de segredo de justiça". (SILVA; LUCCAS, 2020, p. 233).

12 "§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei." (BRASIL, 2018).

titular. Nesse sentido, em consonância com interpretação extraída da GDPR, não basta que os dados já estejam disponíveis para livre acesso do público, é necessário que o titular tenha protagonizado os atos que os tornaram públicos (INFORMATION COMISSIONER'S OFFICE)[13]. Resta traçada a diferença entre os dados de acesso público e os tornados manifestamente públicos pelo titular, sendo que ambas as categorias integram o gênero que se pode chamar de *dados disponíveis publicamente*[14].

Apesar de que sob primeira vista o primeiro elemento que compõe a definição aparente possuir acepção cristalina, faz-se necessário atentar-se para o cumprimento de algumas condições para que um dado pessoal seja considerado *tornado* manifestamente público *pelo titular.* Analisar a presença de consciência do titular sobre a decisão tomada, isto é, se no momento de divulgação havia ciência que os dados tornar-se-iam públicos é relevante para auferir se de fato houve iniciativa deliberada e intencional (MOREIRA, 2019).

Ainda, pressupõe-se que, ante a divulgação consciente e manifesta do titular dos seus dados pessoais, deva haver um desejo e expectativa de que esses dados continuem sendo tratados posteriormente[15]. Isso porque, o ato do titular de tornar manifestamente públicos seus dados pessoais está quase que inerentemente vinculado a um posterior tratamento dos mesmos. Quando, por exemplo, um titular divulga intencionalmente informações pessoais em seu perfil público, é clara sua expectativa de que esta publicação seja, no mínimo, visualizada, e dessa forma, tratada - já que o acesso por si só é considerado uma operação de tratamento pelo art. 5º, X, da LGPD (TAVARES, 2022, p. 76).

É necessário portanto (i) a ciência do titular de que seu ato tornará os dados pessoais em questão manifestamente públicos e (ii) o desejo e expectativa do titular de que estes sejam objeto de tratamento posterior (TAVARES, 2022, pp. 75-76).

---

13 "The term 'manifestly made public' is not defined by the UK GDPR. But it clearly assumes a deliberate act by the individual. It's not enough that it's already in the public domain – it must be the person concerned who took the steps that made it public." (INFORMATION COMISSIONER'S OFFICE – ICO, 2022).

14 Termo utilizado por Giovana Tavares para referenciar-se de modo amplo as duas categorias de dados pessoais previstas no art. 7º, §§ 3º e 4º, ou seja, dados pessoais de acesso público e dados tornados manifestamente públicos pelo titular.

15 "On the other hand, such data would have to be made public by the data subject, and more than that, manifestly made public, so as to indicate that they wish and expect such data to be further processed. No need to mention that all other provisions, including the principles and the Article 6, still apply, and also the personal data may be processed only if the purpose of the processing could not reasonably be fulfilled by other means". (FOITZIK, 2019).

Como visto, ambas as características estão conectadas. A segunda, por sua vez, é dependente da primeira, isto é, havendo ciência do titular, o desejo e a expectativa de tratamento posterior, em regra, a acompanharão.

O segundo elemento da definição - *manifestamente público* - também merece atenção, muito por conta da delimitação de qual seria a diferença entre o tornado público e o tornado manifestamente público. Ainda, existe mais de uma possibilidade de interpretação acerca de qual dos dois elementos aqui explorados se refere a condição *manifestamente*: se faz referência à intenção do titular de torná-lo público ou ao caráter claramente público que o dado atingiu ao ser divulgado pelo titular (MOREIRA, 2019). Para André de Oliveira Schenini Moreira, a resposta contempla “uma mistura de ambas as interpretações” (MOREIRA, 2019).

Já conforme entendimento da autoridade de proteção de dados do Reino Unido, Information Commissioner's Office (ICO), a informação pessoal estará manifestamente pública, quando, na prática, estiver acessível pelo público geral de modo irrestrito, não bastando que ela se encontre teoricamente acessível ao público (INFORMATION COMMISSIONER’S OFFICE). Assim, dados manifestamente públicos não teriam qualquer tipo de restrição de acesso (BIONI, 2019, p. 270).

Por exemplo, no caso de certidões disponibilizadas pelo Poder Judiciário para auferir a capacidade de solvência do devedor, - além de não serem tornados públicos pelo titular - não são manifestamente públicos, pois para ter acesso a estes dados pessoais é necessária uma consulta a base de dados do Poder Judiciário, ou seja, depara-se com uma espécie de filtro. Situação diversa ocorre quando o titular disponibiliza em um perfil público de uma rede social suas informações pessoais, tornando-as acessíveis a quem quer que seja. É possível concluir que, no primeiro caso, há uma espécie de restrição de acesso, pois é necessária uma consulta para chegar ao dado pessoal, já no segundo caso, o dado pessoal está acessível sem qualquer restrição, classificando-se, portanto, como *manifestamente público* (BIONI, 2019, p. 270).

Nesse sentido, reunindo os quesitos já aprofundados, para atestar se os dados pessoais foram, de fato, tornados manifestamente públicos pelo titular, é essencial analisar se: (i) quem os divulgou foi o próprio titular; (ii) o contexto no qual o dado foi tornado público permite um acesso irrestrito; e (iii) houve intenção do titular no momento da divulgação (TAVARES, 2022, p. 80). Ou seja, o dado pessoal tornado manifestamente público pelo titular é “aquele divulgado intencionalmente pelo próprio

titular de forma manifestamente pública” (TAVARES, 2022, p. 80).

De modo didático, Tavares expõe de forma visual em formato de um quadro, quais são os critérios de identificação das categorias de dados pessoais de acesso público e de dados pessoais tornados manifestamente públicos pelo titular.

Quadro 1. Critérios de identificação das categorias de dados pessoais disponíveis publicamente

Gênero	**Dado pessoal disponível publicamente**	
Espécies	Dado pessoal de acesso público	Dado pessoal tornado manifestamente público pelo titular
Quem tornou o dado acessível publicamente?	Terceiro	Titular
O dado pessoal foi tornado manifestamente público?	Não necessariamente	Sim
A divulgação pública deve ser um ato deliberado e intencional?	Sim	Sim
Os dados precisam ser acessados pelo público geral de forma irrestrita?	Não necessariamente	Sim
O que justifica a divulgação pública?	Obrigação legal de publicidade	Vontade do titular

Fonte: Tavares (2022, p. 81).

Portanto, é possível observar que o dado pessoal de acesso público e dado pessoal tornado manifestamente público pelo titular guardam importantes distinções entre si quanto (i) a quem tornou o dado pessoal público, (ii) a necessidade de ter sido tornado manifestamente público, (iii) à irrestrição de acesso e (iv) ao motivo que justifica a divulgação pública. Por conseguinte, o tratamento de cada uma destas categorias de dados pessoais, também exigem diferentes requisitos.

A LGPD, assim como a GDPR, constrói-se a partir de um modelo ex ante de proteção de dados, cujo centro reside na ideia de que nenhum dado é irrelevante em face do processamento automatizado na sociedade da informação. E por isso, que o modelo proposto pela legislação pátria aplica uma tutela jurídica dos dados pessoais a todos os setores econômicos, de modo a impor de forma homogênea algumas condições para o tratamento de dados pessoais independentemente do setor de atuação do agente de tratamento (MENDES, 2019, p. 45).

A compreensão dessas condições, que aqui serão tratadas como requisitos, é de fundamental importância para delimitar quais os parâmetros impostos pela LGPD

para o tratamento de dados pessoais disponíveis publicamente, o que inclui a prática de *data scraping* voltada a essa categoria de dados. Tais requisitos serão divididos entre gerais e específicos e, antes de partir para uma análise de quais são os requisitos específicos, é essencial apresentar os requisitos gerais que concernem o tratamento de quaisquer categorias de dados pessoais.

3.3 REQUISITOS PARA O TRATAMENTO DE DADOS DISPONÍVEIS PUBLICAMENTO

A LGPD, assim como a GDPR, constrói-se a partir de um modelo *ex ante* de proteção de dados, cujo centro reside na ideia de que nenhum dado é irrelevante em face do processamento automatizado na sociedade da informação. E por isso, que o modelo proposto pela legislação pátria aplica uma tutela jurídica dos dados pessoais a todos os setores econômicos, de modo a impor de forma homogênea algumas condições para o tratamento de dados pessoais independentemente do setor de atuação do agente de tratamento (MENDES, 2019, p. 45).

A compreensão dessas condições, que aqui serão tratadas como requisitos, é de fundamental importância para delimitar quais os parâmetros impostos pela LGPD para o tratamento de dados pessoais disponíveis publicamente, o que inclui a prática de *data scraping* voltada a essa categoria de dados. Tais requisitos serão divididos entre gerais e específicos e, antes de partir para uma análise de quais são os requisitos específicos, é essencial apresentar os requisitos gerais que concernem o tratamento de quaisquer categorias de dados pessoais.

3.3.1 Requisitos gerais para o tratamento de dados pessoais

No que diz respeito aos requisitos gerais para o tratamento de dados pessoais, Mendes (2019, p. 47) apresenta um modelo de três níveis para aplicação da Lei Geral de Proteção de Dados Pessoais, através do qual deve-se observar (i) as condições de legitimidade para o tratamento de dados pessoais; (ii) cumprimento de procedimentos para garantia da proteção dos dados pessoais - que encontram-se na Lei como direitos do titular e obrigações dos agentes de tratamento; e (iii) aplicação de sanções administrativas e civis no caso de violação aos direitos expostos nos itens anteriores.

No primeiro nível, para que o tratamento seja considerado legítimo é preciso analisar se (i) o tratamento está amparado em uma das bases legais previstas no art. 7º ou no art. 23 da LGPD e se (ii) há observância dos princípios insculpidos no art. 6º da LGPD. Ou seja, para que qualquer tratamento seja legítimo é preciso avaliar e indicar qual base legal deverá fundamentá-lo (MENDES; DONEDA, 2018, p. 472), já que dentre as características do modelo proposto pela LGPD está a exigência da determinação de uma base legal para o tratamento de dados pessoais.

A observância dos princípios dispostos no art. 6º da LGPD deve ser levada em conta neste primeiro nível. Os princípios previstos na normativa nacional e comuns a outras legislações internacionais estão entre os incisos I e VII, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade, transparência e segurança. A partir disso, a LGPD inova ao dispor sobre outros três. São os princípios da não discriminação, da prevenção e da responsabilização e prestação de contas - também referida como *accountability* (MENDES, 2019, p. 49). Ainda, cumpre destacar o papel atribuído ao princípio da boa-fé objetiva conforme sua previsão no próprio *caput* do art. 6º da Lei.

Dessa forma, somam-se dez princípios, além da boa-fé objetiva prevista no próprio caput do art. 6º. Como princípios, emanam seus ditames para toda a LGPD, servindo de elemento integrativo da norma, motivo pelo qual passa-se a apresentar a definição de cada um deles em maiores detalhes.

De início, a previsão do *caput* pela observância da boa-fé respalda a aplicação deste princípio geral do direito privado também à seara da proteção de dados. Ou seja, as partes possuem o dever de agir com base em valores éticos e morais da sociedade, como uma regra de conduta. A boa-fé objetiva permeia diversos princípios da LGPD, com especial destaque ao da transparência, da prevenção e da prestação de contas.

Adiante, o inciso I do art. 6º introduz o princípio da finalidade, que atrela o tratamento dos dados a “propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. Nota-se a preocupação do legislador em restringir a liberdade do responsável pelo tratamento de dados, de modo que este tratamento não seja operado sem embasamento em uma finalidade específica, legítima, explícita e informada ao titular. Desse modo, o princípio da finalidade gera implicações de ordem prática ao tratamento de dados, servindo como critério para “valorar a razoabilidade

da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)" (DONEDA, 2021, p. 187).

O inciso II trata do princípio da adequação, conceituada como a "compatibilidade do tratamento com as finalidades informadas ao titular de acordo com o contexto do tratamento". Pela literalidade, pode-se perceber a sua íntima relação com o princípio da finalidade. Brancher, Kujawski e Castellano (2019, p. 70) entendem que juntos "estabelecem os limites dentro dos quais os controladores podem coletar e utilizar dados pessoais, conferindo legitimidade a essas operações". A adequação tem como pressuposto a compatibilidade da coleta e do tratamento dos dados com as finalidades originalmente informadas ao titular, e no caso de dados disponíveis publicamente, como se verá em seguida, a compatibilidade é aferida em relação à finalidade que motivou a disponibilização dos dados.

O inciso III apresenta o princípio da necessidade, cujo âmago é limitar as operações envolvendo o tratamento de dados ao mínimo necessário. É dizer, a coleta e o tratamento de informações, especialmente no âmbito virtual, devem se deter naqueles elementos que são essenciais, sendo o extravagante dispensável.

A seu turno, os incisos IV e VI assentam como princípios as máximas do livre acesso e da transparência, constituídas como garantias aos titulares. De um lado, o livre acesso garante a "consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais". De outro modo, a transparência garante "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

Os incisos IX e V dispõem, respectivamente, sobre os princípios da não-discriminação e qualidade dos dados, os quais guardam estreita relação entre si em uma era em que processamento de dados é realizado em grande volume. A qualidade dos dados impõe que as informações pessoais se mantenham corretas e atualizadas durante o fluxo de dados, enquanto que a não-discriminação, apesar de não introduzir nada novo ao ordenamento jurídico, adquire papel fundamental tendo em vista o volume de decisões automatizadas realizadas por meio do uso de algoritmos atualmente (BRANCHER, KUJAWSKI, CASTELLANO, 2019, p. 76-77).

Os incisos VII e VIII abordam à segurança e à prevenção, respectivamente, os quais se preocuparam em estabelecer obrigações aos agentes de tratamento como a de implementar medidas de segurança capazes de impedir que dados pessoais

sejam comprometidos em algum momento do seu ciclo de vida (BRANCHER, KUJAWSKI, CASTELLANO, 2019, p. 80).

Por fim, o inciso X perpassa os demais princípios ao delimitar que, para se cumprir o princípio da responsabilidade ou prestação de contas, não basta apenas que os agentes de tratamento cumpram com suas obrigações, mas que consigam demonstrar que o fizeram.

No segundo nível do modelo proposto por Mendes, atenta-se à garantia dos direitos dos titulares e às obrigações impostas pela Lei aos agentes de tratamento.

Os direitos dos titulares, já introduzidos no primeiro capítulo, estão previstos no art. 18 da LGPD, e dentre eles estão o direito de acesso, de retificação, de cancelamento e de oposição. Ainda, existem outros direitos que podem ser extraídos do texto do art. 20 da LGPD, como o direito à explicação, à intervenção humana em pocesso decisório automatizado e direito à auditoria, nas hipóteses em que à decisão possa trazer riscos de discriminação para o titular (MENDES, 2019, pp. 50-51).

Entre as obrigações dos agentes de tratamento, estão (i) a indicação de encarregado de dados pelo controlador, com exceção de se enquadrar na hipótese de agente de tratamento de pequeno porte, o qual tem a obrigatoriedade de indicação do encarregado dispensada, conforme Resolução CD/ANPD Nº 2, de 27 de Janeiro de 2022 (BRASIL, 2022)[16]; (ii) adoção de medidas de segurança, técnicas e administrativas adequadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme art. 46 da LGPD; (iii) manutenção de registro das atividades de tratamento realizadas - obrigação que alcança tanto controlador como operador, com previsão no art. 37 da Lei; (iv) comunicação por parte do controlador à Autoridade Nacional de Proteção de Dados, em caso de incidente de segurança, nos termos do art. 48 da LGPD.

Os dois níveis de aplicação da LGPD servem como requisitos gerais ao tratamento de dados pessoais, visto que uma atividade de tratamento pressupõe todos os quesitos acima referidos: (i) indicação de uma base legal para o tratamento;

[16] Resolução CD/ANPD Nº 2, de 27 de Janeiro de 2022 dispõe acerca da aplicação da LGPD para os chamados agentes de tratamento de pequeno porte, conceituados pela própria Resolução como: “I - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;” (BRASIL, 2022).

(ii) respeito aos princípios previstos no art 6º da Lei; e (iii) observância dos procedimentos para garantia da proteção dos dados pessoais. Desse modo, carecendo de qualquer um destes elementos, o tratamento de dados pessoais não estará em harmonia com o que dispõe a legislação.

3.3.2 Distinções entre as hipóteses do §§ 3º, 4º e 7º do Art 7º da LGPD

Não basta, entretanto, analisar o tratamento de dados pessoais disponíveis publicamente apenas levando-se em conta os requisitos gerais. Isso porque os §§ 3º, 4º e 7º do art. 7º da LGPD estipulam regras específicas para o tratamento de dados pessoais de acesso público e tornados manifestamente públicos pelo titular. Pretende-se analisar estes requisitos para chegar-se a uma delimitação dos parâmetros legais estabelecidos pela LGPD para o tratamento de dados disponíveis publicamente.

Existem importantes distinções entre as hipóteses previstas nos §§ 3º e 4º e no § 7º no que concerne às hipóteses de tratamento de dados pessoais. A primeira diz respeito à finalidade à qual se refere o tratamento de dados em comparação com a finalidade pela qual o dado foi disponibilizado.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> [...]
>
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
>
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
>
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para **novas finalidades**, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (grifo nosso).

Conforme é possível vislumbrar pela leitura dos dispositivos, o §7º aborda a hipótese de tratamento de dados para *novas finalidades*, ou seja, finalidades diversas das que motivaram a disponibilização. Por conseguinte, conclui-se que as hipóteses dos §§ 3º e 4º só poderiam retratar o tratamento para *finalidades equivalentes*, isto é,

idênticas às que motivaram a disponibilização (TAVARES, 2022, p. 93-94), já que, do contrário, perder-se-ia o sentido da existência da previsão de tratamento para novas finalidades disposta no §7º.

Em vista disso, para a presente pesquisa, adotar-se-á classificação feita por Tavares (2022) quanto à uniformidade entre a finalidade do tratamento e a finalidade para a qual o dado tornou-se disponível publicamente; e quanto ao grau de sucessão na cadeia de tratamento (TAVARES, 2022, p. 93-94). Conforme classificação proposta pela autora, os §§ 3º e 4º tratam de hipótese de tratamento equivalente, já que a finalidade do tratamento deve ser idêntica àquela que motivou a disponibilização dos dados pessoais - sejam eles de acesso público ou tornados manifestamente públicos pelo titular -, enquanto o § 7º prevê hipótese de tratamento compatível, através do qual as finalidades do tratamento são diversas, porém ainda compatíveis à original (TAVARES, 2022, p. 93-94).

Outra distinção relaciona-se ao grau de sucessão no tratamento de dados pessoais. No caso de dados pessoais de acesso público, pressupõe-se já ter ocorrido um tratamento inicial - primário -, que é a própria disponibilização do dado por terceiro. Assim, o tratamento de dados pessoais de acesso público classifica-se como tratamento *secundário*. Já o tratamento de dados pessoais tornados manifestamente públicos pelo titular classifica-se como *primário*, pois tendo sido o próprio titular quem divulgou os dados pessoais, a coleta deste dado acessível ao público será o primeiro tratamento empregado. Por fim, o tratamento realizado para novas finalidades resta classificado como tratamento *posterior* (TAVARES, 2022, p. 93-94).

Dessa forma, unindo as classificações, o *tratamento secundário equivalente* refere-se à hipótese prevista no §3º, o *tratamento primário equivalente* à previsão do §4º e *o tratamento posterior compatível* à hipótese do § 7º.

Com isto posto, torna-se factível endereçar o objeto da presente pesquisa, que busca estabelecer com maior clareza quais os critérios para o tratamento realizado através de técnicas de *data scraping* de dados pessoais disponíveis publicamente e avançar na análise dos requisitos específicos impostos pela LGPD para tratamento desta categoria de dados pessoais.

3.3.3 Requisitos específicos para o tratamento de dados pessoais de acesso público (§3º do art 7º da LGPD)

O §3º do art 7º[17] da LGPD dispõe expressamente que o tratamento de dados pessoais de acesso público deve considerar a boa-fé, a finalidade e o interesse público que justificaram sua disponibilização.

A boa-fé possui duas acepções no ordenamento jurídico pátrio. A boa-fé subjetiva pode ser referenciada como sinônimo de boa intenção, sendo o contrário de má-fé. Enquanto que a objetiva determina um padrão de comportamento leal e correto, fundamentado na lisura e probidade. Ao mencionar no caput do art. 6º o princípio da boa-fé, deve-se entendê-lo no seu aspecto objetivo, vez que o subjetivo já é exigência de todo o ordenamento jurídico, o qual veda o agir de má-fé (FLUMIGNAN; FLUMIGNAN, 2020, l. 2352).

Trata-se de uma cláusula geral que contém um princípio, e este é o motivo pelo qual está inserida em destaque no caput do artigo. Assim, ao tempo que é cláusula geral e também princípio, tem função integradora e de garantia de coesão na interpretação e aplicação da Lei (MARTINS, 2020, p. 115).

Em resumo, a boa-fé objetiva, sob a ótica da LGPD, determina que o tratamento de dados pessoais deve estar pautado na ética e em padrões objetivos de lealdade possíveis de serem aferidos contextualmente (MENDES, 2019, p. 49). Por isso, sua ligação com as legítimas expectativas do titular, já que o tratamento pautado em lealdade, honestidade, e probidade - pautado na boa-fé objetiva - perpassa a observância destas expectativas legítimas.

Para Bioni (2019), a boa-fé, juntamente com a confiança, são os elementos que compõem a concepção da legítima expectativa do titular. Isso porque, para que sejam observados os princípios da boa-fé e da confiança no tratamento de dados pessoais, é essencial obedecer a legítima expectativa do titular de que seus dados pessoais sejam tratados de acordo com o propósito pelo qual foram disponibilizados ou de que sejam tratados de acordo com o contexto de uma relação preestabelecida (BIONI, 2019, p. 247). Desse modo, observar-se-á a boa-fé quando o tratamento não desvirtuar as legítimas expectativas dos seus titulares (LIMA, 2019, p. 187).

[17] "§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização." (BRASIL, 2018)

No esforço empregado para realização desta aferição do que constitui a legítima expectativa do titular que a privacidade contextual adquire um papel essencial. Para determinar se o fluxo informacional é apropriado ou inapropriado, deve-se ter em conta o contexto no qual os dados se inserem (NISSENBAUM, 2010, p. 182). Conforme elucida Bioni (2019, p. 242):

> A teoria da privacidade contextual estrutura-se sob a premissa de que o fluxo informacional deve ser apropriado de acordo com as suas respectivas esferas sociais. Por meio dessa análise contextual o titular dos dados pessoais detém legítimas expectativas de como eles fluirão, o que determina, então, a sua integridade. Falar em legítimas expectativas de privacidade nos reconduz em considerar quais são os desígnios do titular dos dados, mesmo que não sob uma perspectiva subjetiva de cada indivíduo, mas sob uma faceta objetiva pertinente a um padrão social. (grifo nosso).

Portanto, o tratamento equivalente de dados de acesso público está limitado a uma regra de conduta que impõe um padrão de comportamento leal e honesto, que se concretiza com a observância dos interesses legítimos e expectativas razoáveis do titular, os quais podem ser aferidos por meio de uma análise contextual (TAVARES, 2022, p. 102):

> A licitude do tratamento equivalente de dados de acesso público passa a ser também contextual. Ela não é delimitada por um propósito único e inflexível, mas orientada por uma gama de expectativas no contexto de uma relação específica. Exatamente por isso, a privacidade contextual mostra-se tão útil, na medida em que ela consegue ser elástica o suficiente para possibilitar novos usos compatíveis dos dados pessoais de acesso público que não poderiam ser previamente especificados de forma exaustiva no texto da LGPD [...]. (TAVARES, 2022, p. 107).

O princípio da *finalidade*[18], definido no art 6º, inciso I, da LGPD, de modo geral, impõe coerência entre o tratamento de dados empregado e a finalidade informada ao titular (TEPEDINO; FRAZÃO; OLIVA, 2019). A Lei exige que o tratamento seja realizado para propósitos *legítimos*, *específicos*, *explícitos* e *informados ao titular*, sem possibilidade de tratamento posterior incompatível com essas finalidades.

Dessa forma, para que atenda um propósito específico e explícito, deve o agente de tratamento estabelecer de modo expresso e limitado quais as finalidades

[18] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;" (BRASIL, 2018)

do tratamento de dados, sob pena de constituir-se ilegítimo, no caso da indicação de finalidade amplas ou genéricas (MENDES, 2011). Para Doneda (2021, p. 187), trata-se de princípio essencial, pois através dele é possível estruturar um critério para valorar a razoabilidade da utilização de dados pessoais para determinada finalidade.

A especificidade da finalidade prevista no §3º do art. 7º é exigência da observância da finalidade para a qual o dado foi disponibilizado publicamente. Dessa forma, para que o tratamento se enquadre na hipótese do §3º, não basta apenas o tratamento seguir propósitos legítimos, específicos e explícitos, é necessário que ele seja *equivalente* ao propósito por trás de sua disponibilização.

Neste contexto do tratamento de dados pessoais de acesso público surge um importante questionamento: como pode o titular ser informado sobre um tratamento classificado como secundário, que se caracteriza pela inexistência de relação direta entre o titular e o agente de tratamento que emprega tal tratamento? (TAVARES, 2022, p. 114). Para Tavares (2022), como a finalidade do tratamento foi em um primeiro momento já explicada ao titular pelo primeiro agente de tratamento na cadeia, isto é, pelo terceiro que disponibilizou o dado publicamente, pode se concluir que a finalidade é subentendida. Isso somente se considerarmos que trata-se de fato de hipótese de enquadramento do §3º, ou seja, que trata-se de tratamento com propósito idêntico ao que justificou a disponibilização (TAVARES, 2022, p. 114).

Assim, tratando-se de uso secundário previsto no §3º do art. 7º da LGPD, não parece existir obrigatoriedade em prestar informação ao titular a respeito da finalidade, por parte do novo agente de tratamento, pois pode-se presumir que o titular já foi avisado a respeito da finalidade do tratamento em momento anterior (TAVARES, 2022, p. 116).

Havendo clara identidade entre a finalidade original e a que se pretende alcançar em um segundo momento, há um tratamento equivalente, e mantém-se o controle do titular de dados, pois os dados estão sendo tratados de modo previsível, de acordo com suas legítimas expectativas (BIONI, 2019, p. 273). Para Tavares (2022, p. 115):

> Ainda que o indivíduo não saiba mais quem está tratando o seu dado, ele terá a segurança, confiança e legítima expectativa de que o tratamento está sendo realizado para a finalidade que justificou a sua disponibilização, permitindo, assim, a manutenção de um controle por parte do titular, ainda que indireto. (TAVARES, 2022, p. 115).

Ainda que o princípio da finalidade demonstre estreita relação com o princípio da boa-fé, visto que ambos cumprem um papel de limitar o tratamento de dados, bem como de atender expectativas legítimas e razoáveis dos titulares, o primeiro, no caso da hipótese de tratamento prevista no §3º, impõe que a finalidade do tratamento que se quer operar deve ser idêntica àquela que justificou sua disponibilização (TAVARES, 2022, p. 121).

O *interesse público* é o terceiro requisito específico para a hipótese de tratamento equivalente de dados de acesso público. Pode ser definido como "o interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da Sociedade e pelo simples fato de o serem" (MELLO, 2005, p. 62). Não se confunde, portanto, com o interesse do próprio Estado (GLASSMAN, 2020, p. 898), já que representa a dimensão pública dos interesses individuais dos administrados (MELLO, 2005, p. 60).

É um conceito variável, que carrega certa indefinição pois detém variadas possibilidades de materialização, podendo se traduzir em segurança pública, saneamento básico, entre outros (COTS; OLIVEIRA. 2018, p. 177). Assim, ao realizar a análise do interesse público que justificou a disponibilização dos dados pessoais deve-se restringir qual o interesse público envolvido no tratamento dos dados pessoais, e não o utilizar de modo genérico ou indeterminado.

Apesar de ser um conceito permeado de desafios quanto a sua delimitação (BRANCO, 2020, p. 26), compreender o interesse público em harmonia com a proteção e o atendimento a direitos fundamentais é uma chave considerando que o interesse público não é uníssono em uma sociedade plural, podendo existir vários interesses públicos, inclusive, conflitantes (JUSTEN FILHO, 1999, p. 115-136; AMARAL, 2001, p. 35-38).

Com base nesta perspectiva de interesse público, como conceito que não se legitima pela coletivização abstrata, mas que tem fundamento na proteção aos direitos fundamentais, transcendentes aos interesses particulares dos próprios titulares, chega-se à conclusão que aqueles dados pessoais indispensáveis ao atendimento da transparência pública são passíveis de publicização, enquanto deve-se afastar do conhecimento público os demais (MATOS; RUZYK, 2020, p. 206).

Quanto ao tratamento de dados de acesso público, o interesse público que justificou a disponibilização dos dados pessoais perpassa o direito de acesso à informação, previsto no inciso XXXIII do artigo 5º da Constituição Federal, e deve ser

compreendido, no âmbito da proteção de dados, como aquilo que é necessário para o controle social da transparência pública (MATOS; RUZYK, 2020, p. 208).

Logo, a partir do exposto, é evidente a relação de interdependência entre os três requisitos específicos que balizam o tratamento equivalente de dados de acesso público. O princípio da boa-fé impõe padrão de conduta que leve em conta as legítimas e razoáveis expectativas do titular, as quais podem ser aferidas a partir da finalidade pela qual o dado foi disponibilizado, que está intimamente ligada ao interesse público vinculado ao dever de publicização do dado. Ou seja, o motivo pelo qual o dado se tornou acessível publicamente no primeiro momento - *interesse público* - delimita qual o objetivo - *finalidade* - da disponibilização pública do dado pessoal, que, por sua vez, serve para aferir as legítimas expectativas do titular e cumprir os padrões objetivos de lealdade quanto ao tratamento - *boa-fé* (TAVARES, 2020, p. 128).

3.3.4 Requisitos específicos para o tratamento equivalente de dados tornados manifestamente públicos pelo titular

As redes sociais serviram e servem ao papel fundamental de diminuir os limites impostos pelas barreiras físicas e geográficas ao redor do mundo. É através delas que os indivíduos desenvolvem ou sustentam laços de amizade, familiares, profissionais e comerciais, conectam-se com pessoas novas e mantêm-se informados sobre acontecimentos dos mais variados gêneros (TAVARES, 2022, p. 129).

Aspecto relevante sobre este contexto é a situação paradoxal que se cria em relação à privacidade. Ao tempo que os usuários buscam uma maior proteção à privacidade, expõem cada vez mais suas vidas a incontáveis pessoas através das redes sociais, o que inclui informações pessoais. No *LinkedIn, Facebook, Tinder*, diferentes dados pessoais poderão ser tratados para realização de cadastro do usuário, para encontrar o “par ideal” ou para criação de conexões com pessoas que compartilham de interesses similares (TAVARES, 2022, p. 130-131).

Por isso, pode-se afirmar que o fenômeno das redes sociais é talvez um dos mais relevantes cenários em que o titular tem a possibilidade de tornar seus dados pessoais manifestamente públicos.

A questão é que as redes sociais não escapam das normativas em relação à proteção de dados pessoais, e o espaço de confiança e privacidade do titular deve

prevalecer nestes cenários (TAVARES, 2022, p. 130). Quer dizer, mesmo os dados tornados manifestamente públicos pelo titular merecem tutela jurídica e limitação quanto à sua utilização, porque, como já exposto, o direito à proteção de dados supera a dicotomia entre público e privado, protegendo indistintamente tanto aquelas informações que permanecem sob esfera privada, como aquelas que estão acessíveis ao público.

A LGPD disciplina o tema em seu art. 7º, §4º, abordando o tratamento de dados tornados manifestamente públicos pelo titular e estabelecendo alguns requisitos para tanto. Ainda, acerca dos possíveis cenários de tratamento de dados tornados manifestamente públicos pelo titular, existe a previsão do §7º do art. 7º[19]. Contudo, esta hipótese se diferencia do que está prescrito no §4º, pois se refere ao tratamento para *novas* finalidades e tece, ainda, outros requisitos que não estão presentes no §4º [20].

A exigência de se resguardar os direitos do titular e os princípios previstos na Lei está entre os requisitos explícitos delineados no §4º. Demonstra-se, portanto, que não é porque o dado foi tornado manifestamente público pelo titular que se renuncia aos direitos que lhe são garantidos pela legislação. Assim, trata-se de previsão legal que expressamente esclarece que a hipótese não é uma carta branca (MATTIUZO, FAVARO, 2022, p. 408-409). Tal exigência também está prevista no §6º do art. 7º[21], e, logo, mesmo não havendo essa especificação no §4º, a obrigação se manteria para os agentes de tratamento de igual forma.

Considerando que os direitos dos titulares já foram tratados no primeiro capítulo desta pesquisa, ao explicar alguns dos conceitos básicos para desenvolvimento da pesquisa, e que os princípios insculpidos no art. 6º da LGPD também já foram apresentados neste capítulo dentro da esfera dos requisitos gerais para o tratamento, analisar-se-ão os aspectos que dizem respeito ao cenário mais específico do tratamento equivalente de dados tornados manifestamente públicos pelo

---

19 "§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei." (BRASIL, 2018, § 7º).

20 "§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei." (BRASIL, 2018, § 4º)

21 "§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular." (BRASIL, 2018, §6º)

titular.

Considerando, inclusive, a observância exigida dos agentes de tratamento aos princípios insculpidos na Lei, a exemplo do princípio da finalidade e boa-fé, devem-se tecer considerações semelhantes aquelas que se referem ao tratamento de dados de acesso público. Desse modo, é necessário preservar a compatibilidade entre o uso e as circunstâncias pelas quais a informação foi tornada pública (TEPEDINO; TEFFÈ, 2020, p. 100), quer dizer, entre o motivo que levou o titular a compartilhar aqueles dados na rede e o posterior uso que poderá ser feito por terceiros. Mais uma vez, a análise contextual adquire papel valioso para aferir a legitimidade do tratamento (TEPEDINO; TEFFÈ, 2020, p. 100).

Aqui, adquire importância o questionamento de como se poderia conferir a finalidade vinculada ao ato do titular de tornar manifestamente público seus dados pessoais, considerando não ser costumeiro que se defina esse propósito no ato de publicização. Assim, torna-se necessária uma análise interpretativa do agente de tratamento para delinear a razoabilidade da utilização dos dados pessoais, partindo-se da subentendida finalidade, aferida contextualmente (TAVARES, 2020, p. 145-146).

Tavares (2022) exemplifica, de modo prático, quais seriam as finalidades gerais possíveis de se extrair de algumas redes sociais. No caso do *LinkedIn*, a finalidade da plataforma relaciona-se a criação e ao fortalecimento de relações profissionais, logo, os dados tornados manifestamente públicos pelo titular na rede social poderiam ser utilizados - de modo equivalente - para uma oferta de emprego ou oportunidade de estudo. Já no *Facebook*, a finalidade é mais genérica, a rede social tem como propósito estimular relações sociais e auxiliar o usuário no fortalecimento de contatos, e, considerando o contexto de disponibilização, portanto, não seria razoável o tratamento para fins de cobrança de dívida, por exemplo (TAVARES, 2022, p. 146-147).

Para Bioni (2019), terceiros, a princípio, não poderiam utilizar dados de uma rede social, ainda que de perfil público, para propósitos de *marketing.* Todavia, no caso de uma rede profissional como a do *LinkedIn*, o tratamento de dados por terceiros - como *headhunters* - para conectar usuários com vagas profissionais seria compatível. Para o autor, esse uso é compatível com o propósito da plataforma em si, mas principalmente com a razão pela qual os dados são publicizados (BIONI, 2019, p. 271).

Havendo a observância destes critérios, consta no §4º que a coleta de consentimento é dispensada. Para alguns autores a dispensa do consentimento se refere ao consentimento manifestado expressamente, de modo que a Lei presume haver uma espécie de consentimento implícito no ato de publicar os próprios dados, sendo esta uma autorização para seu tratamento (MARCACINI, 2020). Também é chamado de consentimento contextual, pois, sendo respeitado o contexto de publicização do dado, de modo a ser tratado conforme as legítimas expectativas do titular, o indivíduo continua a exercer controle sobre seus dados, mesmo que não declare sua vontade (BIONI, 2019, p. 273).

Com isto posto, é possível concluir que a equivalência no tratamento de dados tornados manifestamente públicos pelo titular impõe uma (i) análise contextual (TAVARES, 2022, p. 150), a qual passa pela observância, em especial, dos princípios da finalidade e da boa-fé, similar à hipótese do §3º, além do cumprimento de requisitos gerais como (ii) a observância, como um todo, dos princípios da LGPD e a (iii) garantia dos direitos dos titulares.

3.3.5 Requisitos específicos para tratamento posterior de dados disponíveis publicamente (art. 7º, § 7º)

Conforme § 7º, do art. 7° da LGDP, os requisitos necessários para o tratamento posterior de dados disponíveis publicamente - aqui compreendidos tanto como os dados de acesso público, quanto os dados tornados manifestamente públicos pelo titular abarcam a observância de: (i) propósitos legítimos e específicos (ii) fundamentos previstos na LGPD (iii) princípios estabelecidos pela Lei e (iv) preservação dos direitos dos titulares[22].

Considerando que os últimos requisitos, ainda que destacados no § 7º, são critérios a serem levados em conta em qualquer tratamento, analisar-se-á, neste subcapítulo, os requisitos específicos a respeito da nova finalidade do tratamento posterior, isto é, a necessidade de realização do tratamento posterior para propósitos

[22] "§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei." (BRASIL, 2018).

específicos, legítimos e, como será visto em seguida, compatíveis com a finalidade da publicização do dado.

Assim como já determinado pelo art. 6º, I, da LGPD, que preconiza o princípio da finalidade, a hipótese do §7º não constitui exceção, vez que exige-se que o tratamento respeite propósitos legítimos e específicos. A *especificação* dos propósitos estabelece limites às finalidades para as quais os controladores podem utilizar os dados pessoais coletados (ARTICLE 29 WORKING PLACE, 2013, p. 15).

Na *Opinion 03/2013*, o *Article 29 Working Party* estabelece que a finalidade deve ser clara e especificamente identificada a ponto de ser tornar possível a determinação de quais tipos de tratamentos estarão ou não incluídos na esfera de alcance deste propósito. Assim, finalidades genéricas ou vagas como “melhoria da experiência do usuário” ou “propósitos de marketing” provavelmente não atenderão ao requisito de serem específicas[23].

Deve também a finalidade ser *legítima*, o que significa, que o propósito do tratamento deve estar de acordo e em harmonia com a lei de modo geral, ou seja, com as demais legislações, federais estaduais ou municipais, princípios constitucionais, direitos fundamentais, etc. (ARTICLE 29 WORKING PARTY, 2013, p. 20). No caso, mais do que analisar os requisitos impostos pela LGPD, é necessário debruçar-se sobre outras legislações que podem dizer respeito ao tratamento a ser empregado, como o Marco Civil da Internet, Código de Defesa do Consumidor, entre outras.

Ainda que não esteja expressamente determinado no § 7º, é necessário traçar um outro requisito para a hipótese em análise. A finalidade, além de legítima e específica, precisa ser *compatível* com o propósito que justificou a publicização do dado em um primeiro momento, tendo em vista que, através de leitura sistemática da LGPD, a hipótese do § 7º continua condicionada aos princípios gerais da lei, com destaque ao da finalidade, que, por sua vez, proíbe tratamento posterior incompatível (TAVARES, 2022, p. 197). Logo, se a nova finalidade não dispuser de compatibilidade

---

[23] “The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being ‘specific’. That said, the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved. In some clear cases, simple language will be sufficient to provide appropriate specification, while in other cases more detail may be required.” (ARTICLE 29 WORKING PARTY, 2013, p. 15.)

com a que motivou a publicização do dado, o tratamento será contrário ao que é preconizado pelo princípio da finalidade, no art 6º, inciso I da LGPD.

De qualquer modo, é relevante destacar que o princípio da finalidade e da adequação não impõe uma completa vedação para reutilização dos dados, e que, para o caso de tratamento de dados disponíveis publicamente, há uma restrição ao tratamento para novas finalidades apenas se estas forem incompatíveis com a finalidade original (WIMMER, 2021, p. 294). Tanto é assim que ao prever, no art. 6º, I, que o princípio da finalidade se materializa pela "realização do tratamento [...] *sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*" o dispositivo legal admite implicitamente o tratamento posterior, desde que compatível.

A finalidade e a adequação, para Brancher; Kujawski e Castellano (2019, p. 70-71):

> [...] existem justamente para oferecer uma abordagem balanceada, reconciliando a previsibilidade e a segurança jurídica indispensáveis em operações de tratamento e a necessidade pragmática de se estabelecer um certo grau de flexibilidade.

Apesar de alguns autores (COTS; OLIVEIRA, 2018, p. 78) entenderem que a previsão de tratamento posterior de dados disponíveis publicamente para novas finalidades, estabelecida no § 7º, contraria o princípio da finalidade, a posição que se adota na presente pesquisa é no sentido de que não necessariamente haverá incompatibilidade quando do tratamento de dados disponíveis publicamente para novas finalidades[24], não sendo uma associação automática (BRANCHER; KUJAWSKI; CASTELLANO, 2019, p. 71; TAVARES, 2022, p. 199; ARTICLE 29 DATA PROTECTION WORKING PARTY, 2013, p. 21).

Inclusive, no Regulamento Geral de Proteção de Dados da União Europeia - através do art. 5º, par. 1, alínea "b" em associação com o art. 6.9, par. 4 - é possível inferir esta particularidade: que outra finalidade não exige nova justificativa e o tratamento para nova finalidade ainda continua coberto pela justificativa do tratamento original, desde que seja compatível com o propósito original (DÖHMANN, 2021, p. 122).

---

[24] Nesse sentido: "Rather than imposing a requirement of compatibility, the legislator chose a double negation: it prohibited incompatibility. By providing that any further processing is authorised as long as it is not incompatible (and if the requirements of lawfulness are simultaneously also fulfilled), it would appear that the legislators intended to give some flexibility with regard to further use. Such further use may fit closely with the initial purpose or be different. The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis, as will be shown below" (ARTICLE 29 WORKING PARTY, 2013, p. 21).

Aqui, a análise contextual também cumpre papel essencial, sendo que cada caso precisa ser analisado em suas particularidades. Os critérios para *avaliação da compatibilidade* são levantados pela própria GDPR no art. 6[25] (4) e já abordados pela doutrina pátria (BRANCHER; KUJAWSKI; CASTELLANO, 2019, p. 71). São eles: (i) a relação entre a finalidade original e a finalidade do novo processamento; (ii) o contexto em que os dados pessoais foram coletados e as expectativas razoáveis dos titulares com relação ao seu uso posterior; (iii) a natureza dos dados pessoais e as consequências do processamento posterior nos titulares; e (iv) as garantias adotadas pelo controlador a fim de assegurar o processamento adequado e prevenir qualquer impacto indevido nos titulares (BRACHER; KUJAWSKI; CASTELLANO, 2019, p. 70-71).

O primeiro critério, já abordado anteriormente, diz respeito a correspondência entre a finalidade inicial e a finalidade do tratamento posterior, no que tange a análise substancial entre estas finalidades. Pode-se constatar durante a avaliação de compatibilidade que o propósito para tratamento posterior já estava mais ou menos implícito das finalidades iniciais ou que se trata de um próximo passo no processamento guiado pela finalidade original. A questão é quanto maior a distância entre o propósito inicial e o do tratamento posterior, mais problemático para a avaliação de compatibilidade (ARTICLE 29 WORKING PARTY, 2013, p. 23-24).

Quanto ao segundo critério deve-se levar em conta as legítimas expectativas do titular, o que guarda estreito vínculo, conforme já apresentado, com a análise do contexto de coleta ou, neste caso, de publicização do dado. Trata-se aqui de avaliar o que razoavelmente um titular de dados poderia esperar do uso dos seus dados baseado no contexto. Quanto mais específico e restritivo for o contexto de publicização, maiores as limitações para tratamento dos dados posteriormente (ARTICLE 29 WORKING PARTY, 2013, p. 24).

---

25 "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation." (EUROPEAN PUBLIC SERVICE UNION, 2018).

O terceiro critério observa um dos principais objetivos das legislações acerca da proteção de dados pessoais, isto é, a proteção dos indivíduos frente aos impactos de usos inapropriados ou excessivos de dados pessoais. Nesse sentido, a categoria dos dados pessoais tratados têm um papel importante em determinar estes impactos, por isso a importância de analisar se haverá tratamento de algum tipo de dado sensível, conforme art. 5º, inciso II - 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 (ARTICLE 29 WORKING PARTY, 2013, p. 25).

Por fim, o quarto critério busca atender uma consequência inerente da avaliação de compatibilidade. Frente a deficiências em determinados pontos, pode-se, em certos casos, haver compensações através do melhoramento no desempenho em outros aspectos. Por exemplo, (i) fornecer informações adicionais aos titulares; (ii) permitir *opt-in* ou *opt-out* frente a uma mudança de finalidade no tratamento; (iii) coletar consentimento específico para o novo tratamento, entre outros (ARTICLE 29 WORKING PARTY, 2013, p. 26-27).

A avaliação de compatibilidade, em vista do que foi apresentado, mostra-se complexa e essencialmente contextual (TAVARES, 2022, p. 204). Para aferição desta compatibilidade tão fundamental para o tratamento posterior de dados disponíveis publicamente, a proposta de avaliação de compatibilidade mostra-se de grande relevância, principalmente considerando as similaridades entre o RGPD e a LGPD.

Para que seja exemplificado como pode ser aferida esta compatibilidade, segue exemplo delimitado por Giovana Milanez Tavares, a partir de casos inspirados nos exemplos do Anexo 4, parte integrante do Parecer 03/2013 sobre a limitação de finalidade, elaborado pelo Grupo de Trabalho Article 29 Working Party (TAVARES, 2022, p. 205-207):

> Imagine que um fabricante de automóveis identifica um defeito significativo em uma série de carros que pode causar graves acidentes nas rodovias se não for reparado. O fabricante, então, ao abrigo da legislação nacional, é obrigado a informar os clientes por todos os meios razoáveis acerca do mau funcionamento dos veículos adquiridos e chamar todos os automóveis comprados desta série especificamente (recall) para sanar tais defeitos, sob pena de ser responsabilizado por qualquer prejuízo aos adquirentes dos automóveis.
>
> Imagine-se, também, que a legislação nacional não fornece maiores detalhes sobre como exatamente os proprietários dos automóveis devem ser notificados, mas foi adotada uma prática costumeira em

> que, mediante solicitação, os cartórios fornecem uma lista atualizada de todos os proprietários de automóveis em questão para o fabricante.
>
> De acordo com esta prática, apesar de os dados serem de acesso público, a transferência é documentada em um contrato padrão desenvolvido pelos cartórios que prevê condições estritas sobre o uso dos dados. O contrato, entre outras coisas, proíbe o uso dos dados para fins adicionais (como marketing). Outras salvaguardas também são previstas, como medidas técnicas e organizacionais para proteger a segurança dos dados pessoais.
>
> Em primeiro lugar, há que se destacar que as informações atualizadas dos veículos nos cartórios provavelmente serão uma fonte muito mais confiável para confirmação da titularidade dos automóveis do que quaisquer outros dados de vendas que possam ser mantidos pelo fabricante. Portanto, é do interesse direto dos próprios titulares dos dados (bem como do público em geral) que os atuais proprietários dos veículos sejam identificados pelos meios mais confiáveis existentes e da forma mais rápida possível, a fim de minimizar o risco de eventuais acidentes. Este já é um indicador forte e óbvio de compatibilidade.
>
> Somado a isso, embora a legislação possa não ser suficientemente específica sobre a possibilidade do uso de informações do registro público de veículos em cartórios, é possível verificar que o uso de tais dados de acesso público para esta finalidade pode ser esperado até certo ponto, ou pelo menos não parece ser inapropriado ou questionável. Este fator também indica o possível resultado positivo da avaliação de compatibilidade.
>
> Com base nessas considerações, o tratamento posterior dos dados pessoais constantes no registro público de veículos para a finalidade de recall é provavelmente considerado compatível. Isso porque a nova finalidade parece estar relacionada à original e, inclusive, pudesse talvez até ser razoavelmente esperada dela. Somado a isso, o tratamento ocorre no claro interesse dos titulares dos dados (portanto, com um impacto positivo sobre eles). Ainda, a natureza dos dados (ou seja, quem possui um carro específico) não é excessivamente sensível (embora não seja trivial), o que também confirma a análise.
>
> Contudo, por óbvio, podem surgir algumas dúvidas em virtude do elemento adicional da transferência de dados para um terceiro (fabricante de automóveis). A transferência pode apresentar alguns riscos, embora provavelmente sejam relativamente limitados. Em particular, o fabricante pode usar indevidamente os dados para fins adicionais (como marketing direto) ou pode simplesmente não adotar medidas técnicas e organizacionais suficientes para garantir a segurança das informações. Por este motivo, as salvaguardas contratuais mencionadas anteriormente desempenham um papel decisivo.

Dessa forma, apesar de os dados pessoais constantes no registro público de veículos ter como finalidade precípua garantir segurança jurídica às operações de compra e venda de automóveis, a partir da identificação da real titularidade do bem e de possíveis ônus gravados nele, parece razoável considerar que uma nova finalidade

de tratamento posterior desses mesmos dados pessoais para fins de recall é provavelmente compatível.

Portanto, a exigência de propósitos específicos, legítimos e compatíveis é necessária para que se garanta a previsibilidade e a segurança jurídica em relação ao tratamento posterior de dados disponíveis publicamente.

Para além da legitimidade, especificidade e compatibilidade do propósito, o § 7º do art. 7º mantém os requisitos gerais de tratamento: a observância dos princípios e fundamentos da LGPD, assim como os direitos dos titulares, demonstrando mais uma vez a importância da interpretação sistemática da Lei Geral de Proteção de Dados.

Tratam-se, por conseguinte, de requisitos gerais que se referem ao tratamento como um todo, enquanto que os requisitos específicos se referem a nova finalidade conferida ao tratamento posterior (TAVARES, 2022, p. 209).

Assim, dentro da esfera do *data scraping* voltado a dados disponíveis publicamente, é fundamental a análise: (i) de qual categoria de dados está se tratando, (ii) de quais os requisitos exigidos para tanto, e (iii) da avaliação se eles estão sendo cumpridos ou podem ser implementados pelo agente de tratamento, para se chegar mais próximo a uma conclusão sobre a licitude da prática caso a caso.

Como se verá em seguida, a análise dos requisitos específicos do tratamento de dados disponíveis publicamente compõe o presente capítulo, juntamente com parcela dos requisitos gerais, pois é a partir da compreensão dos mesmos que se reúnem importantes insumos para chegar a uma conclusão quanto ao requisito geral da necessidade de indicação de base legal para este tipo de tratamento. Ainda, pretende-se analisar também algumas abordagens para compreensão da técnica de *data scraping* perante o que dispõe a LGPD, o que perpassa uma nova perspectiva sobre o poder do titular de controlar seus dados pessoais.

4 BASES LEGAIS PARA FUNDAMENTAÇÃO DO *DATA SCRAPING* E A TEORIA DA PRIVACIDADE CONTEXTUAL COMO RELEVANTE REFERENCIAL TEÓRICO

A necessidade de indicação de base legal é o último requisito a ser tratado na presente pesquisa, tendo em vista que, como se verá a seguir, é resultado da compreensão dos demais requisitos relativos ao tratamento de dados disponíveis publicamente, independentemente da hipótese se encaixar no §3º, §4º ou §7º, todos do art. 7º da LGPD. Por isso, inicialmente, tratar-se-á neste capítulo sobre as possíveis bases legais capazes de justificar o *data scraping* voltado a dados pessoais disponíveis publicamente.

Em seguida, propõe-se um aprofundamento na teoria da privacidade contextual, proposta por Helen Nissenbaum (2010), e suas implicações na compreensão do sistema de proteção de dados pessoais nacional. Tal detalhamento justifica-se no fato de que, como demonstrado ao longo desta pesquisa, a análise contextual constitui-se fator fundamental para a aferição de requisitos como o da compatibilidade, da boa-fé objetiva e da finalidade.

Assim, apresenta-se com maior aprofundamento o modelo proposto por Helen Nissenbaum (2010), buscando-se propor a teoria da privacidade contextual como uma abordagem que auxilia a ampliar a concepção tradicional de autodeterminação informativa.

4.1 POSSÍVEIS BASES LEGAIS PARA FUNDAMENTAÇÃO DA PRÁTICA DE *DATA SCRAPING* VOLTADO A DADOS PESSOAIS DISPONÍVEIS PUBLICAMENTE

Como visto no capítulo anterior desta pesquisa, a indicação de base legal corresponde a uma obrigação do agente de tratamento diante do modelo *ex ante* de proteção de dados pessoais adotado pela Lei Geral de Proteção de Dados, sendo um requisito geral para qualquer tipo de tratamento.

Como já explicitado na apresentação de conceitos fundamentais trazidos pela Lei no primeiro capítulo desta pesquisa, existem 10 bases legais previstas nos incisos do art. 7º da LGPD, sendo elas: (i) consentimento, (ii) cumprimento de obrigação legal ou regulatória, (iii) execução de políticas públicas, (iv) realização de estudos por órgão

de pesquisa, (v) execução de contrato, (vi) exercício regular de direitos, (vii) proteção da vida ou incolumidade física, (viii) tutela da saúde, (ix) legítimo interesse e (x) proteção do crédito. Ainda, no art. 11 da Lei estão previstas as bases legais específicas para o caso de dados pessoais considerados sensíveis[26].

Contudo, neste capítulo, busca-se abordar a possibilidade de compreender as hipóteses dos §§ 3º, 4º e até mesmo do 7º, como bases legais autônomas, desde que observados os requisitos dispostos em Lei. Ainda, foca-se no legítimo interesse como possível base legal para o *data scraping* - e para tratamentos semelhantes no contexto do *Big Data* - de dados disponíveis publicamente, explorando os parâmetros necessários para sua aplicação, considerando que, em boa parte dos modelos de negócio que se estruturam na economia de dados, as possíveis bases legais se resumem ao consentimento e ao legítimo interesse.

4.1.1 As hipóteses dos §§ 3º, 4º e 7º do art. 7º da LGPD como bases autônomas

A expressão constante tanto no *caput* do art. 7º, quanto *caput* do art. 11 de que "o tratamento [...] somente poderá ser realizado" nas hipóteses identificadas em seus incisos seguintes, pode dar a impressão de que se trata de regra sem exceções. Todavia, a hipótese do art. 14, §1º[27], demonstra a possibilidade de que, ao longo do texto da Lei, existam hipóteses mais específicas e adequadas nas quais pode-se

[26] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[27] Previsão que trata dos dados de crianças e adolescentes e que impõe o consentimento do responsável legal como hipótese permissiva do tratamento desta categoria de dados. Conforme o dispositivo legal: "Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal."

fundamentar o tratamento de dados pessoais, além daquelas expressamente previstas nos arts. 7º e 11 (TAVARES, 2022, p. 150-151).

Para Wimmer, lógica similar aplica-se à previsão do art. 23[28] da LGPD. Apesar do legislador, ao prever de modo taxativo as bases legais, ter buscado maior sistematicidade à Lei, apenas utilizando-se de grande esforço hermenêutico seria possível afirmar que as bases legais previstas no art. 7º podem dar conta da variedade de contexto em que dados pessoais são tratados pelo Poder Público (WIMMER, 2019, p. 131). No mesmo sentido vai o entendimento de Mendes e Doneda, que consideram o art. 23 como uma hipótese autorizativa de tratamento adicional, para além das dispostas no art. 7º (MENDES, DONEDA, 2018, p. 472-473).

Portanto, apesar do caput do art. 7º da LGPD determinar que o tratamento "somente poderá ser realizado" nas hipóteses mencionadas nos seus incisos, considerando os casos apresentados acima, não é razoável compreender que tal taxatividade impõe que agentes apoiem atividades de tratamento em bases legais imprecisas e inadequadas. Assim, a compreensão deve ser no sentido de que o tratamento somente poderá ser realizado se pautado em uma base legal, sendo que este fundamento justificador pode estar, inclusive, fora do rol do art. 7º da LGPD (BAIÃO; TEIVE, 2020, p. 315).

Ainda que parte da doutrina (COTS; OLIVEIRA, 2018, p. 104) entenda que o art. 7º estabelece rol taxativo de hipóteses autorizativas de tratamento, diante da lógica exposta acima, discute-se sobre a necessidade de que os cenários do §§ 3º e 4º sejam fundamentados em alguma das bases legais dispostas nos incisos do art. 7º (TAVARES, 2022, p. 150).

É justamente por se entender que a interpretação mais adequada da expressão "somente poderá ser realizado" é aquela que impõe a necessidade da indicação de base legal fundada na LGPD, esteja ela dentro ou fora do que estabelecem os arts. 7º e 11; que se defende a leitura dos §§ 3º e 4º como, por si sós, hipóteses autorizativas de tratamento.

---

[28]"Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II - (VETADO); e III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei."

Compreende-se que os §§ 3º e 4º constituem bases autônomas, visto que, diante dos critérios desenhados especialmente para a categoria de dados disponíveis publicamente e para o contexto em que se inserem, os requisitos tornam-se mais compatíveis e específicos para as hipóteses que abarcam, e, logo, os dispositivos são mais adequados do que qualquer outra hipótese de tratamento do art. 7º (TAVARES, 2022, p. 155). Ainda, tratam-se de fundamentos expressamente dispostos na LGPD, sendo que esta "flexibilização" da taxatividade dos arts. 7º e 11 têm limites estabelecidos pelo próprio texto legal, não havendo como existir outras bases legais que não aquelas inseridas na norma, ou do contrário, perder-se-ia de vista o objetivo da proteção de dados pessoais contra seu tratamento indiscriminado.

Tavares (2022), no seguinte trecho, identifica como as hipóteses dos §§ 3º e 4º estão em consonância com a sistemática de proteção de dados pessoais, mesmo que, em uma primeira leitura, o dispositivo pareça conceder demasiada flexibilidade ao agente de tratamento:

> Nesse sentido, há que se evidenciar o equilíbrio implícito proposto pela LGPD. Ora, as previsões dos §§ 3º e 4º permitem, de um lado, que o agente de tratamento utilize os dados pessoais disponíveis publicamente sem a necessidade de amparo em outra base legal. No entanto, isso somente poderá acontecer caso literalmente todos os requisitos previstos em ambos os parágrafos sejam integralmente observados e cumpridos no caso concreto. Ou seja, a flexibilidade da base legal autônoma nesse caso se justifica a partir da rígida exigência de critérios especificamente desenhados para o tratamento dessa categoria de dados pessoais – critérios esses que só fazem sentido justamente diante da natureza dos dados de acesso público e tornados manifestamente públicos pelo titular. (TAVARES, 2022, p. 156)

Em outro sentido, Teffé e Viola compreendem que a hipótese do §3º não dispensa a indicação de outra base legal autorizativa contida no art. 7º ou 11, pois admitir que dados disponíveis publicamente possam ser tratados sem uma base legal específica, significa que uma informação publicada poderia ser utilizada para finalidade distinta sem que o novo controlador precisasse demonstrar a adequação com alguma das hipóteses autorizativas de tratamento (TEFFÉ; VIOLA, 2021, p. 139).

Todavia, conforme visto ao longo desta pesquisa, por força de exclusão, o §3º trata da hipótese de tratamento cuja finalidade seja idêntica a que justificou à divulgação do dado, isso significa dizer que não haveria possibilidade de tratamento para finalidade distinta, já que, não existindo equivalência entre as finalidades original

e secundária, o tratamento se enquadraria no § 7º do art. 7º.

Com isto posto, compreende-se que tratar o § 3º do art. 7º como base legal autônoma não significa permitir abusos no tratamento de dados ou gerar “brecha” ao desonerar o agente de tratamento de indicar base legal do art. 7º. Pelo contrário, significa exigir, em adição aos requisitos gerais para qualquer tratamento - como observância aos princípios e garantia dos direitos dos titulares -, pressupostos ainda mais específicos e adequados ao contexto de tratamento de dados disponíveis publicamente, os quais foram especialmente desenhados para este cenário - a saber: a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Quanto ao § 4º, é consonante, pela clareza do próprio dispositivo legal, que, cumprindo-se os requisitos do dispositivo, é dispensada a coleta de consentimento para tratamento de dados pessoais manifestamente públicos. Há quem afirme que trata-se de uma hipótese de dispensa de manifestação *expressa* do consentimento, já que a Lei presume que o ato de publicar os próprios dados pessoais é uma manifestação de vontade do titular e uma autorização para tratá-los, desde que observados os demais requisitos (MARCACINI, 2020, l. 2821 de 8687).

A questão que se levanta acerca do dispositivo é sobre a possibilidade de extensão da dispensa do consentimento para as demais hipóteses autorizativas previstas no art. 7º, quando preenchidos os demais pressupostos estabelecidos, isto é, se a exceção se estende às demais bases legais (MATTIUZO; FAVARO, 2021, p. 405).

A discussão se deve ao fato de que a previsão de exceção do consentimento teve origem no primeiro Projeto de Lei proposto pelo Ministério da Justiça, cuja única base legal prevista era o consentimento, e assim a hipótese de dispensa do consentimento estava anexada a tal disposição central. Ao longo do aprimoramento do texto legal, manteve-se a referência ao consentimento no §4º, o que levantou a dúvida se tal dispensa deveria ser aplicada às demais bases do art. 7º e 11 no caso de dado tornado manifestamente público pelo titular (MATTIUZO; FAVARO, 2021, p. 405).

Pois bem, partindo-se de dedução lógica, não haveria sentido em limitar à hipótese do § 4º apenas ao consentimento , já que o dispositivo se refere ao caput - não ao inciso I - do art. 7º. Ainda, se a dispensa se limitasse apenas ao consentimento, seria forçoso concluir pela existência de hierarquia entre as bases legais, tema que hoje já pode ser considerado superado, considerando que é evidente que todas as

hipóteses autorizativas são igualmente aplicáveis e válidas (MATTIUZO; FAVARO, 2021, p. 405). Assim, conclui-se que na hipótese do §4º não há necessidade de indicação de uma nova base legal para o tratamento, pois trata-se de verdadeira hipótese autorizativa para o tratamento de dados (TEFFÉ; VIOLA, 2021, p. 139).

Por fim, o § 7º do art. 7º também gera debates sobre sua autonomia como base legal. Como foi exposto, por se tratar de hipótese de tratamento posterior para novas finalidades, somente poderá ser realizado quando compatível com a finalidade original, e claro, quando observar os outros pressupostos que dizem respeito a este tratamento. Para aferição da existência desse elo entre finalidade original e posterior, a avaliação da compatibilidade é um importante instrumento, sendo que o mesmo já é indicado no contexto da GDPR[29].

Caso o agente de tratamento avalie e conclua pela compatibilidade, compreende-se não ser necessária indicação de nova base legal para o tratamento posterior dos dados pessoais. Se, por outro lado, houver incompatibilidade, cabe ao agente de tratamento a obtenção de consentimento dos titulares ou a satisfação de uma das demais hipóteses que justificam o tratamento (VAINZOF, 2019, p. 140-142).

De qualquer modo, ainda que mais tarde a Autoridade Nacional de Proteção de Dados se manifeste sobre o tema e entenda pela necessidade de indicação de alguma das bases legais do art. 7º, a questão é que, em qualquer um dos casos, mantém-se a obrigação imposta ao agente de tratamento de obedecer a legitimidade, a especificidade e a compatibilidade dos propósitos, além dos requisitos gerais de tratamento. Isso porque, a necessidade do tratamento se prestar a finalidades legítimas e específicas está presente como requisito expresso no rol de princípios do art. 6º, em seu inciso I - e a necessidade de compatibilidade do tratamento encontra guarida no mesmo dispositivo, ainda que implicitamente, por meio do qual se proíbe a incompatibilidade de finalidade no tratamento posterior de dados pessoais. Assim, como o caso em questão é o tratamento posterior de dados pessoais para novas finalidades a aferição da compatibilidade deve se dar entre a finalidade que motivou a publicização e a nova que se pretende empregar ao tratamento.

Por conta disso, conclui-se que, apesar da relevância da discussão, esta torna-se menos central frente ao fato de que todas as demais obrigações da Lei se

[29] Conforme pode-se depreender da *Opinion 03/2013* adotada pelo *Article 29 Data Protection Working Party*, que dá diretrizes (no item III.2) de como realizar a avaliação de compatibilidade, ou seja, como verificar a compatibilidade entre a finalidade original e a nova.

mantêm para o agente de tratamento, e tendo em vista que, de uma forma ou de outra, este terá que avaliar a especificidade, a legitimidade e a compatibilidade do propósito do tratamento antes de realizá-lo de fato. Lógica semelhante também se aplica às hipóteses dos §§ 3º e 4º, claro que considerando as diferenças nos requisitos específicos de cada um dos dispositivos.

Com todo o exposto, neste e demais capítulos da presente pesquisa, é possível chegar a um modelo prático apto a auxiliar na determinação da base legal a justificar o *data scraping* voltado a dados disponíveis publicamente, passando pela análise, em especial, da compatibilidade ou identidade da finalidade, da categoria dos dados tratados, e do cumprimento de requisitos específicos, se houverem. Em similaridade ao que é proposto por Giovana Milanez Tavares, propõe-se um formato de avaliação para análise da observância dos critérios normativos para indicação da base legal (TAVARES, 2022, p. 156-157), neste caso, a fim de justificar a prática de *data scraping* de dados disponíveis publicamente. Para isso deve-se realizar análises em 4 diferentes níveis que dizem respeito a:

(i) categoria dos dados: isto é, se os dados tratados são de fato considerados de acesso público ou tornados manifestamente públicos pelo titular - não sendo o caso, as hipóteses dos §§ 3º, 4º e 7º não se enquadram, devendo o agente de tratamento avaliar a fundamentação em outra das bases legais dispostas pela LGPD;

(ii) finalidade do tratamento: se é a mesma que justificou a disponibilização do dado - para enquadramento nos §§ 3º ou 4º - ou é compatível - para enquadramento no § 7º;

(iii) requisitos específicos: se estão sendo cumpridos os pressupostos particularmente desenhados para a hipótese que se pretende enquadrar o tratamento - além dos requisitos gerais, por óbvio;

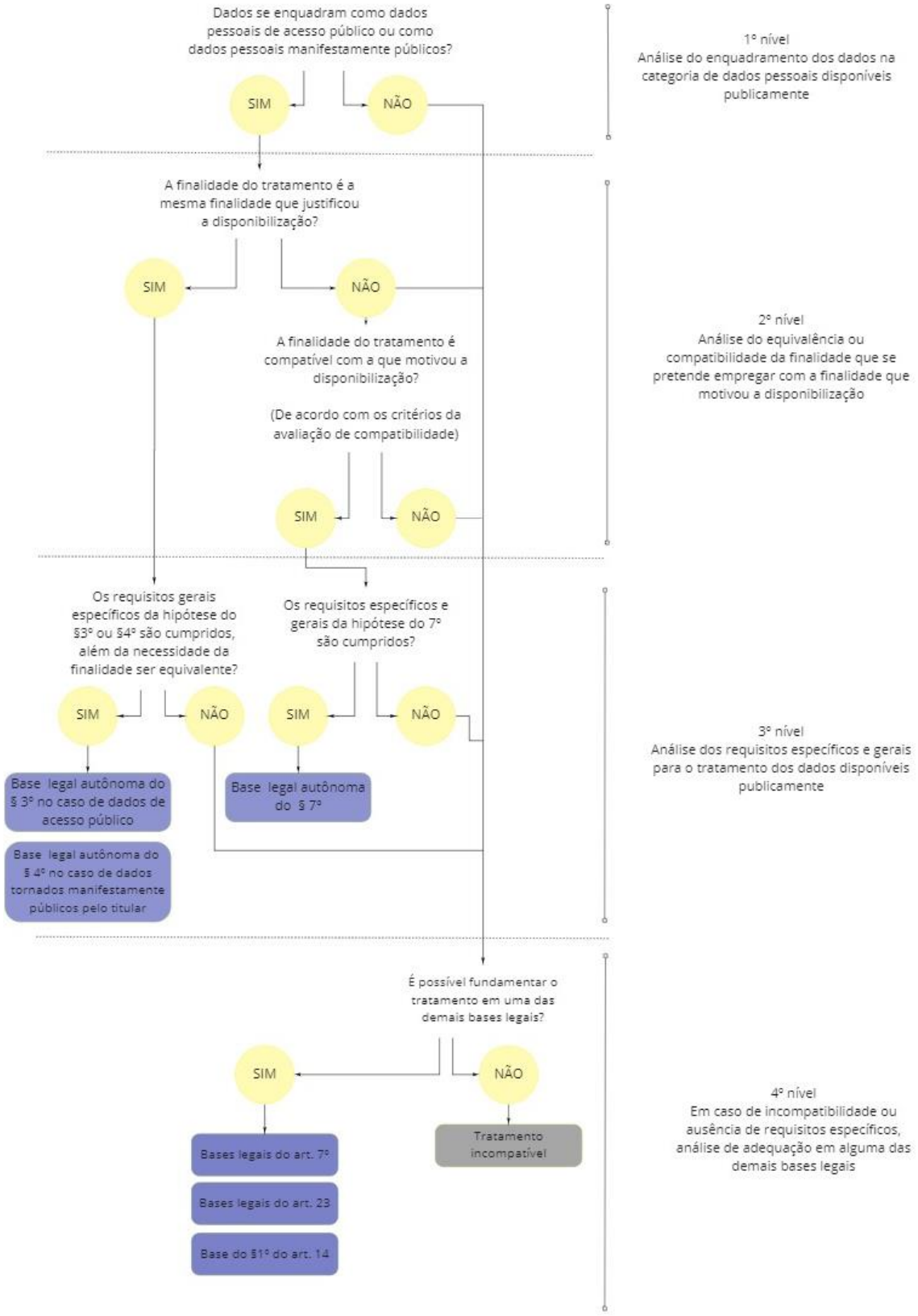
(iv) e em caso de ausência de compatibilidade ou de identidade entre finalidade pretendida e finalidade original, ou não havendo cumprimento de algum dos requisitos específicos, a análise da adequação em alguma das demais bases legais.

A fim de que o *data scraping* seja legítimo e lícito, a prática deve necessariamente apoiar-se em alguma base legal, seja em alguma das defendidas aqui como autônomas, sejam nas demais do art. 7º. Não sendo isso possível, trata-se

de tratamento incompatível (TAVARES, 2022, p. 157).

Assim, conclui-se que somente após análise aprofundada (i) do conceito de dado de acesso público e dado tornado manifestamente público pelo titular, (ii) do conceito de finalidade equivalente ou compatível, e (iii) dos requisitos gerais e específicos das hipóteses dos §§3º, 4º e 7º, do art. 7º da LGPD; que se torna possível avaliar, de fato, qual a base legal mais adequada frente ao *data scraping* voltado a dados pessoais disponíveis publicamente. Assim, para essa avaliação, propõe-se uma análise em 4 níveis, conforme se demonstra através do fluxograma (Figura 1).

Figura 1. Fluxograma dos critérios normativos para indicação da base legal mais adequada ao tratamento de dados disponíveis publicamente



Fonte: Tavares (2022, p. 157).

Quanto ao primeiro nível, que diz respeito à análise da categoria dos dados pessoais, é necessário conferir atenção aos cenários das redes sociais, isso porque, a publicação em perfis de redes sociais não necessariamente significa que o titular está tornando um dado pessoal manifestamente público.

Se o titular faz uma postagem em um perfil público de rede social, os dados, evidentemente, podem ser considerados manifestamente públicos. Todavia, se o perfil da rede social for privado ou se existirem configurações que delimitem o alcance daquela postagem por exemplo, não há como demonstrar que as informações foram tornadas *manifestamente* públicas (TAVARES, 2022, p. 77-78).

Dentro deste cenário das redes sociais, o caso da Clearview AI demonstra como dados acessíveis na *Web* e postados nas mídias sociais, inclusive em perfis públicos, não necessariamente poderiam ser considerados tornados manifestamente públicos pelo titular.

A Clearview AI[30] criou um programa de reconhecimento facial através da prática de *data scraping* de mais de três bilhões de imagens de redes sociais, como *Twitter* e *Facebook*. A empresa afirmou que as imagens teriam sido tornadas manifestamente públicas pelos usuários e que, portanto, não haveria interesse de privacidade acerca das informações (PRIVACY INTERNACIONAL, 2021, p. 1).

Contudo, ainda que as imagens tenham sido publicadas em perfis públicos, as fotos coletadas não necessariamente teriam sido tornadas públicas pelo titular, já que as redes sociais permitem que um usuário publique fotos suas e de qualquer outra pessoa. Essas pessoas, por sua vez - que podem ser amigos, desconhecidos em lugares públicos, ou clientes de empresas -, por não terem postado diretamente a foto, não a *tornaram pública*, e inclusive, poderiam nem sequer ter conhecimento de que suas imagens estariam disponíveis publicamente[31].

Nesse sentido, inclusive, foi a determinação da autoridade de proteção de dados da Austrália - Office of the Australian Information Commissioner (OAIC) - que

[30] Apesar do caso servir para análise de diversos aspectos concernentes ao *data scraping* de dados disponíveis publicamente, por enquanto se atentará a como o caso se relaciona com o primeiro ponto de análise apresentado acima, isto é, ao momento de avaliação da categoria de dados pessoais.

[31]"Second, it is common knowledge for anyone even mildly versed in using the Internet and social media that many online photos of individuals have not been made public by the data subject themselves. Social media allows a user to upload photos of themselves, and of any other person. These other persons (may they be friends of the uploader, unknown bystanders in public spaces, or customers of businesses that post pictures of their establishment and clients online) have not themselves uploaded their facial images online, and may not even know that photos containing their faces have been uploaded and are present on the public Internet."(PRIVACY INTERNACIONAL COMPLIANT, 2021, p. 30)

afirmou que é provável que diversas imagens tenham sido “raspadas” para a base de dados da Clearview AI sem terem sido publicadas pelo próprio indivíduo que aparece na imagem (OAIC, 2021, p. 46). Logo, no caso, não se cumpriu o requisito específico exigido para que os dados sejam considerados tornados manifestamente públicos pelo titular, já que, para isso, se impõe que o *titular* tenha tornado a informação pessoal pública, e não terceiro.

Em razão disso, havendo uma devida avaliação dos requisitos para enquadramento na categoria, seria possível conceber que nem todos os dados pessoais coletados pela empresa poderiam se enquadrar dentro da categoria de dados manifestamente tornados públicos pelo titular. Assim, o segundo nível surge, justamente, para que se avalie se através do *data scraping* pretende-se coletar de fato dados pessoais disponíveis publicamente ou simplesmente dados pessoais.

Por sua vez, no segundo nível, o exemplo da Clearview AI claramente enquadra-se como um tratamento para novas finalidades. Nesse sentido, na reclamação[32] contra a empresa, endereçada pela Privacy Internacional (PI)[33], foi apontado que a prática de processamento de dados disponíveis publicamente de redes sociais tem sido objeto de crítica devido a preocupações sobre sua compatibilidade com expectativas razoáveis de privacidade (PRIVACY INTERNACIONAL, 2021, p. 16).

Na reclamação ainda consta que, em consulta sobre a utilização da monitoração das redes sociais realizada pelo *European Asylum Support Office*, a *European Data Protection Supervisor*[34] (EDPS) considerou que o monitoramento de redes sociais geralmente resulta no uso de dados pessoais além de seu propósito

[32] “On 27 May 2021, Privacy International (PI) filed complaints against Clearview AI with the UK and French data protection authorities (ICO and CNIL). Simultaneously, similar complaints were filed by Hermes Centre for Transparency and Digital Human Rights in Italy, Homo Digitalis in Greece, and noyb - the European Center for Digital Rights in Austria. On 29 November 2021, the UK data protection authority (ICO) announced that it had found "alleged serious breaches of the UK's data protection laws", and issued a provisional notice to stop further processing of the personal data of people in the UK and to delete it. It also announced its ’provisional intent to impose a potential fine of just over £17 million‘ on Clearview AI.” (PRIVACY INTERNATIONAL, 2021b)

[33] Privacy International é uma organização não-governamental britânica constituída em 1990 e que tem como objetivo principal a monitoração da vigilância e das invasões de privacidades individuais conduzidas por governos ou organizações.

[34] O European Data Protection Supervisor (EDPS) é a autoridade de proteção de dados para as instituições da União Europeia. Um dos seus principais objetivos é supervisionar as instituições da União Europeia quanto ao aspecto da proteção de dados.(EUROPEAN DATA PROTECTION SUPERVISOR, 2022)

inicial[35]. Em análise ao caso, portanto, a opinião constante da reclamação foi a de que provavelmente haveria uma ausência de compatibilidade no tratamento realizado pela Clearview AI em relação à finalidade original que justificou a disponibilização dos dados nas redes sociais (PRIVACY INTERNACIONAL, 2021, p. 16).

Na determinação da OAIC restou concluído que boa parte dos indivíduos não teriam ciência e nem *expectativas razoáveis* de que imagens e vetores teriam sido coletados pela Clearview AI e armazenados em base de dados (OAIC, 2021, p. 46). A CNIL[36], em decisão sobre o caso, considerou que não haveria qualquer relação entre os titulares de dados e a empresa, e que, mesmo sendo possível haver expectativas razoáveis de que terceiros acessem fotos de tempos em tempos, a natureza publicamente disponível do dado não é suficiente para entender que os titulares poderiam razoavelmente esperar que suas imagens fossem utilizadas para alimentar um software de reconhecimento facial (CNIL, 2021, n.p).

Como visto, as razoáveis expectativas estão inerentemente vinculadas à compatibilidade entre a finalidade original e a posterior. Compreender quais entendimentos têm sido aplicados, na prática, colabora para entendimento do que pode ser interpretado como razoavelmente esperado pelo titular e, consequentemente, aproxima a compreensão de quais atividades deverão ser consideradas compatíveis com a finalidade original.

Quanto ao terceiro nível de análise, um dos principais requisitos específicos é a avaliação da equivalência ou da compatibilidade da finalidade do tratamento posterior com a que motivou a disponibilização do dado. Pois bem, o que se observa na prática, é que empresas que tenham como modelo de negócios a agregação e estruturação de dados ou que se enquadram como *data brokers*, poderão agregar

[35] 61. The practice of gathering and processing publicly available data from social media platforms, coined ‘social media intelligence’ (‘SOCMINT’) or ‘social media monitoring’, has been decried in recent years for concerns about its compatibility with reasonable expectations of privacy. As part of a consultation on the use of social media monitoring by the European Asylum Support Office, the European Data Protection Supervisor (‘EDPS’) considered that social media monitoring “involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate. 62. “Clearview’s processing is a particularly intrusive form of social media monitoring, which goes far beyond the consultation and analysis of publicly available informatio on an ad hoc basis. Clearview’s automatic collection, storage and processing for extraction of biometric identifiers make it further removed from any reasonable expectations of data subjects and therefore in no way compatible with the principle of fairness”.(PRIVACY INTERNACIONAL COMPLIANT, 2021, p. 16)

[36] Autoridade de proteção de dados francesa, que também se manifestou sobre o tema devido a extensão do *data scraping* e outros tipos de tratamento empregados pela Clearview AI para indivíduos europeus, em especial, franceses.

uma pluralidade de informações, a partir de uma pluralidade de fontes e origens, com objetivo de utilizá-las para uma pluralidade de propósitos.

Em boa parte desses casos, existirá uma necessidade de coleta de dados - a partir do qual se desenvolverá uma inteligência, analisando e estruturando os dados pessoais -, e aqui encaixa-se o *data scraping*, considerado em seu conceito amplo, isto é, sendo uma técnica pela qual se utiliza um *bot* para coletar, analisar e organizar dados da web de maneira automatizada (LIU, 2020, p. 28).

A Neoway[37], por exemplo, afirma que coleta quase a totalidade de dados pessoais por meio de bases de dados públicas, que existem em função da Lei de Acesso à Informação (NEOWAY, p. 19). Ainda, a empresa fornece soluções com as mais diversas finalidades, como marketing, compliance, prevenção de fraudes, análises jurídicas, gestão de crédito, entre outros. Dessa forma, percebe-se que existem variadas finalidades envolvidas na coleta de dados pessoais realizados pela empresa, cenário que, inclusive, não é incomum.

O JusBrasil, de forma semelhante, coleta dados de diversas fontes públicas oficiais, como diários oficiais e processos judiciais constantes nos sites dos Tribunais, e os utiliza para várias finalidades, dentre elas: (i) gerar análises estatísticas, através da correlação e do cruzamento de dados; (ii) compartilhar informações com terceiros para viabilizar a prestação dos serviços e o acesso à plataforma; (iii) compartilhar informações no âmbito de outras plataformas, produtos e serviços que fazem parte do grupo econômico ao qual a empresa faz parte, entre outras (JUSBRASIL, 2020).

O *data broker* TransUnion[38] oferece soluções de checagem de crédito, marketing, entre outras, e, conforme suas políticas de privacidade (TRANSUNION, 2021), realiza coleta de dados pessoais de variadas fontes de terceiros - como bancos, entidades governamentais, informações publicamente disponíveis e parceiros de marketing - e de diversos tipos de dados, incluindo, dados pessoais publicamente disponíveis.

Nesses casos, devido a diversidade de propósitos para utilização de dados

---

[37] Conforme site da empresa, a Neoway desenvolve soluções de *Big Data Analytics* e Inteligência Artificial. Disponível em: https://www.neoway.com.br/.

[38] A empresa enquadra-se no conceito de *data broker* considerando que algumas de suas soluções constam registradas na lista de *data brokers* da Califórnia (disponível em <https://oag.ca.gov/data-brokers>). Importante esclarecer que, de acordo com a legislação da Califórnia - Civil Code § 1798.99.80 -, aquelas empresas que se adequam à acepção de *data brokers* - isto é, negócios que conhecidamente coletam e vendem para terceiros informações pessoais de consumidores com os quais não possuem relação direta - devem registrar-se frente ao Office of the Attorney General, através de seu website.

pessoais constante em uma base de dados, a avaliação da compatibilidade torna-se complexa e de difícil parametrização. Há que se levar em conta cada uma das finalidades posteriores que se pretende empregar ao tratamento de dados disponíveis publicamente, assim como cada uma das finalidades que envolvem o contexto das fontes de coleta de dados pessoais. Ainda, levanta-se o questionamento acerca da possibilidade de um resultado positivo na avaliação de compatibilidade, considerando que dados coletados da mesma fonte são utilizados para finalidades distintas. Nesse cenário, ganha relevância a análise do contexto do fluxo percorrido pelos dados pessoais, além da observância do princípio da transparência.

Para que se obtenha um ponto de partida mais objetivo quanto ao estabelecimento das finalidades de bancos de dados ou *sites* utilizados como fontes para o *data scraping*, é importante que as plataformas que disponibilizam dados pessoais na Internet busquem determinar quais as finalidades da disponibilização dos dados, com intuito de tornar mais palpável a avaliação de compatibilidade aos agentes que poderão tratar os dados disponíveis publicamente de modo posterior.

Por fim, quanto ao nível quatro, caso não seja possível tratamento com base nos §§3º, 4º ou 7º, parte-se para avaliação da possibilidade de adequação nas demais bases legais previstas nos incisos do art. 7º. Isto é, em caso de incompatibilidade, o controlador deverá comprovar outro fundamento, como o consentimento antes de coletar dados para um novo propósito (VAINZOF, 2020, p. 140-142).

Conforme visto, existem diversos tipos de “corretagem” de dados dentro da esfera dos *data brokers* e de outras empresas cuja atividade envolva a coleta e agregação de dados pessoais como forma de prestação de serviços a terceiros, sendo que parte destas empresas realiza o tratamento de dados pessoais para fornecimento dos mais variados serviços e não de apenas um. Considerando que não é incomum tal prática, torna-se possível conceber que boa parte dos negócios nesta área teriam dificuldade de fundamentar o tratamento em outras bases legais que não o consentimento ou o legítimo interesse - como é o caso de empresas com soluções de marketing e prospecção, por exemplo -, com exceção de casos mais específicos.

Para Mattiuzo e Favaro, caso a doutrina adotasse a ideia de que os dados só seriam *manifestamente* públicos caso houvesse algum tipo de prova de validação da ciência do titular, a atividade de *data brokers* tornar-se-ia inexequível, e serviços relevantes dependentes destas empresas deixariam de ser prestados, afetando atividades de inúmeros setores da economia (MATTIUZO, FAVARO, 2021, p. 411) e,

consequentemente, o caráter inovador e disruptivo de operações que se baseiam em contextos de *data mining* e inteligência artificial. Lógica similar pode se aplicar ao caso de coleta de consentimento por parte de *data brokers* ou empresas com modelos de negócios similares. Se fosse necessária a coleta de consentimento do titular a toda atividade de tratamento realizada para novas finalidades, haveria uma fadiga[39] do instituto, além de que a adoção de tal base legal geraria travas para o negócio, podendo até torná-lo inviável (TAVARES, 2022, p. 212). Em realidade, na maior parte das vezes, seria inexequível para a empresa obter consentimento explícito de cada indivíduo cujos dados são coletados em massa e de modo automatizado (LIU, 2020, p. 52-53).

Bioni relata problemáticas a serem enfrentadas em decorrência da necessidade de obtenção de consentimento em caso de tratamento para novas finalidades (BIONI, 2019, p. 240):

> Sem exaurir a lista de argumentos, destaca-se que: a) construir-se-ia um regime problemático para a dinamicidade das relações sociais, na medida em que a "trava" do consentimento estaria a todo momento bloqueando o fluxo dos dados pessoais; b) em meio a essa "burocratização", os cidadãos seriam sobrecarregados com tal estratégia normativa, já que exigir, a todo momento, o seu consentimento, o levaria à exaustão – a chamada fadiga do consentimento –, o que encontra ressonância nas limitações cognitivas do ser humano (subcapítulo 4.1.2); c) a inovação seria prejudicada. Toda e qualquer atividade precisaria de um espaço não previamente definido para criação, de modo que exigir um escopo inventivo pré-definido na economia dos dados seria inviabilizá-lo.

Diante de tais problemáticas, surge o legítimo interesse como uma opção que desonera o agente da coleta de consentimento. Contudo, isso não significa que a utilização da base legal se trata de um cheque em branco. Pelo contrário, o legítimo interesse trata-se de uma válvula de escape para que as demais bases legais não sejam "sobrecarregadas" (BIONI, 2019, p. 249). E diante da sua flexibilidade, visto que não há na LGPD uma clara determinação de escopo de aplicação desta hipótese autorizativa, adquire especial peso as expectativas do titular, além da finalidade, necessidade e proporcionalidade da utilização de dados (TEFFÉ; VIOLA, 2021, p. 141).

[39] Termo utilizado por Bruno Bioni para referir-se à exaustão do uso do instituto que poderia ser alcançada nos casos de exigência de consentimento para todo tratamento realizado para nova finalidade. Logo após o parágrafo aqui referenciado, trata-se do tema através de citação direta de trecho de livro redigido pelo jurista.

4.1.2 Legítimo Interesse como base legal para *data scraping* de dados pessoais disponíveis publicamente

Dadas algumas dificuldades associadas ao consentimento no contexto do *Big Data*, o legítimo interesse surge como uma alternativa frente à obtenção do consentimento, podendo ser utilizado como fundamento do processamento de dados, o que possibilita um equilíbrio entre benefícios comerciais e sociais e os direitos e interesses dos indivíduos (INFORMATION COMMISSIONER'S OFFICE, 2017, p. 32-34). Encaixam-se nesta hipótese autorizativa tratamentos em que a obtenção do consentimento do titular poderia criar óbice para a exploração regular de dados pessoais, ou quando se constatar que outras bases legais não são adequadas com o tratamento realizado no contexto da internet das coisas e *Big Data* (TEFFÉ; VIOLA, 2021, p. 141).

Na esfera do *data scraping,* que se vincula diretamente ao contexto do *Big Data,* pode se compreender que o legítimo interesse é a hipótese que pode melhor se adequar ao tratamento a depender do contexto de tratamento realizado pelo agente.

O *data broker* Acxiom, empresa que oferece soluções voltadas ao marketing, em sua política de privacidade voltada para GDPR, afirma utilizar-se de fontes disponíveis publicamente e de terceiros para coleta de dados pessoais (AXCIOM, 2018). Dentro das bases legais que utiliza está o legítimo interesse da organização ou de seus parceiros, para marketing direto, prevenção de fraude, segurança da informação, e propósitos organizacionais.

A Serasa Experian, que tem como modelo de negócio a coleta e agregação de dados para prestação de seus serviços, oferece soluções de gestão de riscos, marketing e certificação digital e na política de privacidade do seu aplicativo (SERASA EXPERIAN, 2021) afirma, dentre outras bases legais, se basear no legítimo interesse para tratamento de dados pessoais. Os dados coletados pela empresa incluem dados pessoais disponíveis publicamente, já que as fontes pelas quais coleta dados incluem: (i) dados disponíveis publicamente mantidos por órgãos da Administração Pública Direta ou Indireta; (ii) convênios com órgãos públicos; (iii) dados disponíveis na internet por meio de processos automatizados; entre outros. É relevante destacar que as políticas de privacidade destacadas não deixam claro se a base legal do legítimo

interesse fundamenta, de fato, a atividade de coleta e agregação de dados em específico.

O que se pretende destacar, no entanto, é a possibilidade das empresas utilizarem e já estarem fundamentando alguns tratamentos de dados pessoais disponíveis publicamente nesta base legal. A questão se centraliza, portanto, em quais os limites e os parâmetros para aplicação do legítimo interesse em situações de *data scraping* de dados disponíveis publicamente.

É importante destacar que quando uma organização se baseia no legítimo interesse, apesar de não precisar buscar o consentimento do titular, como não há a responsabilidade do titular em concordar com o processamento, a responsabilidade recai completamente nas mãos da própria organização no sentido de ter de realizar e carregar uma avaliação do legítimo interesse e ter de garantir sempre que seus processos respeitem os direitos e interesses dos titulares (INFORMATION COMMISSIONER'S OFFICE, 2017, p. 34).

Justamente para trazer maior concretude para a hipótese autorizativa, tanto a LGPD, quanto a experiência internacional propõe parâmetros para sua aplicação. O Grupo de Trabalho do Artigo 29 propõe um teste da ponderação ou de proporcionalidade, em inglês denominado como *legitimate interest assessment* (LIA), em seu parecer sobre a base legal, o qual serviu de base para a redação da GDPR (TEFFÉ; VIOLA, 2021, p. 143).

O objetivo do teste de proporcionalidade ou avaliação de legítimo interesse é balancear os direitos envolvidos no tratamento de dados pessoais, do titular de dados e de quem faz uso dessas informações, isto é, os agentes de tratamento (BIONI, 2019, p. 252). O resultado do teste indica se o legítimo interesse poderá ser invocado como fundamento jurídico para o tratamento. O processo de avaliação pode ser dividido em quatro fases, de modo a garantir eficácia na realização do mesmo (ARTICLE 29 WORKING PARTY, 2013, p. 36-37).

São eles: (i) avaliação dos interesses legítimos; (ii) o impacto sobre o titular do dado; (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto prejudicial (TEFFÉ; VIOLA, 2021, p. 143).

Na LGPD, ainda que de modo disperso, constam parâmetros que levam a fases de avaliação similares. O art. 10, *caput*, estabelece a necessidade de avaliar a existência de uma finalidade legítima, a partir de situação concreta. Nesta avaliação

dos legítimos interesses é necessário verificar se o interesse é legítimo, isto é, se não contraria outros comandos legais e quais os benefícios ou vantagens auferidos pelo controlador com o uso de dados pessoais (BIONI, 2019, p. 253). Ainda, o interesse deve ser definido de modo claro, e deve ser real e atual, sendo que interesses demasiadamente vagos ou especulativos não serão suficientes (ARTICLE 29 WORKING PARTY, 2013, p. 38).

A segunda fase, para Bioni, trata-se daquela relativa à necessidade, que passa pela avaliação da minimização e da adequação em outras bases legais, estando prevista no art. 10, §1º da LGPD. É necessário avaliar se os dados coletados para o tratamento em questão são realmente aqueles necessários para se atingir a finalidade pretendida, e ainda, se o tratamento não poderia ser fundamentado por alguma das demais bases legais. (BIONI, 2019, p. 254).

Aqui deve-se prestar especial atenção em relação à estratégia de “quanto mais dados, melhor”. A priori, pode parecer algo quase inerente à empresas que trabalham com análise e estruturação de dados, todavia, tal modelo não respeita o princípio da necessidade. O ideal, portanto, é que haja uma ideia bem delimitada sobre para quais serviços os dados coletados irão ser utilizados, e com base nisso, buscar uma coleta de dados em harmonia com o mínimo necessário para cumprir a finalidade desejada.

A terceira fase, respaldada pelo inciso II do art. 10, traz a ideia de balanceamento de interesses, e é a principal fase do teste de proporcionalidade (TEFFÉ; VIOLA, 2021, p. 144) É a fase em que se sopesam os interesses do controlador e de terceiros diante dos interesses do titular dos dados. Isso é parametrizado pela noção de compatibilidade entre o uso adicional e aquele que originou a coleta dos dados pessoais, o que demanda, para Bioni, uma análise contextual a fim de examinar se o uso seria esperado pelo titular (BIONI, 2019, p. 254-255).

Destaca-se, neste ponto, a similaridade do teste de proporcionalidade e a avaliação de compatibilidade para analisar se a nova finalidade do tratamento posterior de dados disponíveis publicamente é compatível com a que justificou a divulgação. Com isto posto, importante fazer um juízo crítico: caso uma organização, através da avaliação de compatibilidade, chegue a conclusão que a finalidade não é compatível e que também o tratamento não se enquadraria nas demais bases legais do art. 7º, seria possível fundamentar o tratamento no legítimo interesse? Isto é, não

havendo compatibilidade entre a nova finalidade e a que justificou a disponibilização do dado, o tratamento poderia obter resultado positivo no teste de proporcionalidade, requisito para fundamentação com base no legítimo interesse?

Considerando o que foi exposto acima, acerca das similitudes do teste de proporcionalidade e avaliação de compatibilidade, percebe-se em ambas um ponto em comum: a necessidade de observância das expectativas dos titulares, seja em relação à finalidade informada a ele, seja em relação à finalidade que motivou a publicização. Nesse sentido, mostra-se difícil conceber a obtenção de um resultado positivo para o teste de proporcionalidade no caso de um tratamento cujas novas finalidades não são compatíveis com as que motivaram a disponibilização do dado, ou seja, no caso de um tratamento que não avançou na avaliação de compatibilidade devido a incompatibilidade da finalidade nova com a original.

Adicionalmente, ainda na terceira fase, deve-se analisar os possíveis impactos, em especial os negativos, para os titulares, como os de discriminação. Havendo impactos positivos, a balança tende a estar mais equilibrada (BIONI, 2019, p. 255). Para Bruno Bioni, acerca desta fase do teste de proporcionalidade (BIONI, 2019, p. 255):

> Em síntese, do início ao fim, essa fase do teste é calibrada pelo vocabulário da teoria da privacidade contextual, devendo-se analisar as legítimas expectativas em jogo e, principalmente, se o fluxo informacional é apropriado-íntegro para o livre desenvolvimento da personalidade do titular.

Na quarta fase, devem-se identificar possíveis salvaguardas a serem aplicadas ao caso concreto, conforme §§2º e 3º do art. 10 indicam. A exemplo: maior transparência, mecanismos de *opt-out*, que permitem o cidadão realizar a opção de estar fora dos tratamentos que considerar incompatíveis com suas legítimas expectativas (TEFFÉ; VIOLA, 2021, p. 144), e medidas de mitigação de riscos aos titulares de dados, como pseudoanonimização, tecnologias para reforçar a proteção da privacidade, avaliações de impacto, eliminação dos dados logo após a utilização, entre outras (ARTICLE WORKING PARTY, 2013, p. 65-66).

Assim, pode-se concluir que o legítimo interesse é uma alternativa de base legal para tratamento de dados disponíveis publicamente através do *data scraping*, desde que a hipótese autorizativa encontre fundamento no teste de proporcionalidade, isto é, desde que o tratamento encontre baliza nas avaliações da legitimidade,

necessidade, balanceamento (proporcionalidade) e adoção de salvaguardas.

No caso de *data scraping* de dados pessoais disponíveis publicamente, como já demonstrado, é necessário buscar o elo entre a nova finalidade e aquela que justificou a publicização do dado para aferição desta compatibilidade, análise esta que integra o teste de proporcionalidade, e também a avaliação de compatibilidade referida na presente pesquisa acerca do tratamento posterior para novas finalidades - hipótese do art. 7º, §7º.

Por isso, compreende-se que a discussão sobre a autonomia da hipótese do § 7º, do art. 7º da LGPD adquira menor relevância, visto que, como exposto anteriormente no que diz respeito aos casos do §§3º e 4º, fundamentando o *data scraping* ou qualquer tratamento de dados disponíveis publicamente na hipótese do art. 7º, inciso IX ou na hipótese do § 7º, o agente de tratamento não se desobriga das demais obrigações previstas na LGPD, e ainda, de uma forma ou de outra, deverá obrigatoriamente avaliar a compatibilidade ou proporcionalidade do processamento, tendo em vista a expectativa do titular e o contexto do tratamento.

4.2 ABORDAGEM NECESSÁRIA PARA CONCEBER UM EQUILÍBRIO ENTRE O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E O *DATA SCRAPING*

O contexto do Big Data ergueu, em âmbito internacional, discussões e questionamentos sobre a aplicação das leis relativas à proteção de dados nos cenários de processamento de dados cada vez mais intensificados que se operam nessa sociedade da informação. E é evidente que o *data scraping* está incluso nesta esfera.

Dentre estes questionamentos estão aqueles que se referem a como conciliar a observância dos princípios, dos fundamentos e dos direitos dos titulares previstos na LGPD com um contexto no qual existem dificuldades triviais, como a de informar o titular acerca da existência de tratamento. Ou ainda, como cumprir a necessidade de informar as finalidades específicas do tratamento ao titular tendo em vista que uma disponibilização de um dado pessoal em uma rede social, por exemplo, abre incontáveis possibilidades de tratamento posterior.

Evidente que não se busca responder todos os contornos de tais problemáticas, porém, ao apresentar a teoria da privacidade contextual, elaborada por

Helen Nissenbaum, propor-se-á uma ampliação da concepção de autodeterminação informativa, de modo a auxiliar a compreensão de como manter o controle do titular sobre o fluxo de seus dados pessoais ao tempo que se abre espaço para a inovação tecnológica e os benefícios que dela decorrem para a sociedade.

Trata-se de um panorama complementar a abordagem da autodeterminação informacional - que, tradicionalmente, se apresenta como sinonímia da ideia de consentimento - com potencial de suprir possíveis lacunas, não devendo ser vista como um substituto de tal abordagem, que continua detendo extrema relevância e aplicabilidade.

4.2.1 Teoria da privacidade contextual e suas implicações para compreensão do contexto de processamento intenso e ágil de dados no sistema de proteção de dados pessoais nacional

A autodeterminação informacional refere-se ao direito do indivíduo de autodeterminar as suas informações pessoais, isto é, de exercer controle sobre o trânsito de dados relativo ao próprio titular (VAINZOF, 2020, p. 24-26). Para Rodotà, trata-se de um poder permanente de controlar seus próprios dados (RODOTÀ, 2008).

A estratégia regulatória da proteção de dados pessoais baseada no consentimento, fundada no racional da autodeterminação informacional, é robusta e figura como central em parte da produção teórica e empírica (BIONI, 2019, 210-211). E recorre-se à eleição do consentimento do titular de dados pessoais como técnica legislativa para permitir esse controle. Por meio desse consentimento, o titular emite autorizações sobre o fluxo dos seus dados pessoais (BIONI, 2019, 238).

A abordagem da autodeterminação informativa funda-se nos princípios da especificação da finalidade e no consentimento, a partir dos quais surge o princípio da limitação dos propósitos - *purpose limitation principle* - que impõe que o uso dos dados pessoais limite-se a finalidade autorizada, sendo que em caso de qualquer outro uso haveria necessidade de obtenção de um novo consentimento (BIONI, 2019, p. 238-239).

Todavia, a perspectiva materializada pela ideia tradicional da autodeterminação informativa, possui problemáticas como: (i) gerar uma fadiga do consentimento devido a sobrecarga de exigência desta autorização do titular de dados

para cada tratamento que se processar, se esta fosse a única estratégia normativa (TAVARES, 2022, p. 212); e (ii) prejudicar a inovação e as novas tecnologias ou negócios que envolvam tratamento de dados pessoais, diante da dificuldade de *presentificar* as finalidades específicas de uso dos dados pessoais dentro do contexto da inovação na economia dos dados (BIONI, 2019, p. 273).

Tais problemáticas geram grandes implicações no contexto do *Big Data*, o que inclui o *data scraping*, já que se desenvolveu maior capacidade de reutilização da mesma base de dados para propósitos diferentes. A questão é que, neste contexto, muitas vezes, não se sabe e nem seria possível, ao momento da coleta do dado, delimitar especificamente as finalidades do tratamento. Como seria possível limitar a utilização do dado a uma finalidade específica se a própria tecnologia objetiva alargar estes possíveis usos? (BIONI, 2019, p. 240).

Assim, a abordagem tradicional da autodeterminação informacional, balizada pelos princípios da especificação e limitação dos propósitos, demonstra incompatibilidade com este novo contexto. O tratamento automatizado e secundário de dados pessoais para novas finalidades, acelerado pelo contexto do *Big Data*, o que inclui, em especial, dados disponíveis publicamente, reclama ser vislumbrado por outra perspectiva.

Esclarece-se aqui que não se busca propor uma solução para tais cenários, mas sim expor a possibilidade de analisar a proteção de dados a partir de outras perspectivas, e não somente aquela tradicional referente ao paradigma da autodeterminação informativa, ou seja, propõe-se o emprego de outros relatos normativos para conceber um equilíbrio entre a proteção de dados e os fenômenos do processamento automatizado de dados e outros decorrentes do Big Data, que impedem uma *presentificação* das finalidades de processamento. Através da perspectiva que se propõe a seguir, busca-se uma forma de assegurar os interesses dos titulares, seus direitos e liberdades individuais, de modo que os titulares mantenham domínio sobre seus dados pessoais, ao tempo que possibilita a inovação e os avanços tecnológicos, desde que se observe certos fatores.

Nesse sentido, a proposta de Helen Nissenbaum mostra-se um referencial teórico com potencial para ser considerado como alternativa ao relato normativo utilizado tradicionalmente. Inclusive, a autora compreende mais amplamente o conceito de privacidade, para além da abordagem de privacidade como o direito do indivíduo de limitar, consentir ou controlar diretamente o fluxo de suas informações

(NISSENBAUM, 2010, p. 2):

> [...] [muitos] argumentam que proteger a privacidade significa estritamente limitar o acesso à informação pessoal ou garantir o direito das pessoas de controlar as informações sobre si mesmas. Eu discordo. O que as pessoas mais se preocupam não é simplesmente restringir o fluxo de informações, mas assegurar que ele flua apropriadamente [...].

A autora propõe, então, que, para a aferição do fluxo informacional como apropriado ou inapropriado, seja aplicado o *framework* da integridade contextual[40] (NISSENBAUM, 2010, p. 127). Tal modelo fornece uma descrição dos fatores que determinam quando os indivíduos poderão considerar novas tecnologias ou sistemas de informação como ameaças à privacidade (NISSENBAUM, 2010, p.2).

A intelecção do que está dentro da esfera do apropriado decorre do *contexto* de cada relação na qual as informações pessoais fluem, isto é, de cada contexto do fluxo informacional. A partir dessa análise, por meio da qual deve-se extrair uma linguagem informacional, torna-se exequível a avaliação da *integridade* do tráfego dos dados pessoais (BIONI, 2019, p. 245-246). A chave na construção deste *framework* da integridade contextual, portanto, são as normas informacionais que decorrem de um exame cuidadoso do *contexto* (BIRNHACK, 2011, p. 20).

Para o exame do contexto, Helen Nissenbaum direciona a análise dos seguintes fatores: (i) o tipo da informação, (ii) as partes, que são tanto os sujeitos da informação como quem está a enviando ou recebendo, e (iii) os princípios que baseiam a transmissão da informação (NISSENBAUM, 2010, p. 141). Nas palavras de Bruno Bioni, tais elementos foram traduzidos como (i) atores, (ii) atributos (tipo) do dado pessoal e (iii) forma com que é disseminado (BIONI, 2019, p. 213).

Assim, cada contexto tem uma linguagem informacional, que impõe uma lógica ao fluxo informacional, em relação (i) aos tipos de informações trocadas (ii) entre emissário e recipiente, e em relação (iii) aos terceiros que podem ingressar neste fluxo (BIONI, 2019, p. 213-214).

---

[40] Importante destacar que Nissenbaum busca se distanciar em propor uma teoria de privacidade. Nas palavras da autora: "The framework of contextual integrity is an account of these social determinants (not a full-blown theory of privacy" (p. 189). A autora define o framework da privacidade como "[...] a justificatory framework for establishing whether sociotechnical devices, systems, and practices affecting the flow of personal information in society are morally and politically legitimate. Although, as such, it is neither a theory of a legal right to privacy nor a definition of a legal concept of privacy, it can serve as a foundation for law and regulation by providing a standard against which legislation (existing or proposed) and detailed rules are tested." (p. 236).

Consequentemente, cada contexto designa as expectativas do titular das informações, depositadas ao recipiente, de como o fluxo informacional fluirá. Essas expectativas do titular, decorrentes do contexto do fluxo informacional, fazem com que, por exemplo, o paciente não espere que seu médico troque informações com seu empregador e que este informe rendimentos e atribuições profissionais para fins da prestação de atendimento médico; ou faz com que o aluno não repasse confidências amorosas ao seu professor (BIONI, 2019, p. 214-215).

Reunindo-se as informações necessárias, ou seja, os fatores contextuais - incluindo atores, tipo da informação e para quais terceiros a informação é transmitida - torna-se possível verificar a integridade contextual do fluxo informacional (BIONI, 2019, p. 238), cuja avaliação caberá ao agente de tratamento.

Como conclusão da teoria da privacidade contextual[41], tem-se que o fluxo de dados pessoais não ocorre no vácuo, mas sim "sob um conjunto de circunstâncias que determinam sua integridade" (BIONI, 2019, p. 216). Através da análise contextual, calibra-se quais as expectativas do titular de dados e compreende-se os parâmetros para que o fluxo informacional respeite a integridade contextual. A conclusão é que, existindo um fluxo informacional íntegro, o cidadão continua exercendo domínio sobre seus dados pessoais, mesmo sem ter declarado sua vontade, pois a integridade contextual pressupõe o respeito às expectativas do titular (BIONI, 2019, p. 215-216).

Assim, considerando a proteção de dados como direito da personalidade, que possui valor social, e tendo em conta a negociabilidade limitada característica dos direitos da personalidade, compreende-se que a perspectiva proposta pela teoria da privacidade contextual completa o paradigma da determinação informacional e localiza-se como uma alternativa para que não se deixe somente para os indivíduos a carga da proteção dos dados pessoais. A privacidade contextual, em resumo, amplia as perspectivas normativas para solucionar casos que o consentimento não dá conta de decifrar (BIONI, 2019, p. 256).

A teoria da privacidade contextual, portanto, adiciona relevantes contornos ao tratamento de dados pessoais disponíveis publicamente, assim como à aplicação da base legal do legítimo interesse. Ao unir o legítimo interesse com o novo paradigma

[41] Apesar de referir-se ao modelo apresentado por Helen Nissenbaum como uma teoria, Bruno Bioni trata de esclarecer que "utiliza-se o termo 'privacidade contextual' como um processo de decisão heurística, cujo centro de análise não está focado em capturar significado completo da privacidade, mas identificar como sucedem violações a tal direito". (BIONI, 2019, p. 212).

que se cria a partir da teoria da privacidade contextual demonstra-se como a autodeterminação informativa vai além do consentimento (BIONI, 2019, p. 267-270). Isso porque o cidadão também exerce domínio sobre seus dados, desde que sejam tratados com *previsibilidade*, de acordo com suas legítimas expectativas, elemento pelo qual se chega através de uma análise *contextual* (BIONI, 2019, p. 268).

Similarmente ocorre em relação ao tratamento de dados pessoais disponíveis publicamente. Ao garantir proteção a esta categoria de dados pessoais, a lei supera a dicotomia entre público e privado, e a forma com que o faz implica na aplicação da privacidade contextual. A aferição de licitude do tratamento, tanto com base no § 3º como no caso do § 4º, requer uma análise *contextual* para calibrar quais as legítimas expectativas do titular a fim de observar o princípio da boa-fé e da confiança, além de balizar a avaliação da equivalência da finalidade com aquela que motivou a publicização (TAVARES, p. 106 e 150).

Em relação ao § 7º, a análise contextual também ganha importante papel. Inclusive, o próprio parecer do Grupo de Trabalho do Artigo 29, ao dispor dos critérios da avaliação de compatibilidade entre a finalidade original e a finalidade posterior do tratamento, prevê a análise do *contexto* no qual os dados foram coletados e as expectativas do titular quanto sua utilização posterior (TAVARES, 2022, p. 200-201).

Com isto posto, conclui-se que o *data scraping*, como um dos possíveis tratamentos dentro do contexto do *Big Data* e dos processamentos automatizados e massivos, não escapa da necessidade de passar por uma análise contextual e de observar o paradigma da privacidade contextual como alternativa ao tradicional escopo da autodeterminação informativa, visto que, ao ter em conta a *integridade contextual*, o titular mantém domínio sobre seus dados, ainda que sem declarar sua vontade.

Portanto, a bagagem normativa da privacidade contextual mostra-se de extrema utilidade ao dar uma roupagem mais ampla para a autodeterminação informativa, de modo a proporcionar maior flexibilidade. Tal teoria consegue equilibrar a dificuldade em *presentificar* os propósitos dentro do contexto do *Big Data* com os meios para governar e delimitar tais usos para os dados pessoais e garantir um fluxo informacional íntegro ao valor social da privacidade. Foca-se em uma normativa *ex ante* para empoderar o titular de dados com o controle dos seus dados (BIONI, 2019, p, 274-275), para além do momento em que clica no botão "*li e aceito os termos de uso*".

5 CONCLUSÕES

É fato que as evoluções nas tecnologias da informação e comunicação, em especial no contexto do *Big Data*, tornou possível avanços no processamento de dados e possibilitou o crescimento de diversos modelos de negócios baseados no tratamento de dados - inclusive os pessoais -, como os chamados *data brokers*.

Deste contexto, decorrem diversos impactos e prejuízos relativos ou tangenciais à proteção de dados pessoais que se tornam objeto de preocupação. Dentre eles: a discriminação decorrente do perfilamento dos indivíduos, o descumprimento da finalidade informada ao titular no momento da coleta, a inferência de dados de caráter sensível do titular, e outros.

Alguns casos citados ao longo desta pesquisa que demonstram esses riscos são: o caso da Clearview AI, que não conseguiu demonstrar o cumprimento do princípio da finalidade no tratamento de dados pessoais que realizava, a observância das legítimas expectativas do titular, e a indicação de base legal adequada ao tratar dados sensíveis, no caso, biométricos; e o caso da Cambridge Analytica, que foi paradigmático para demonstrar como o tratamento indevido de dados pessoais pode ter o condão de influenciar processos eleitorais e o próprio regime democrático.

Diante da relevância e atualidade do tema, portanto, tratou-se de buscar delimitar quais os parâmetros legais impostos pela Lei Geral de Proteção de Dados para a prática de *data scraping*, que se insere no contexto de inúmeras organizações que, por algum motivo, coletam dados da *web* de modo automatizado.

Para isso, inicialmente foi traçado: (i) um apanhado histórico e da evolução conceitual das ideias sobre privacidade e proteção de dados, de modo a traçar similitudes e diferenças entre as duas acepções; (ii) um panorama da privacidade e da proteção de dados pessoais no contexto nacional, até a promulgação da Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e (iii) os conceitos basilares insculpidos pela LGPD.

Demonstrou-se como o nascimento da ideia de privacidade guarda estreita relação com a percepção de um direito de estar só ou de escolher quais informações guardar da esfera pública. Todavia, o desenvolvimento da sociedade informacional

gerou a necessidade de um novo olhar sobre o direito da privacidade, visto que a acepção anterior não dava conta de proteger de modo amplo a dignidade da pessoa humana no contexto cada vez mais ágil e massivo do processamento de dados. Assim, o que se desenvolve, modernamente, é uma concepção mais ampla sobre o direito à privacidade que envolve o controle do indivíduo sobre o fluxo dos seus dados pessoais e a imposição de deveres aos agentes de tratamento para que se tutelasse todo o fluxo de dados pessoais do titular. O direito à privacidade passa a desdobrar-se em torno do dado pessoal.

Assim, com o crescimento das preocupações acerca do processamento de dados pessoais dos indivíduos, desenvolveram-se inovações legislativas que centravam-se na proteção dos dados pessoais dos indivíduos. Tais leis são divididas em quatro gerações, sendo que cada geração demonstra uma mudança de paradigma quanto à própria ideia sobre proteção dos dados pessoais.

Da evolução observada nas gerações de leis mencionadas, contempla-se a diferença entre o direito à privacidade e o direito de proteção de dados pessoais. O primeiro ampliou-se ao ponto de não ser mais mero sinônimo para o direito de estar só, e sim para ser encarado como um direito ao controle dos dados pessoais, o qual perpassa o direito do indivíduo de não sofrer interferências alheias e o direito de controlar suas informações pessoais, o que necessita de uma proteção dinâmica ao longo de todo o fluxo de dados.

O direito à proteção de dados, por sua vez, diferentemente da privacidade, supera a dicotomia entre público e privado. Independentemente de se tratar de informação de natureza pública ou privada, a Lei Geral de Proteção de Dados acoberta ambos os casos, isto é, o direito à proteção de dados garante proteção jurídica, inclusive àquela informação que não é mais considerada privada.

Acerca do panorama nacional sobre a temática, apresenta-se visão da doutrina de como o direito de proteção de dados, mesmo que há pouco tempo não constasse na Constituição Federal de forma expressa, poder-se-ia ser vislumbrado como um direito fundamental.

Em observância à crescente relevância do tema, recentemente o direito à proteção de dados pessoais foi alçado ao status de direito fundamental, passando a constar de forma expressa no inciso LXXIX do art. 5º da Constituição Federal, não deixando dúvidas sobre a relevância e o protagonismo da proteção de dados como meio para garantir a dignidade da pessoa humana na sociedade atual.

Ainda, anteriormente à LGPD, outras legislações infraconstitucionais tangenciam o tema, demonstrando que a proteção de dados pessoais não se trata de pauta recente no Brasil. Evidente que, com a promulgação da LGPD, houve de fato uma sistematização da proteção de dados no país e uma centralização de disposições acerca do tema, que anteriormente se mostravam excessivamente esparsas e sem sistemática.

Para estruturar um sistema de proteção de dados, a legislação pátria inspirou-se na *General Data Protection Regulation* (GDPR), e tratou de estabelecer alguns conceitos e parâmetros fundamentais sobre a matéria na legislação pátria, no caso, na LGPD.

A fim de delinear os limites do objeto desta pesquisa foi preciso, em seguida (i) tratar do conceito de *data scraping*, sua intensificação no contexto do *Big Data*, e seus impactos e prejuízos à privacidade e à proteção de dados pessoais; (ii) delimitar conceitos para o dado pessoal de acesso público e dado tornado manifestamente público pelo titular, tendo como base, inclusive, o entendimento de autoridades de proteção de dados internacionais sobre o assunto, para que se compreendesse em quais casos de fato haveria um tratamento dos chamados dados disponíveis publicamente - termo utilizado nesta pesquisa para se referir a ambas as categorias, em conjunto, anteriormente citadas - e (iii) traçar quais os requisitos gerais, necessários para qualquer tratamento de dados pessoais, e em especial, os requisitos específicos dispostos nos §§3º, 4º e 7º do art 7º da LGPD, exigidos, respectivamente, para o tratamento equivalente de dados de acesso público, tratamento equivalente de dados pessoais tornados manifestamente públicos pelo titular, e tratamento posterior para novas finalidades de dados disponíveis publicamente.

O *data scraping* pode ser conceituado, de modo geral, como uma técnica pela qual se coleta dados da *web* de modo automatizado. Os dados pessoais de acesso público, por sua vez, são aqueles que são de livre acesso ao público geral, que foram divulgados por terceiros - que não o próprio titular - e que ainda possuem uma obrigação legal de publicidade vinculada aos mesmos. Por fim, os dados pessoais manifestamente públicos pelo titular precisam ter sido divulgados através de ato consciente do próprio titular e estarem acessíveis de modo irrestrito.

Desse modo, tendo havido uma delimitação desses conceitos torna-se possível o reconhecimento do âmbito de aplicação dos requisitos para o tratamento de dados disponíveis publicamente.

Os requisitos impostos pelo §3º do art. 7º envolvem, em especial, a observância (i) da boa-fé objetiva: que impõe que o tratamento de dados pessoais esteja pautado na ética e em padrões objetivos de lealdade; (ii) da finalidade: que exige que os propósitos do tratamento sejam legítimos, específicos e explícitos, e ainda, no caso, sejam equivalentes ao que justificou a disponibilização do dado; (iii) do interesse público: no caso, o que motivou a publicização do dado.

Os requisitos que devem ser observados para hipótese do §4º do art. 7º são (i) a análise contextual do tratamento, pela qual avaliam-se princípios como o da finalidade e da boa-fé, em semelhança ao caso do §3º; (ii) a observância dos princípios da Lei e (iii) a garantia dos direitos dos titulares; sendo que estes dois últimos requisitos constituem, conforme demonstrado nesta pesquisa, requisitos gerais que devem ser observados em qualquer tipo de tratamento de dados pessoais.

Por sua vez, os requisitos a serem cumpridos para hipótese do § 7º do art. 7º são a observância (i) de propósitos legítimos e específicos, (ii) da compatibilidade da finalidade original com a nova que se pretende empregar, (iii) dos fundamentos da Lei (iv) dos princípios insculpidos pela LGPD e (v) dos direitos dos titulares.

Quando cumpridos os seus requisitos específicos - claro que conjuntamente com os requisitos gerais -, serão aplicáveis as hipóteses estudadas nesta pesquisa dos §§3º, 4º ou 7º, do art. 7º da LGPD.

Por fim, (i) propõe-se alguns níveis de avaliação, como uma consequência da delimitação dos demais requisitos, para se chegar a uma conclusão sobre a base legal a fundamentar a prática de *data scraping* voltada à dados disponíveis publicamente e (ii) apresenta-se uma abordagem fundamental para conceber um equilíbrio entre as práticas cada mais comuns no *Big Data*, o que inclui o *data scraping*, com os direitos e liberdades fundamentais do titular de dados e o merecido controle sobre seus próprios dados pessoais.

A proposta de níveis de avaliação para compreensão de qual a base legal mais indicada consiste em analisar quatro aspectos, e a depender das respostas, traça-se uma sugestão de qual seria a base legal mais adequada: (i) Análise da equivalência ou compatibilidade da finalidade; (ii) Análise da categoria de dados pessoais; (iii) Análise dos requisitos gerais e específicos; (iv) Em caso de incompatibilidade ou ausência de requisito específico, parte-se para análise de adequação em alguma das demais bases legais.

Levou-se em consideração, para a proposição dos quatro níveis de avaliação

para indicação da base legal, a possibilidade de compreensão das hipóteses do §§3º 4º e 7º do art. 7º da LGPD como bases autônomas. Ainda, aprofundou-se na base legal do legítimo interesse, tendo em vista sua relevância para fundamentação do *data scraping* como opção diversa da base legal do consentimento, buscando-se, em especial, estabelecer quais seus parâmetros e quais os limites a serem observados para que a utilização desta hipótese autorizativa seja, de fato, cabível.

Por fim, apresentou-se a teoria da privacidade contextual, proposta por Helen Nissenbaum, para apresentar um referencial teórico complementar relevante para se equilibrar a garantia de controle do titular sobre as informações pessoais de sua titularidade com as novas formas de tratamento de dados pessoais, atreladas ao contexto do *Big Data*. Conclui-se, portanto, que o controle do titular sobre os dados pessoais não deve ser centralizado somente na perspectiva da autodeterminação informacional como sinonímia de consentimento. Isso porque, em algumas circunstâncias, a aplicação deste instituto não será exequível ou sua obtenção será excessivamente onerosa. Assim, com base em tal teoria, torna-se possível compreender que havendo integridade contextual durante o fluxo informacional dos dados pessoais, o que requer à observância de certas regras, o titular continua exercendo seu controle sobre seus dados pessoais, ainda que sem ter explicitado sua vontade, pois respeitam-se suas legítimas expectativas.

Essa perspectiva pode ser aplicada, com as devidas cautelas, no tratamento de dados disponíveis publicamente, inclusive na prática de *data scraping*. Desse modo, é importante esclarecer que uma abordagem com base na teoria da privacidade contextual está longe de se tratar de cheque em branco, pelo contrário, a teoria ganha espaço complementar como uma abordagem que amplia a própria acepção de autodeterminação informacional, transpondo a ideia tradicional de que a autodeterminação informacional vincula-se quase como sinonímia de consentimento. Com isso, a análise da integridade do fluxo informacional pode demonstrar-se como pertinente ferramenta que torna possível a garantia dos direitos dos titulares ao tempo que não inibe a inovação por completo. Assim, ainda que não se tenha uma expressa manifestação da vontade do titular, enquanto se olhar para a integridade contextual manter-se-á um respeito às legítimas expectativas do titular, e, consequentemente, uma compatibilidade e proporcionalidade nas finalidades.

REFERÊNCIAS

AMARAL, Diogo Freitas do. **Curso de Direito Administrativo**, 10ª reimpressão. Coimbra: Almedina, 2001. Vol. II.

ARTICLE 29 DATA PROTECTION WORKING PARTY. Directive 95/46/EC, 00569/13/EN/WP203 [The working party on the protection of individuals with regard to the processing of personal data. Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995. European Commission, Directorate General Justice, Brussels, Belgium]. **Opinion 03/20113 on purpose limitation**, Adopted on 02 April 2013.

AXCIOM. **GDPR Privacy Notice**. 2018. Disponível em https://www.acxiom.com/about-us/privacy/gdpr/. Acesso em: 04 de mar de 2022.

AZAMBUJA, Antonio João Gonçalves de; GRANVILLE, Lisandro Zambenedetti; SARMENTO, Alexandre Guilherme Motta. **A privacidade, a segurança da informação e a proteção de dados no *Big Data.*** Parc. Estrat. Brasília, DF, v. 24, n. 48, p. 9-32, jan.-jun. 2019. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/914/831. Acesso em: 04 mar. 2022.

BAIÃO, Renata Barros Souto Maior; TEIVE, Marcelo Muller. **O artigo 23 da LGPD como base legal autônoma para o tratamento de dados pessoais pelo poder judiciário**. In: PALHARES, Felipe. Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil; Revista dos Tribunais, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed., Revista, Atualizada e Reformulada. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo (org.). **Proteção de dados**: contexto, narrativas e elementos fundantes [livro eletrônico]. São Paulo, SP: B. R. Bioni Sociedade Individual de Advocacia, 2021. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1629122366livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf. Acesso em: 04 mar. 2022.

BIONI, Bruno Ricardo; MENDES, Laura Schertel. O regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. *In:* BIONI, Bruno Ricardo (org.). **Proteção de dados**: contexto, narrativas e elementos fundantes [livro eletrônico]. São Paulo, SP: B. R. Bioni Sociedade Individual de Advocacia, 2021. p. 362-393. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1629122366livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf. Acesso em: 04 mar. 2022.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques. A construção multissetorial da LGPD: história e aprendizados. *In:* BIONI, Bruno Ricardo (org.). **Proteção de dados**: contexto, narrativas e elementos fundantes [livro eletrônico]. São Paulo, SP: B. R. Bioni Sociedade Individual de Advocacia, 2021. p. 15-58. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1629122366livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf. Acesso em: 04 mar. 2022.

BRACHER, Paulo Marcos Rodrigues; KUJAWSKI, Fabio Ferreira; CASTELLANO, Ana Carolina Heringer Costa. Princípios gerais de proteção de dados pessoais: uma análise dos princípio elencados no art. 6º da Lei nº 13.709/2018 (LGPD). *In*: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia (coord.). **Proteção de Dados Pessoais no Brasil**: uma nova visão a partir da Lei nº 13.709/2018. Belo Horizonte: Fórum, 2019. p. 63-85.

BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. *In*: MULHOLLAND, Caitlin (Org.). **A LGPD e o novo marco normativo no Brasil.** Porto Alegre, RS: Arquipélago editorial, Edição Kindle, 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Presidência da República. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 12 de Setembro de 1990, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 04 mar. 2022.

BRASIL. Supremo Tribunal de Justiça. **RE 418.416** - Santa Catarina. Relator: Min. Sepúlveda Pertence – Tribunal Pleno. Data de Julgamento: 10 maio 2006. Diário da Justiça: Seção 1, Brasília, DF, de 02 fev. 2007, p. 74, Ement. V. 02262-03, p. 545.

BRASIL. Presidência da República. **Lei nº 12.527, de 18 de novembro de 2011a**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 18 de Novembro de 2011, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 04 mar. 2022.

BRASIL. Presidência da República. **Lei nº 12.414, de 09 de junho de 2011b**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 10 de Junho de 2011, p. 2. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 04 mar. 2022.

BRASIL. Presidência da República. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a Proteção de Dados Pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018, n. 157, Seção 1, p. 59. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 mar. 2022.

BRASIL. Congresso Nacional. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 11 fev. 2022, Ed. 30, Seção 1, p. 2. Disponível em: https://in.gov.br/en/web/dou/-/emenda-constitucional-n-115-379516387. Acesso em: 04 mar. 2022.

BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD Nº 2, de 27 de janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 28 jan. 2022, Ed. 20, Seção 1, p. 6. Disponível em: https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019. Acesso em: 04 mar. 2022.

COMMISSION NATIONALE DE l'INFORMATIQUE ET DES LIBERTÉS. **Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI**. 2021. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_med_2021-134.pdf. Acesso em: 04 de mar. 2022.

CONTROLADORIA-GERAL DA UNIÃO (CGU). Secretaria de Prevenção da Corrupção e Informações Estratégicas. **Manual da Lei de Acesso à Informação para Estados e Municípios**. Brasília, DF: CGU, 2013.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. São Paulo, SP: Thomson Reuters; Revista dos Tribunais, 2018. 264p.

COUNCIL OF EUROPE. **European Court of Human Rights**. Roma, Itália, 04 de novembro de 1950. Disponível em: https://www.echr.coe.int/documents/convention_eng.pdf. Acesso em: 03 mar. 2022.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro, RJ: Renovar, 2006.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade a proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. Revista e atualizada. São Paulo, SP: Thomson Reuters Brasil; Revista dos Tribunais, 2021.

DONEDA, Danilo *et al.* **Tratado de Proteção de dados pessoais**. Rio de Janeiro, RJ: Forense, 2021. 743p.

EUROPEAN PUBLIC SERVICE UNION (EPSU). **The General Data Protection Regulation (GDPR):** an EPSU Briefing. May 2018. Disponível em: https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf. Acesso em: 03 mar. 2022.

FERRAZ JR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Rev. Fac. Direito Univ. São Paulo, São Paulo, SP, v. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 03 mar. 2022.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. **Privacidade e proteção de dados pessoais: perspectiva histórica**. InCID: Revista de Ciência da Informação e Documentação, Ribeirão Preto/SP, v. 12, n. 2, p. 151-172, 2021. DOI: 10.11606/issn.2178-2075.v12i2p151-172

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wéverton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. *In*: LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. Edição Kindle, São Paulo: Almedina, 2020.

FOITZIK, Piotr. **Publicy available data under the GDPR**: main considerations. IAPP - The Privacy Advisor, May 2019. Disponível em: https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/#:~:text=In%20general%2C%20processing%20of%20publicly,some%20data%20might%20be%20relevant). Acesso em: 03 mar. 2022.

FORTES, Vinícius Borges. Convergências conceituais para os direitos de privacidade na internet e a proteção dos dados pessoais. *In*: PIRES, Cecília Maria Pinto; PAFFARINI, Jacopo; CELLA, José Renato Gazziero (org.). **Direito, Democracia e Sustentabilidade**: Programa de Pós-Graduação *Stricto Sensu* em Direito da Faculdade Meridional. Erechim, RS: Deviant, 2017. Cap. 13, p. 271-291. Disponível em: https://www.editoradeviant.com.br/wp-content/uploads/woocommerce_uploads/2017/07/Direito-Democracia-e-Sustentabilidade-Programa-de-Pos-Graduacao-Stricto-Sensu-em-Direito-da-Faculdade-Meridional.pdf. Acesso em: 03 mar. 2022.

GLASSMAN, Guillermo. Interfaces entre o dever de transparência e a proteção dos dados pessoais no âmbito da Administração Pública. *In*: DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (coord.). **LGPD e a Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

GLEZ-PEÑA, Daniel *et al.* **Web scraping technologies in an API world.** Briefings in Bioinformatics. v. 15, n. 5, p. 788-797, 2013. DOI: 10.1093/bib/bbt026.

GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados Pessoais**: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre, RS: Editora Fi, 2020. 455p.

HIRSCHEY, Jeffrey Kenneth. **Symbiotic relationships:** pragmatic acceptance of data scraping. Berkeley Tech. L. J., v. 29, n. 4, p. 897-927, 2014. DOI: 10.15779/Z38B39B.

INFORMATION COMISSIONER'S OFFICE (ICO). **What are the conditions for processing?** 2022. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#:~:text=%E2%80%9Cprocessing%20is%20necessary%20for%20reasons,and%20the%20interests%20of%20the. Acesso em: 03 mar. 2022.

JUSBRASIL. **Política de Privacidade**. 2020. Disponível em: https://suporte.jusbrasil.com.br/hc/pt-br/articles/360041534212-Pol%C3%ADtica-dePrivacidade-da-Plataforma-Jusbrasil. Acesso em: 04 de mar. de 2022.

JUSTEN FILHO, Marçal. **Conceito de interesse público e a "Personalização" do Direito Administrativo**. Rev.Trimestral Direito Público, São Paulo, SP, n. 26, p. 115-136, 1999.

KASPA, Lakshmi Prasanna *et al*. **Towards extended Data Mining:** an examination of technical aspects. Procedia Comput Sci. Amsterdan, v. 139, n. 2018, p. 49-55, 2018. DOI: https://doi.org/10.1016/j.procs.2018.10.216.

LEONARDI, Marcel. **Legítimo interesse**. Rev. Adv. São Paulo, SP, Ano XXXIX, n. 144, p. 67-73, Nov. 2019. Disponível em: https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/70/index.html#zoom=z. Acesso em: 03 mar. 2022.

LIU, Han-Wei. **Two decades of laws and practice around screen scraping in the common law world and its open banking watershed moment**. Washington Internacional L. J. v. 30, n. 1, p. 28-62, Dec. 2020. Disponível em: https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1858&context=wilj. Acesso em: 03 mar. 2022.

MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18)**. Goiânia, GO: RM Digital Education, 2019. 142 p.

MARCACINI, Augusto Tavares Rosa. Regras Aplicadas ao Tratamento de Dados Pessoais. *In*: LIMA, Cintia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. Edição Kindle, São Paulo: Almedina, 2020.

MARTINS, Renata Duval. Princípios da Lei Geral de Proteção de Dados: desenvolvimento normativo no Brasil e análise conceitual. *In*: PINTO, Danielle Jacon Ayres; ROVER, Aires Jose; PEIXOTO, Fabiano Hartmann. **Direito, governança e novas tecnologias II** [Recurso eletrônico on-line]. Florianópolis: CONPEDI, 2020. Disponível em: http://conpedi.danilolr.info/publicacoes/olpbq8u9/lxxdq7f2. Acesso em: 04 mar. 2022.

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo, SP: Thomson Reuters Brasil; Revista dos Tribunais, 2019.

MATTIUZO, Marcela; FAVARO. Iasmine Lima. Dados manifestamente públicos e dados não sujeitos à LGPD: Diferenciando conceitos e estabelecendo parâmetros. *In*: FRAZÃO, Ana; CUEVA (coord.), Ricardo Villas Bôas (coord.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil; Revista dos Tribunais, 2021.

MENDES, Laura Schertel. **O direito fundamental à proteção de dados pessoais.** Rev. Direito do Consumidor, v. 20, n. 79, p. 45-81, jul./set. 2011.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo, SP: Saraiva, 2014. -(Série IDP: linha pesquisa acadêmica).

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coord.). **Lei Geral de Proteção de Dados**: São Paulo: Revista dos Tribunais, Nov. 2019. – (Caderno Especial). p. 35-56.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Rev. Direito Consumidor, São Paulo, v. 120, ano 27, p. 469-483, nov.-dez. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116/991. Acesso em: 04 mar. 2022.

MOREIRA, André de Oliveira Schenini. **A exceção dos dados pessoais tornados manifestamente públicos pelo titular.** Migalhas. 07 Jan. 2019. Disponível em: https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd. Acesso em: 04 mar. 2022.

NEOWAY. **Manual Básico de LGPD**. 2021. Disponível em: https://f.hubspotusercontent10.net/hubfs/7323764/files/pdf/neoway-lgpd-manual0902.pdf?hsCtaTracking=e15c3a76-256a-433c-8528-bcb79fb9c7bd%7C531c95f7-4c1c-4fe1-88d6-7dc6537c47fb. Acesso em: 04 de mar. de 2022.

NISSENBAUM, Helen Fay. **Privacy in context**: **technology, policy, and the integrity of social life**. Stanford: Stanford University Press, 2010.

OBSERVATÓRIO. 2018: **Uma conjunção astral.** Memória do Observatório: Episódio 3/5. 2022. Disponível em: https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/. Acesso em: 04 mar. 2022.

OFFICE OF THE AUSTRALIAN INFORMATION COMISSIONER. **Comissioner initiated investigation into Clearview AI**, Inc. CII20/00006, 14 de out. 2021. Disponível em: http://www.austlii.edu.au/cgibin/sign.cgi/au/cases/cth/AICmr/2021/54. Acesso em: 04 de mar. 2022

OLIVEIRA, Jaqueline Simas de. **Google é multado em 50 milhões de euros na França por violação ao GDPR**: notas sobre a decisão e lições relevantes para a prática brasileira. JOTA, Opinião & Análise, Dados Pessoais [Internet]. 24 de janeiro de 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/google-e-multado-em-50-milhoes-de-euros-na-franca-por-violacao-ao-gdpr-24012019. Acesso em: 03 mar. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**: Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III), New York, USA, 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 03 mar. 2022.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 (LGPD)**. 2. ed. São Paulo, SP: Saraiva Educação, 2020. 152p.

RODAS, Sérgio. **Constitucionalização da proteção de dados é marco e aumenta segurança jurídica.** Consultor Jurídico. Preservação da privacidade [online]. 11 de fevereiro de 2022. Disponível em: https://www.conjur.com.br/2022-fev-11/constitucionalizacao-protecao-dados-marco-aumenta-seguranca. Acesso em: 03 mar. 2022.

RODOTÀ, Stefano. **Vida na Sociedade da Vigilância**: à privacidade hoje. Rio de Janeiro, RJ: Renovar, 2008. 381p.

RODRIGUES, Wagner de Oliveira; ROCHA, Vanderson Barbosa da. **Dados pessoais no Brasil**: normativas e diálogos institucionais rumo à atual Lei Geral de Proteção de Dados Pessoais. Rev. Direito Civil, Jundiaí, SP, v. 3, n. 2, p. 43-72, jul./dez. 2021. Disponível em: https://revistas.anchieta.br/index.php/RevistaDirCivil/article/view/1811/1597. Acesso em: 03 mar. 2022.

RUARO, Regina Linden; MAÑAS, José Luis Piñar; MOLINARO, Carlos Alberto (org.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre, RS: Editora Fi, 2017.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção de dados pessoais na sociedade da informação**. Direito Estado Soc., Rio de Janeiro, RJ, n. 36, p. 178-199, jan./jun. 2010. DOI: 10.17808/des.36.212. Disponível em: https://revistades.jur.puc-rio.br/index.php/revistades/article/view/212/191. Acesso em: 03 mar. 2022.

RUARO, Regina Lindes; MOLINARO, Carlos Alberto. Conflito real ou aparente de interesses entre o direito fundamental à proteção de dados pessoais e o livre mercado. *In*: RUARO, Regina Linden; MAÑAS, José Luis Piñar; MOLINARO, Carlos Alberto (org.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre, RS: Editora Fi, 2017. p. 13-46.

SÃO PAULO (ESTADO). **Lei nº 5.702/1987, de 5 de junho de 1987**. Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa. São Paulo, SP, 05 de junho de 1987. Disponível em: https://governo-sp.jusbrasil.com.br/legislacao/190377/lei-5702-87. Acesso em: 20 dez. 2021.

SELLARS, Andrew. **Twenty years of web scraping and the computer fraud and abuse act**. Journal of Science & Technology Law (JoSTL). Boston University, v. 24, p. 372-415, 2018. Disponível em: https://scholarship.law.bu.edu/faculty_scholarship/465. Acesso em: 20 dez. 2021.

SERASA EXPERIAN. **Termos de Uso e Política de Privacidade do Serasa.** 2021. Disponível em: https://www.serasa.com.br/app/politica-de-privacidade. Acesso em: 04 mar. 2022.

SILVA, Alexandre Pacheco; LUCCAS, Victor Nóbrega. Público, porém não disponível: os limites de tratamento do dado pessoal público. *In*: RAIS, Diogo; PRADO FILHO, Francisco Octavio de Almeida (coord.). **Direito Público Digital**: o Estado e as novas tecnologias: desafios e soluções. São Paulo: Thomson Reuters Brasil, 2020.

TAVARES, Giovana Milanez. Compliance de dados pessoais disponíveis publicamente: boas práticas para a confirmação da licitude dos dados de acesso público e tornados manifestamente públicos pelo titular. *In*: FRAZÃO, Ana; CUEVA (coord.), Ricardo Villas Bôas (coord.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil; Revista dos Tribunais, 2021.

TAVARES, Giovanna Milanez. **O tratamento de dados pessoais disponíveis publicamente e os limites impostos pela LGPD**. Rio de Janeiro, RJ: Editora Processo, 2022. 256 p.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos arts. 7º e 11. *In:* DONEDA, Danilo *et al*. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 132-162.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo, SP: Thomson Reuters Brasil; Revista dos Tribunais, 2019. 424 p.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. **O consentimento na circulação de dados pessoais**. Rev. Brasileira Direito Civil, Belo Horizonte, MG, v. 25, p. 83-116, jul./set. 2020. DOI: 10.33242/rbdc.2020.03.005.

TRANSUNION. **Trans Union LLC Privacy Notice**. 2021. Disponível em: https://www.transunion.com/privacy/transunion. Acesso em: 04 de mar. de 2022

VAINZOF, Rony. Capítulo 1: Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo, SP: Thomson Reuters, 2019.

WAKKA. Wagner. Facebook é condenado a pagar US$ 5 bilhões por caso Cambridge Analytica. Canal Tech, Internet, Redes Sociais. 24 de julho de 2019. Disponível em: https://canaltech.com.br/redes-sociais/facebook-e-condenado-a-pagar-us-5-bilhoes-por-caso-cambridge-analytica-144841/. Acesso em: 04 mar. de 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 20 dez. 2021.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. *In*: DONEDA, Danilo *et al*. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 271-288.