

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Eleonora Coelho Dozza

USO SECUNDÁRIO DE DADOS PESSOAIS E SEU FUNDAMENTO NO LEGÍTIMO
INTERESSE NO BRASIL PÓS-LGPD

Porto Alegre

2023

ELEONORA COELHO DOZZA

**USO SECUNDÁRIO DE DADOS PESSOAIS E SEU FUNDAMENTO NO
LEGÍTIMO INTERESSE NO BRASIL PÓS-LGPD**

Dissertação de Mestrado apresentada ao programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul, na área de concentração fundamentos da experiência jurídica, como requisito para a obtenção de grau de Mestre em Direito.

Orientador: Prof. Dr. Fabiano Menke

Porto Alegre

2023

FICHA CATALOGRÁFICA

CIP - Catalogação na Publicação

DOZZA, ELEONORA COELHO
USO SECUNDÁRIO DE DADOS E SEU FUNDAMENTO NO
LEGÍTIMO INTERESSE NO BRASIL PÓS-LGPD / ELEONORA
COELHO DOZZA. -- 2023.
128 f.
Orientador: FABIANO MENKE.

Dissertação (Mestrado) -- Universidade Federal do
Rio Grande do Sul, Faculdade de Direito, Programa de
Pós-Graduação em Direito, Porto Alegre, BR-RS, 2023.

1. USO SECUNDÁRIO DE DADOS. 2. LEGÍTIMO INTERESSE.
3. PRINCÍPIO DA FINALIDADE. 4. RELATÓRIO DE IMPACTO À
PROTEÇÃO DE DADOS. I. MENKE, FABIANO, orient. II.
Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

ELEONORA COELHO DOZZA

USO SECUNDÁRIO DE DADOS PESSOAIS E SEU FUNDAMENTO NO LEGÍTIMO
INTERESSE NO BRASIL PÓS-LGPD

Dissertação de Mestrado apresentada ao programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul, na área de concentração fundamentos da experiência jurídica, como requisito para a obtenção de grau de Mestre em Direito.

Porto Alegre, julho de 2023.

BANCA EXAMINADORA

Prof. Dr. Fabiano Menke

Universidade Federal do Rio Grande do Sul

Orientador

Prof. Dr. Cristiano Colombo

Fundação Escola Superior do Ministério Público

Prof. Dr. Rafael de Freitas Valle Dresch

Universidade Federal do Rio Grande do Sul

Profª Pós Dra. Gabrielle Bezerra Sales Sarlet

Pontifícia Universidade Católica do Rio Grande do Sul

AGRADECIMENTOS

Agradeço, primeiramente, ao meu orientador, Professor Dr. Fabiano Menke, pelo seu incentivo, dedicação e acompanhamento ao longo de todo o Mestrado.

Agradeço ao Professor Cristiano Colombo que, com seu cuidado e preocupação, sugeriu uma bibliografia impecável, que engrandeceu esta pesquisa.

Agradeço à Universidade Federal do Rio Grande do Sul(UFRGS), sem a qual este projeto não seria possível, pela oportunidade de aprender com um corpo docente muito qualificado e atento aos seus discentes.

Agradeço ao Centro de Estudos Europeus e Alemães(CDEA) pela oportunidade de realização do Mestrado, pelo apoio financeiro para o estudo da língua alemã e pela viagem de estudos – *Studienreise* - realizada em outubro de 2022, a qual foi muito relevante para a pesquisa e contou com o acompanhamento do Prof. Dr. Draiton Gonzaga de Souza, o qual foi um excelente anfitrião-professor, durante toda a viagem acadêmica.

Agradeço a minha filha e amiga preciosa, Camila Dozza Zandonai, grande e absoluta incentivadora, como ouvinte e leitora dos dilemas jurídicos envolvidos nesta pesquisa. Sem o seu apoio eu não teria retornado aos bancos acadêmicos. Seu suporte, força e determinação foram e são a minha maior inspiração no caminho do conhecimento e da perseverança.

Agradeço a minha mãe, Maria do Horto Vasconcellos Coelho, por me acompanhar com sua firmeza de caráter e otimismo, os quais são um espelho para mim, e por sua compreensão em minhas afastadas horas, dedicadas à pesquisa.

Agradeço a Andressa de Bittencourt, minha amiga, a qual tive a oportunidade de conhecer durante este Mestrado, e que muito colaborou para que esta pesquisa fosse realizada, com sua experiência e sugestões, as quais foram fundamentais para este trabalho.

E por fim, agradeço a todos os meus familiares e amigos que, em algum momento, entenderam a grandeza e a dificuldade de uma dedicação profunda, com momentos de recolhimento.

Muito obrigada a todos!

RESUMO

Este estudo analisa o uso secundário de dados pessoais e seu fundamento no legítimo interesse, especificamente no Direito Civil. A pesquisa está dividida em três partes. Primeiramente, são analisadas as características do tratamento de dados pessoais e o uso secundário de dados e sua relação direta com o princípio da finalidade. Em seguida, trata-se do diálogo principiológico no uso secundário de dados, com a análise do princípio da finalidade, da boa-fé, da base legal do consentimento e do teste da base legal do legítimo interesse. Dessa forma, são investigadas a avaliação do legítimo interesse e o teste de quatro fases, adotado pela Lei Geral de Proteção de Dados (LGPD), além da análise das questões controvertidas em relação à aplicação do legítimo interesse. Posteriormente, é apresentada uma proposta de alteração legislativa da *lege lata a lege ferenda* no que se refere ao art. 38 da LGPD, que trata do relatório de impacto à proteção de dados. Nesse momento, é feita uma comparação entre a LGPD e o General Data Protection Regulation (GDPR), o qual possui situações nas quais o RIPD é obrigatório. Para verificar a importância desse documento, é analisado o relatório de impacto à proteção de dados do TCU. Por fim, propõe-se a alteração legislativa do art. 38 da LGPD, em razão da necessidade de mitigar os riscos do uso posterior de dados pessoais baseado no legítimo interesse.

Palavras-chave: uso secundário de dados. Legítimo interesse. LGPD. Relatório de impacto à proteção de dados.

ABSTRACT

This study aims to analyze the secondary use of personal data and its legal basis in the legitimate interest, specifically in Civil Law. At first, the characteristics of personal data treatment and the secondary use of data are analyzed as well as its straight relation to the purpose limitation principle. Just after, the principiological dialogue and the analysis of the purpose limitation principle is treated as well as the good faith, the legal basis of the consent and the test of legitimate interest assessment. Thus, the legitimate interest assessment and the test of four steps are investigated, which are adopted by Brazilian Data Protection Law (LGPD), besides the analysis of the controversial issues in relation to the legitimate interest uses. Then, a proposal of legal change connected to the article 38 in LGPD from *lege lata* to the *lege ferenda*, which involves the data protection impact assessment is presented. At this moment, a comparison between LGPD and the General Data Protection Regulation, connected to the data protection impact assessment is made because GDPR has some important obligatory situations in the DPIA. To verify the importance of this document, the DPIA Union Accountant Court (TCU) is analyzed. At the end, a legal change of the article 38 at LGPD is proposed, because of the need of risk mitigation in relation to the secondary use of data based on the legitimate interest.

Key-words: secondary use of data. Legitimate interest. LGPD. Data protection impact assessment.

SUMÁRIO

1 INTRODUÇÃO	09
2 TRATAMENTO DE DADOS PESSOAIS E USO SECUNDÁRIO DE DADOS	14
2.1 Dado pessoal e informação.....	19
2.2. Aspectos do termo “informação relacionada a”.....	26
2.3 Aspectos do termo “pessoa natural identificada ou identificável”.....	34
2.4 Uso secundário de dados pessoais.....	39
3 DIÁLOGO PRINCIPIOLÓGICO NO USO SECUNDÁRIO DE DADOS: TESTE DA BASE LEGAL DO LEGÍTIMO INTERESSE	43
3.1 Princípio da finalidade.....	48
3.2 Boa-fé no tratamento de dados.....	51
3.3 Consentimento no uso secundário de dados.....	56
3.4 Legítimo interesse e a autorização legal ao uso posterior de dados.....	67
3.5 Questões controvertidas na aplicação do legítimo interesse.....	80
4 PROPOSTA LEGISLATIVA DA LEGE LATA A LEGE FERENDA	88
4.1 Uso secundário de dados pessoais com legítimo interesse e a proposta legislativa de alteração da LGPD.....	95
4.2 Análise do Relatório de Impacto à Proteção de Dados do TCU.....	98
5 CONCLUSÃO	105
REFERÊNCIAS BIBLIOGRÁFICAS	109

1 INTRODUÇÃO

A tecnologia e seus avanços possibilitaram uma gama de interações sociais e econômicas que, com o passar do tempo e com o aumento da complexidade da sociedade de informação, necessitaram de tutela específica para o bem jurídico proteção de dados.

O tema da dissertação é o “uso secundário de dados pessoais e seu fundamento no legítimo interesse”. Como preliminar, pode-se dizer que a proteção de dados vem sendo analisada e estudada, e tem sido objeto de iniciativas legislativas na Europa há várias décadas. Em consequência, essa experiência exerceu forte influência sobre a legislação brasileira.

Com relação ao uso secundário de dados, verifica-se que tem direta correlação com o princípio da finalidade, o qual está expresso na Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018, em seu art. 6º, I, que trata da definição da finalidade. Da mesma forma, e sob a mesma tutela, esse princípio está previsto no art. 5º, 1, b) do General Data Protection Regulation (GDPR) da União Europeia.

Para este trabalho, será utilizada, também, a reflexão construída por Solove¹, sobre o uso secundário de dados pessoais, a qual se baseia no questionamento que indaga o motivo da preocupação desse uso além da finalidade coletada, e por que haveria tantas tentativas legais de limitar o seu uso posterior. O autor ainda conceitua uso secundário de dados como sendo o “uso de dados para finalidades não relacionadas àquelas para as quais os dados foram, originalmente, coletados, sem o consentimento do titular dos dados”.

Com relação ao objetivo dessa pesquisa, o que a faz relevante é a análise e observação da possibilidade legal do uso secundário de dados com fundamento no legítimo interesse, o qual está positivado na LGPD em seu arts. 10 e 37, e no GDPR, em seus considerandos 47, 48, 49, 50, 69 e art. 49º. Essa base legal causa insegurança e necessita de análise e investigação, uma vez que trata de um conceito jurídico indeterminado, mas também é considerado, por alguns doutrinadores, como cláusula geral². Independentemente de se estamos a cuidar de

¹ SOLOVE, Daniel J. A taxonomy of privacy. University of Pennsylvania Law Review, v. 154, jan. 2006, p.477-560, p. 519.

² Haja vista o elevado grau de abertura e indeterminação da previsão do legítimo interesse, Laura Schertel Mendes, Danilo Doneda, entre outros, consideram a previsão do legítimo interesse do

conceito jurídico indeterminado ou de cláusula geral, o certo é que o legítimo interesse demanda concreção.

Como pergunta a esse problema, levantamos a seguinte questão: de acordo com o ordenamento jurídico brasileiro existente, quais os limites e condicionantes para a aplicação do legítimo interesse no uso secundário de dados?

A hipótese, a ser confirmada ou refutada, é de que o legítimo interesse, por ser carecedor de valoração pelo intérprete, pode representar, até certo ponto, como um perigoso escape para o uso secundário de dados e, por essa causa, torna-se indispensável alterar a legislação brasileira, para haver mecanismos mais fortes de proteção aos dados pessoais dos titulares.

A concepção metodológica da pesquisa empregada nesta investigação é a hipotético-dedutiva, com pesquisa qualitativa, do tipo bibliográfica-documental. Para tanto, serão analisadas teses, dissertações e artigos produzidos no Brasil, Alemanha, Portugal e Estados Unidos, com um olhar para esses países, com o intuito de analisar suas iniciativas legais e apreendê-las ou, apenas, entendê-las em seu contexto jurídico.

Este estudo não é de direito comparado; porém, frente aos desafios comuns do mundo digitalizado e globalizado, é interessante ter um olhar para iniciativas já adotadas em outros países e em outros blocos econômicos, como a União Europeia, sobre a proteção ao uso secundário dos dados com fundamento no legítimo interesse.

Importa a este trabalho refletir, também, sobre o princípio da finalidade, da necessidade e da transparência, os quais justificam o legítimo interesse. Além disso, o GDPR e a Carta de Direitos Fundamentais da União Europeia são relevantes fontes para este trabalho. Já as contribuições de Sociologia contam com obras que tratam da era do capitalismo de vigilância, do valor monetário dos dados e de temas sensíveis como o protagonismo das plataformas digitais como, por exemplo, “Sociedade em Rede” do autor Manuel Castells, com o objetivo jurídico de verificar o porquê do uso secundário dos dados pessoais e seus fundamentos no legítimo interesse.

Na exposição do estudo, será utilizada a estrutura de sumário dividido em três partes:(i) tratamento de dados pessoais e uso secundário de dados, (ii) diálogo

controlador como uma espécie de cláusula geral, cujo conteúdo deve se preenchido no caso concreto. MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova lei geral de proteção de dados**. Revista do direito do consumidor, v.120, 2018, p.469-483.

principiológico no uso secundário de dados: teste da base legal do legítimo interesse e, por fim, uma (iii) proposta legislativa da *lege lata* a *lege ferenda*.

Para investigar o tema, a primeira parte do trabalho pretende fornecer amparo axiológico a esta pesquisa e inicia com uma abordagem acerca do tratamento de dados pessoais e seu uso secundário, analisando, historicamente, as raízes e heranças alemãs e sua preocupação com a proteção de dados. No decorrer dessa primeira parte serão estudados os conceitos de dado pessoal e informação, os aspectos do termo “informação relacionada a” e a “pessoa natural identificada ou identificável”, além de abordar e refletir sobre o uso secundário de dados pessoais.

O segundo capítulo objetiva estudar o diálogo principiológico no uso secundário de dados: teste da base legal do legítimo interesse. Para contextualizar, será examinado o princípio da finalidade, o qual limita o uso secundário de dados, além de ser um princípio fundamental no tratamento desses dados, os quais não poderão ser tratados de forma incompatível com ele. Após, será verificada a base legal do consentimento, a qual assume com mais propriedade as vestes de um ato do titular, cujo efeito será de autorizar um determinado tratamento para os dados pessoais.

Na sequência, ingressa-se no legítimo interesse e no uso posterior de dados. Com relação ao instituto do legítimo interesse, será verificado e analisado o caráter de norma semanticamente aberta. Entretanto, é preciso esclarecer que dentre as normas abertas aninham-se os princípios normativos, os conceitos indeterminados, as diretivas (normas-objetivo) e as cláusulas gerais³. A cláusula geral, construção de origem alemã, indica “uma estrutura normativa cuja prescrição é vaga na hipótese, isto é, cujo conteúdo não está previamente descrito”⁴. Ela é uma norma vaga, que exige precisão e construção por parte do intérprete. Dessa forma, as cláusulas gerais são portas para a entrada de valores éticos-morais no sistema jurídico⁵.

A base legal do legítimo interesse, a ser tratada, é um instituto jurídico que justifica o uso posterior de dados, por criar algumas possibilidades de tratamento. O

³ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. São Paulo: MARCIAL Popns, 2015, p.120.

⁴ Ibidem, p.122.

⁵ MENKE, Fabiano. **A interpretação das cláusulas gerais**. A subsunção e a concreção dos conceitos. Revista de Direito do Consumidor, v.50, 200, p.9-35, p. 12.

legítimo interesse, historicamente, tem sido encarado como a mais flexível⁶ das bases legais de dados no regime do direito comunitário europeu. Essa base legal ganhou ainda mais relevância diante da emergência de tecnologias e no contexto de uma economia baseada no uso intensivo de dados⁷.

Poderá haver um legítimo interesse, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está a serviço do responsável pelo tratamento. De qualquer forma, a existência de um legítimo interesse requer uma avaliação cuidadosa, em função de saber se o titular dos dados pode prever, razoavelmente, no momento e no contexto em que os dados pessoais são coletados, que esses poderão ser tratados secundariamente.

Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando os dados pessoais forem tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional⁸. Para tratar desse assunto e seus critérios, será abordada e analisada a avaliação do teste de legítimo interesse, com 4 fases, estabelecido por meio do Grupo de Trabalho 29, em seu parecer 06/2014, considerado um teste multifatorial, a ser considerado pelos reguladores e pelos próprios agentes da cadeia de processamento de dados (os controladores), respectivamente, ao interpretarem e se valerem dessa base legal. Além disso, será abordado o teste do Information Commissioner's Office (ICO) composto por 3 fases e a escolha feita pela Lei Geral de Proteção de Dados.

Por fim, o último capítulo apresenta uma proposta legislativa da lege lata a lege ferenda, traçando um paralelo entre o GDPR e a LGPD, com intuito de sugerir uma alteração legislativa no art. 38 da LGPD, no que se refere a atual *faculdade* de determinar ao controlador que elabore um relatório de impacto à proteção de dados pessoais. Hoje, a LGPD prevê apenas a possibilidade da autoridade nacional determinar ao controlador que elabore relatório de impacto à proteção de dados, inclusive os sensíveis. Ao contrário do que ocorre na LGPD, no GDPR há um

⁶ UK Information Commissioner's Office. Guide to the general protection regulation (GDPR). Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection-regulation-gdpr/>>. Acesso em: 06 mar. 2023.

⁷ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 238.

⁸ Considerando 47 do GDPR. EUROPEAN UNION. Regulation(EU) 2016/679. **GD Protection Regulation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 out. 2022.

capítulo denominado *data protection impact assessment and prior consultation*, dedicado a exposições específicas, nos arts. 35º e 36º. É possível encontrar nesses artigos as definições, a indicação da pessoa responsável pelo documento, o momento indicado para a elaboração do *relatório de impacto à proteção de dados*, os casos em que é obrigatória a elaboração, os papéis das autoridades de proteção de dados, entre outros tópicos.

Sugere-se, nesta dissertação, que o RIPD seja obrigatório para determinados casos e com critérios legais bem determinados, aos moldes do GDPR, como será demonstrado no último capítulo. Inclusive, será analisado o relatório de impacto à proteção de dados do Tribunal de Contas da União.

Em síntese, a presente dissertação pretende apresentar uma visão geral do uso secundário de dados pessoais com fundamento no legítimo interesse, apresentando uma possível solução para mitigar os riscos do uso secundário de dados, por meio da alteração legislativa do art. 38 da LGPD, dispositivo esse que deve exigir o relatório de impacto à proteção de dados em algumas situações de risco demasiado, com um olhar para o GDPR no que se refere a esse tema.

2. TRATAMENTO DE DADOS PESSOAIS E USO SECUNDÁRIO DE DADOS

Um dos fundamentos mais relevantes da LGPD é o da autodeterminação informativa, previsto no texto legal, no art. 2º, II. Para tratar dele, necessário se faz perpassar pelo direito à privacidade, também disposto na Lei, em seu art. 2º, I, e debatido, pela primeira vez, por meio de um artigo de Warren e Brandeis, intitulado “The right to privacy”. Essa matéria alcançou o objetivo de expor o fato de que os aparatos tecnológicos invadiram os ‘sagrados domínios da vida privada’⁹, por meio da fotografia e dos jornais.

Os autores Warren e Brandeis, ao fundamentarem o direito à privacidade, relacionaram a sua proteção à inviolabilidade da personalidade, rompendo com a tradição anterior, que associava a proteção da vida privada à propriedade¹⁰. Em suas palavras: “o princípio que protege escritos e outras produções pessoais, não contra o furto ou a apropriação física, mas contra toda e qualquer forma de publicação, não é o princípio da propriedade privada, mas o da inviolabilidade da personalidade”¹¹. Ao identificar o direito à privacidade, Warren e Brandeis buscam definir os seus contornos, na seguinte categorização: a) o direito à privacidade não impede a publicação do que é de interesse geral; b) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito; c) a reparação não será exigível, se a intromissão for gerada por uma revelação verbal, que não cause danos; d) o consentimento do titular afetado exclui a violação do direito; e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; e f) a ausência de dolo não exclui a violação desse direito¹².

⁹ WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. IV, n. 5.

Disponível em:

<https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> Acesso em: 29 dez. 2022.

¹⁰ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 28.

¹¹ WARREN, Samuel; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, v. IV, n.5.

Disponível em:<https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>

>. Acesso em 29 dez. 2022.

<https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> Acesso em: 29 dez. 2022.

¹² WARREN, Samuel; BRANDEIS, Louis. The right to privacy. Harvard Law Review, v. IV, n.5.

Disponível em:

<https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 28 dez. 2022.

A partir dos ensinamentos desse artigo acadêmico supracitado, a proteção à privacidade teve um caráter fortemente individualista (*right to be let alone*), em seus primórdios, com sua feição do direito a ser deixado só. Nesse sentido, sobressaíram as suas características de direito negativo, como a exigência absoluta de abstenção do Estado na esfera privada individual, para a sua garantia¹³.

Com efeito, no transcurso do século XX, a transformação da função do Estado, aliada à função tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade: de um direito com dimensão negativa, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático¹⁴. Houve um processo, no século passado, de contínua reformulação do direito à privacidade, que se transformou para fazer emergir a dimensão de dados pessoais, além de adquirir um caráter positivo e de ser reconhecido internacionalmente, transformou-se para fazer emergir a dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado de dados.

A partir da década de 1970, a transformação desse conceito de direito à privacidade pode ser percebido de forma mais clara, com edição de legislações específicas e de decisões judiciais de diversos países, assim como a aprovação de acordos internacionais e transnacionais em diferentes níveis¹⁵. Por consequência, todos esses instrumentos compartilham o conceito, segundo o qual os dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela jurídica¹⁶.

A primeira geração das normas de proteção de dados pessoais surgiu como reação ao processamento eletrônico de dados nas administrações públicas e nas empresas privadas, bem como às ideias de centralização de dados em gigantes bancos de dados nacionais¹⁷. Pode-se citar, como exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de dados da Suécia (1973), o Estatuto de Proteção de Dados da Alemanha (1977).

¹³ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 29.

¹⁴ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 181.

¹⁵ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 29.

¹⁶ *Ibidem*, p. 30.

¹⁷ MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. **Technology and privacy**: the new lanscape: The Mit Press, 2001.

Além disso, nos Estados Unidos, foram aprovados, nesse mesmo período, o *Fair Credit Reporting Act* (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o *Privacy Act* (1974), aplicável à administração pública¹⁸.

Na sequência, a segunda geração de normas de proteção de dados pessoais ocasiona uma controvérsia interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social¹⁹. Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia, que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados, é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais²⁰.

Com relação à terceira geração de dados²¹, ela é marcada pela decisão do Tribunal Constitucional alemão de 1983²², a qual declarou a inconstitucionalidade de parte da Lei do Censo. Naquela ocasião, o Tribunal interpretou a Lei Federal de Dados Pessoais alemã à luz da Lei Fundamental de Bonn e declarou que os cidadãos possuem o direito à *autodeterminação informativa* (informationelle Selbstbestimmung), reconhecendo uma carga participativa muito maior que àquela, fruto das interpretações das normas de proteção de dados em períodos anteriores²³.

O regime legal de proteção de dados começou a ser consolidado, na Alemanha, a partir de 1970, com a aprovação da *Hessisches Datenschutzgesetz* – HDSG- por meio do Parlamento alemão do estado do Hesse. Naquela época, a expressão proteção de dados (Datenschutz) foi, pela primeira vez, cunhada, e um modelo normativo autônomo foi reconhecido. Essa expressão *Datenschutz* se

¹⁸ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 29.

¹⁹ Ibidem, 30.

²⁰ Ibidem, 31.

²¹ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 41.

²² BvefGE 65, 1, Volkszählung. Ver MARTINS, Leonardo (Org.). Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevideu: Fundação Konrad Adenauer, 2005, p. 233-245. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em: 16 jan. 2023.

²³ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 42.

consolidou na Alemanha, e em toda a Europa, expandindo-se para que se tornasse, gradualmente, um direito fundamental autônomo, que ultrapassa a segurança da informação, a privacidade e o sigilo²⁴.

Em observação e análise da reflexão crítica de Mayer-Schönberger, verifica-se que o autor examina o custo social que o indivíduo tem que pagar para exercer o seu direito à privacidade e à proteção de dados pessoais:

“[...]A proteção de dados pessoais, como liberdade individual, pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas.. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas?”²⁵

De acordo com MENDES²⁶, seguiram-se importantes instrumentos internacionais e transnacionais que contribuíram para a consolidação de um conceito de privacidade ligado à proteção de dados pessoais. Nesse contexto, destacam-se: a Convenção 108 do Conselho da Europa (1981)²⁷, as Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais²⁸(1980) e a Diretiva Europeia 95/46/CE relativa à proteção de dados pessoais²⁹.

A decisão do Tribunal Constitucional Alemão, no julgamento da “Lei do Recenseamento de População, Profissão, Moradia e Trabalho” de 25.03.1982, é considerada uma referência na evolução do conceito de privacidade³⁰. Nesse

²⁴ DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: BIONI, Bruno et al. (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 8.

²⁵ MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Phillip E., ROTENBERG, Marc. Technology and Privacy: the new landscape. Cambridge: Mit: 2001, p. 228.

²⁶ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 38.

²⁷ CONVENÇÃO EUROPEIA. **Convenção 108 do Conselho da Europa**. Disponível em: <<https://rm.coe.int/1680078b37>>. Acesso em: 11 jan. 2023.

²⁸ EUROPEAN UNION. **Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais**. Disponível em: <<https://www.oecd.org/sti/ieconomy/15590254.pdf>>. Acesso em: 11 jan. 2023.

²⁹ PARLAMENTO EUROPEU. **Diretiva Europeia 95/46/CE**. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>>. Acesso em: 11 jan. 2023.

³⁰ MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 30.

histórico julgamento, o Tribunal Alemão radicalizou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade, e decidiu pela inconstitucionalidade parcial da referida lei, quando argumenta a existência de um direito à *autodeterminação informativa* (informationelle Selbstbestimmung), com base nos artigos da Lei Fundamental que protegem a dignidade humana e o livre desenvolvimento da personalidade³¹.

Como afirma Marion Albers, a relevância da autodeterminação informativa reside na flexibilidade oportunizada por uma concepção abstrata de proteção³². Por não possuir um conteúdo fixo de garantia, nem estar limitado apenas às informações pertencentes à esfera íntima ou privada, o direito à autodeterminação informativa pode ser aplicado a uma multiplicidade de casos envolvendo a coleta, processamento ou transmissão de dados pessoais³³. Em razão disso, a finalidade da coleta e o destinatário da informação são mais decisivos para a avaliação da constitucionalidade do processamento de dados do que a classificação dos dados em privados e íntimos³⁴.

A opção legislativa da Lei Geral de Proteção de Dados, de incluir a autodeterminação informativa no texto da lei, indica inspiração na dogmática alemã acerca da matéria, pois foi naquele país que se tornou conhecido e se desenvolveu esse fundamento³⁵ da disciplina de proteção de dados pessoais, a partir da decisão do censo, de 1983.

Por consequência, é possível dizer que, dos fundamentos presentes no art. 2º da LGPD, a autodeterminação informativa é aquela que guarda, juntamente com o respeito à privacidade, a relação mais próxima com a disciplina de proteção de dados³⁶.

³¹ Ibidem.

³² ALBERS, Marion. **A complexidade da proteção de dados**. Direitos Fundamentais e Justiça, ano 10, n. 35, jul.-dez., 2016, p. 19-45.

³³ Ibidem.

³⁴ MENDES, Laura Schertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados**. Portal Jota, 10 de maio de 2020. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>> Acesso em: 12 jan. 2023.

³⁵ MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle(coord.). Lei Geral de Proteção de Dados: aspectos relevantes. São Paulo: Editora Foco, 2021, p. 14-20.

³⁶ MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (coord.). Lei Geral de Proteção de Dados: aspectos relevantes. São Paulo: Editora Foco, 2021.

Não existem precedentes legislativos, no Brasil, de previsão da autodeterminação informativa, em qualquer contexto. Na jurisprudência, antes do julgamento da ADIN 6389, ela foi apresentada em alguns precedentes³⁷ do Supremo Tribunal Federal e do Superior Tribunal de Justiça, mas sem construção mais detalhada³⁸. Trata-se de um importante marco na compreensão dessa nova demanda como um direito tão importante quanto o da privacidade³⁹ (e não apenas seu consectário), porque é elementar à evolução da própria sociedade, de seus indivíduos e de suas instituições. Não basta reconhecer a existência de um direito fundamental apenas em seu caráter formal, pois fundamental é a compreensão e a garantia de sua efetividade⁴⁰. Elementar se fez traçar o histórico da autodeterminação informativa e privacidade, para que se possa adentrar ao objeto da pesquisa, que se constitui no cumprimento do princípio da finalidade e sua multiplicidade de uso. Na sequência do capítulo, investiga-se o conceito de dado pessoal e informação.

2.1 Dado pessoal e informação

A definição de dado pessoal, como bem jurídico próprio⁴¹, encontra-se no art. 5º, I, da LGPD, com o seguinte conceito: "informação relacionada à pessoa natural identificada ou identificável". De forma um pouco mais abrangente e conceitual está a definição de dados pessoais no GDPR, em seu art. 4º(1): "informação relativa a uma pessoa identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização[...]". Esses conceitos são bastante semelhantes, porém o conceito da LGPD é mais sintético, de acordo com o próprio ordenamento jurídico.

³⁷ Como exemplo de precedente, podemos citar: REsp 1.630.659, 3ª Turma, Rel. Min. Nancy Andrighi, j. 27.11.2018, DJ 06.12.2018.

³⁸ Ibidem, p.13.

³⁹ MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (coord.). Lei Geral de Proteção de Dados: aspectos relevantes. São Paulo: Editora Foco, 2021.

⁴⁰ Ibidem.

⁴¹ VIGLIAR, José Marcelo M. LGPD e Proteção de Dados Pessoais na Sociedade em Rede. Grupo Almedina, Portugal, 2022. Disponível em: <<https://app.minhabiblioteca.com.br/reader/books/9786556276373/pageid/24>>. Acesso em: 03 mar 2023.

A LGPD introduz no Brasil um regime geral de proteção de dados pessoais. Essa Lei vem complementar o marco regulatório brasileiro da sociedade da informação ao compor, juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor, o conjunto normativo que moderniza o tratamento da informação no Brasil⁴².

É possível identificar cinco eixos na LGPD, em torno dos quais a proteção do titular de dados se articula⁴³. O primeiro deles diz respeito ao âmbito de aplicação material da lei, caracterizado pela generalidade e unidade: a lei concentra-se na proteção dos dados do cidadão, independentemente de quem realiza o seu tratamento, comando esse que se insere no art. 3º da Lei Geral de Proteção de Dados. Importante ressaltar que apenas os dados referentes às pessoas naturais merecem proteção, conforme dispõem os seus arts. 1º e 5º da LGPD⁴⁴. Já o segundo eixo refere que o tratamento não poderá ser realizado sem que haja uma base normativa que o autorize. Além disso, existem 10 hipóteses autorizativas,

⁴² Conforme MENDES, “a Lei Geral de Proteção de Dados tem como objetivo proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor.[...] Ao refletir sobre as principais influências que moldaram a LGPD, é possível verificar que ela se inspira, em primeiro lugar, no conceito que ficou conhecido como modelo europeu de proteção de dados, amparado na Convenção da Europa 108 de 1981, na Diretiva 46/95/CE e no Regulamento Geral de Proteção de Dados(Regulamento 2016/679).[...]Além disso, também se nota clara influência da legislação brasileira nas normas da LGPD. Do Marco Civil da Internet, por exemplo, tem-se o art. 2º, que enumera os fundamentos da proteção de dados no Brasil. Da lei do Cadastro Positivo, tem-se a regra relativa à revisão das decisões automatizadas(art. 5º, VI, da lei 12.414/2011), conceito desenvolvido, anteriormente, pela Diretiva europeia 46/95, mas que foi introduzido na lei do Cadastro Positivo como um direito à revisão. Do CDC, tem-se o art. 64 da LGPD, relativo ao diálogo das fontes, inspirado no art. 7º do CDC, bem como algumas regras de responsabilidade, em especial, a inversão do ônus da prova, as excludentes de responsabilidade, a possibilidade de danos coletivos, assim como o conceito de tratamento impróprio de dados(art. 42, §§ 2º e 3º, 43 e 44, da lei 13.709/2018)”.

In: MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. São Paulo: Ed. RT, nov.-dez. Revista do Direito do Consumidor, vol. 120, ano 27, p. 469-483.

⁴³ *Ibidem*, p. 470.

⁴⁴ O art. 1º da LGPD prevê o seguinte comando: “esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”. Outro comando elucidativo se encontra no art. 5º da Lei: “I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável”. In: BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

elencadas no art. 7º da LGPD⁴⁵. Para exemplificá-las, citam-se o próprio consentimento do titular ou a previsão legal ou regulamentar do tratamento.

O terceiro eixo da Lei Geral de Proteção de Dados é composto pelos princípios⁴⁶ e direitos do titular, entre eles, aquele que limita o uso secundário de dados pessoais: o princípio da finalidade, o qual vincula o tratamento de dados pessoais ao fim que motivou e justificou a sua coleta. Dessa forma, a aplicação desse relevante princípio tem como consequência a concretização de uma das finalidades últimas da lei, qual seja, a consideração de que o tratamento dos dados pessoais são indissociáveis de uma determinada função, que sempre poderá ser avaliada; ou mesmo que dados pessoais, por estarem, de certa forma, “afetados” por uma finalidade, jamais poderão ser considerados uma mera *res in commercium*⁴⁷. Ainda conforme Mendes e Doneda, o quarto eixo estabelece obrigações para os agentes de tratamento, instituindo não apenas limites ao tratamento de dados em si, como também prevendo uma série de procedimentos que procuram proporcionar maior segurança e reforçar as garantias dos titulares dos dados⁴⁸. A natureza de diversas dessas obrigações dá conta de que a LGPD vai além de proporcionar instrumentos para defesa e proteção do titular – em outras palavras - seus efeitos não se fazem sentir apenas sob requerimento do titular. Ao contrário, há vários mecanismos que procuram reforçar a segurança e prevenir

⁴⁵ O art. 7º da LGPD trata do rol dos requisitos para o tratamento dos dados pessoais, o qual dispõe que esse tratamento pode ser realizado nas seguintes hipóteses: “I - mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador[...]”. In:BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

⁴⁶ Os princípios da LGPD estão elencados em seu art. 6º, e são eles: I-finalidade; II-adequação; III-necessidade; IV-livre acesso; V-qualidade dos dados; VI-transparência; VII-segurança; VIII-prevenção; IX-não-discriminação; X-responsabilização e prestação de contas. In: BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

⁴⁷ MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. São Paulo: Ed. RT, nov.-dez. Revista do Direito do Consumidor, vol. 120, ano 27, p. 469-483.

⁴⁸ Para os autores MENDES e DONEDA, entre as principais obrigações está a do controlador estabelecer um encarregado pelo tratamento de dados, nos termos do art. 41 da LGPD. Note-se que se trata de uma obrigação a ser cumprida pelo controlador e não pelo operador. Entende-se que o encarregado terá como funções receber reclamações dos titulares, comunicar-se com a autoridade nacional de dados e orientar os funcionários para que a organização cumpra com as normas de proteção de dados. A própria lei estabelece a possibilidade de dispensa dessa obrigação que depender de norma a ser editada pela Autoridade Nacional de Proteção de Dados(art. 41,§3º). In: MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. São Paulo: Ed. RT, nov.-dez. Revista do Direito do Consumidor, vol. 120, ano 27, p. 469-483.

problemas e danos no tratamento de dados. Ao mesmo tempo, há também a preocupação em estabelecer uma sistemática própria para medidas de natureza reparativa, em caso de dano⁴⁹. Por fim, o quinto eixo é o da responsabilidade dos agentes na hipótese de ocorrência de danos decorrentes do tratamento de dados e está regulado na seção III do capítulo IV da LGPD⁵⁰.

Em todas as restrições ao tratamento de dados, em conjunto com a assertiva de que a Lei Geral de Proteção de Dados tem como base a sua eliminação, quando o tratamento estiver encerrado- previsto no art. 15 da LGPD⁵¹ - verifica-se a preocupação da lei com o risco presente em seu manejo. Diante dele, a LGPD procura minimizar as hipóteses de tratamento àquelas que sejam, em sentido geral, úteis e necessárias, para que possam mitigar o risco aos direitos e liberdades do titular de seus dados.

No Brasil, foi apenas recentemente - diferentemente do que se deu no caso pioneiro de Portugal, cuja Constituição de 1976 já contemplava, em sua versão original, uma proteção em face do uso da informática e, em parte, também a questão dos dados pessoais - que um direito fundamental autônomo e implicitamente positivado foi reconhecido pelo Supremo Tribunal Federal, em paradigmática decisão proferida pelo Plenário, cancelando provimento

⁴⁹ *Ibidem*, p. 465.

⁵⁰ A Lei Geral de Proteção de Dados aborda “a responsabilidade e o ressarcimento de danos, em seu capítulo IV, seção III, no art. 42 está a previsão de “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de dados pessoais, é obrigado a repará-lo”. Na sequência, o § 1º dispõe que “a fim de assegurar a efetiva indenização ao titular de dados: I - o operador responde, solidariamente, pelos danos causados pelo tratamento, quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43” da LGPD;”II- os controladores que estiverem, diretamente, envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem, solidariamente, salvo nos casos de exclusão, previstos no art. 43” da LGPD [...]. O art. 43 da LGPD dispõe um rol de exclusão de *responsabilidade dos agentes de tratamento de dados*, que se afirma nos seguintes itens: “I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro”. In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

⁵¹ Com a finalidade de estabelecer as hipóteses do término do tratamento de dados pessoais, o art. 15 da LGPD elenca as possibilidades:”I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II – fim do período do tratamento; III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da LGPD, resguardado o interesse público; ou IV – determinação da autoridade nacional, quando houver violação ao disposto na LGPD”. In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

monocrático, em sede de liminar, da Ministra Rosa Weber no bojo da Ação Direta de Constitucionalidade nº 6387 MC-Ref/DF, julgamento em 06 e 07.05.20⁵².

Na ocasião, e a exemplo do que ocorreu em outras ordens constitucionais (Alemanha e Espanha, num primeiro momento), o direito à proteção dos dados pessoais foi deduzido pela Corte Suprema a partir de alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da Constituição – os direitos à privacidade e à intimidade, e um direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa.

O julgamento do plenário referendou a Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6393, 6390, suspendendo a aplicação da Medida Provisória 954/2018⁵³, que obrigava as operadoras de telefonia a repassarem ao IBGE dados identificados de seus consumidores de telefonia móvel, celular e endereço⁵⁴. Relatada pela Ministra Rosa Weber, a decisão contou com a impressionante maioria de 10 votos.

O julgamento é um marco na tutela dos dados pessoais como direito fundamental. Assim, não é exagero afirmar que o seu significado para o Brasil é comparável ao julgamento da Corte constitucional alemã de 1983 que, de forma pioneira, estabeleceu o conceito de autodeterminação informativa naquele país, posteriormente influenciando e moldando os debates internacionais sobre proteção de dados⁵⁵. Curiosamente, tanto no caso brasileiro como no alemão, debatia-se a coleta realizada por órgãos estatais para a produção de estatística oficial,

⁵² Sarlet, Ingo, W. et al. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. Minha Biblioteca, Editora Saraiva, 2022. Disponível em: <[https://app.minhabiblioteca.com.br/reader/books/9786555599527/epubcfi/6/2\[%3Bvnd.vst.idref%3Dcover.xhtml\]!/4/2\[cover\]/2%4050:77](https://app.minhabiblioteca.com.br/reader/books/9786555599527/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover.xhtml]!/4/2[cover]/2%4050:77)>. Acesso em: 07 jan. 2023.

⁵³ A MPV 954/2018, em seu art. 1º, contempla a seguinte redação: "esta medida provisória dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado-STFC e do Serviço Móvel Pessoal-SMP com a Fundação Instituto Brasileiro de Geografia e Estatística-IBGE.

⁵⁴ MENDES, Laura Schertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais**. Portal Jota, 10 de maio de 2020. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020>>. Acesso em: 12 jan. 2023.

⁵⁵ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 56.

destacando a necessidade da implementação de medidas concretas para a proteção de direitos fundamentais, independentemente das boas intenções envolvidas e de sua relevante atuação.

Destacam-se aqui três aspectos centrais da decisão para compreender o seu significado e efeitos no ordenamento brasileiro: primeiro, a superação da falácia de que existiriam dados pessoais neutros desprovidos de proteção, consolidando o dado pessoal como merecedor de tutela constitucional. Como decorrência, tem-se o reconhecimento de um direito autônomo à proteção de dados pessoais e o seu duplo efeito sobre os deveres do Estado (um dever negativo de não interferir indevidamente no direito fundamental e um dever positivo de adotar medidas positivas para a proteção desse direito). Por fim, a partir desse reconhecimento, concluiu-se que o quadro infraconstitucional brasileiro daquele momento, em razão da omissão do poder executivo em criar a Autoridade Nacional de Proteção de Dados (ANPD), encontrava-se em clara contrariedade aos parâmetros e valores constitucionais.

Com a aprovação do Projeto de Emenda Constitucional nº 17/2019 e posterior promulgação, em fevereiro de 2022, da correspondente Emenda Constitucional⁵⁶ nº 115/22, a discussão sobre a conveniência e a oportunidade da inserção de um direito fundamental à proteção de dados pessoais na Constituição restou, de certo modo, superada. De acordo com o texto da EC nº 115, foi acrescido o inciso LXXIX ao artigo 5º, dispondo que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. Mesmo que se pudesse, como já o fizera o STF, reconhecer a proteção de dados como um direito fundamental implícito, daí extraindo todas as consequências atinentes à tal condição, o fato é que sua positivação formal, em sendo o caso, carrega consigo uma carga positiva adicional, ou seja, agrega (ou, ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil.

Com relação ao liame do direito com a tecnologia, tem-se que o papel da informação, como substrato do direito fundamental à proteção de dados, em inúmeras situações jurídicas, é incontestável. Paralelamente, há também a questão

⁵⁶ BRASIL. Constituição Federal. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais>. Acesso em: 31 out. 2022.

da visibilidade e da relevância da informação como um dado próprio do tempo moderno⁵⁷.

Ao longo do tempo, a sociedade conheceu diversas formas de organização social⁵⁸. Em cada época, existiu um elemento central para o seu desenvolvimento, sendo o modelo pelo qual ele se estruturou o fator determinante para estabelecer os seus respectivos marcos históricos⁵⁹.

Quando se faz referência aos termos *dado* e *informação*, é necessário notar, em um primeiro momento, que o conteúdo de ambos se sobrepõe em várias circunstâncias, o que demonstra uma certa desordem em sua utilização⁶⁰.

Contudo, o dado tem o sentido um pouco mais primitivo e fragmentado, como uma informação em estado potencial, antes de ser transmitida⁶¹. Dessa forma, o dado está associado a uma espécie de “pré-informação”, que precede à interpretação e a um processo de elaboração. A informação, em seu refinamento mais elaborado, remete a algo além da representação contida no dado, chegando ao limiar da cognição.⁶² Na informação, mesmo sem aludir ao seu significado, já se pressupõe a depuração de seu conteúdo, pois carrega em si também um sentido instrumental, que visa à redução de um estado de incerteza⁶³.

A legislação brasileira atual apresenta a seguinte definição a respeito de dado pessoal: “informação relacionada à pessoa natural identificada ou identificável”⁶⁴. Tal normatização se encontra no art. 5º, I, da Lei Geral de Proteção

⁵⁷ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 03.

⁵⁸ SILVA, Daniel Pereira Militão. **Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação**. Dissertação (Mestrado) – Faculdade de Direito da PUCSP, 2009, p. 43.

⁵⁹ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 03.

⁶⁰ Nesta dissertação, utilizar-se-á “dado como se estivesse associado a uma espécie de pré-informação, anterior à interpretação e a um processo de elaboração. Por outro lado, informação está associada a determinadas ordens de valor”. In: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados**. 3 ed. São Paulo: Thomson Reuters, 2021, p. 140.

⁶¹ WACKS, Raymond. **Personal Information**. Oxford: Clarendon Press, 1989, p. 25.

⁶² DONEDA, Danilo. **Da Privacidade à Proteção de Dados: fundamentos da lei geral de proteção de dados**. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 140.

⁶³ Segundo o autor, DANILO DONEDA, “o que hoje destaca a informação de seu significado histórico é a maior na sua manipulação, desde a sua coleta e tratamento até a sua comunicação. E o vetor que faz essa diferença é, justamente, o tecnológico: ao incrementar a capacidade de armazenamento e comunicação, cresce também a variedade de formas pelas quais a informação pode ser apropriada ou utilizada. In: DONEDA, Danilo. **Da Privacidade à Proteção de Dados: fundamentos da lei geral de proteção de dados**. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 141.

⁶⁴ BRASIL.L

de Dados -LGPD, de 2018, a qual se reitera na anterior definição europeia do *General Data Protection Regulation* – GDPR (Regulamento Geral de Proteção de Dados)⁶⁵, que data de 2016. Esse regulamento, em seu art. 4(1), também descreve como sendo identificável a pessoa que possa ser identificada direta ou indiretamente por referência a algum identificador, como nome, data de nascimento, número de identificação em cadastros públicos, gênero, e qualquer outro dado pessoal. Para compreender a conceituação de dado pessoal, efetuar-se-á a análise de seus elementos, de forma individualizada, os quais se apresentam da seguinte forma: (i) informação relacionada à; (ii) pessoa natural identificada ou identificável.

2.2 Aspectos do termo “informação relacionada a”

Quando se trata de informação, as tecnologias digitais não se limitam ao tratamento de dados pessoais, porém cada vez mais utilizam dados não pessoais, os quais incluem os que eram originariamente pessoais, mas perderam essa qualidade de forma temporária ou permanente, por meio da anonimização⁶⁶ efetiva.

Em qualquer caso, o conceito de relação pessoal também deve ser estendido para dados inicialmente anônimos⁶⁷, mas não anonimáveis ou, posteriormente, anonimizados⁶⁸.

Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados(LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 10 dez. 2022.

⁶⁵ EUROPEAN UNION. Regulation(EU) 2016/679. **General Data Protection Regulation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 out. 2022.

⁶⁶ Desanonimização é o processo inverso ao da anonimização, o qual está positivado na Lei Geral de Proteção de Dados, em seu art. 5º, inc. 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. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados(LGPD)**. Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 05 jan. 2023.

⁶⁷ Observa-se que a Lei Geral de Proteção de Dados inclui um conceito específico sobre *anonimização*, em seu art. 5º, XI: *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.* Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 26 dez. 2022.

⁶⁸ HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**: transformação digital-desafios para o direito. 2 ed. Rio de Janeiro: Forense, 2022, p. 12.

A informação relacionada é fundamental para identificar quais ligações são relevantes e como distingui-las⁶⁹. Como regra geral, para que a informação seja considerada dado pessoal, ela deve ser relativa a uma pessoa, isto é, deve ser sobre a pessoa⁷⁰. Sendo assim, informações relacionadas a situações, que não são subjetiváveis⁷¹, como, por exemplo, objetos, eventos e animais, não podem ser consideradas dados pessoais, estando, assim, excluídas do campo de aplicação da Lei Geral de Proteção de Dados.

Para se entender a relevância da tecnologia informacional, ela atua na sociedade como fonte de poder há muito tempo. Não obstante os avanços mais recentes, nas últimas décadas, o potencial atrelado à informação tem se intensificado, originando uma nova estrutura social, conectada a um modo de desenvolvimento, denominado por Manuel Castells de *informacionalismo*. Como reflexão acerca dessa estrutura, a primeira característica, relativa ao novo paradigma, é que a informação é a sua matéria-prima: existem tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia⁷². No desdobramento, temos, como segundo aspecto, a consequência do efeito das novas tecnologias: a informação integra a atividade humana, fazendo com que todos os processos, individuais e coletivos, estejam diretamente moldados (embora não determinados) pelo novo meio tecnológico. A terceira característica refere-se à lógica de redes, a qual usa essas novas tecnologias de informação, em qualquer sistema e conjunto de relações.

A morfologia da rede parece estar bem adaptada à crescente complexidade de interação, e aos modelos imprevisíveis do desenvolvimento, derivado do poder criativo dessa interação⁷³. No estágio atual, a sociedade está adaptada a uma nova

⁶⁹ WORKING PARTY. Article 29 Data Protection Working Party. **Opinion 4/2007 on the concept of personal data**. Brussels, 20 jun. 2007, p. 09. Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 04 jan. 2023.

⁷⁰ CORDEIRO, A. Barreto Menezes. **Direito da Proteção de dados**: à luz Do RGPD e da Lei n. 58/2019. Coimbra: Al Medina, 2020, p. 110.

⁷¹ PAIVA, Eduarda Beutinger. **A reversibilidade do processo de anonimização e as suas repercussões no regime de proteção de dados pessoais**. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2021, p. 18.

⁷² CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000. (A era da informação: economia, sociedade e cultura, p. 225.

⁷³ KELLY, Kevin. **Out of Control**: the new biology of machines, social systems and the economic world. USA, 1995, 1. ed Basic Books, p. 101.

forma de organização, em que a informação é o elemento nuclear para o desenvolvimento da economia⁷⁴.

A informação contém, em si, o principal ativo da sociedade da informação, ou seja, sua principal riqueza, sendo seu uso indispensável ao desempenho de qualquer atividade – o que explica a nomenclatura atribuída pela doutrina a essa nova forma de organização social, política e econômica. O trabalho, a educação, a saúde, o lazer, a política, a economia, enfim, tudo depende de informação. Após transcorrido o período histórico da supervalorização da terra, e do predomínio dos bens de produção na revolução industrial, o que prepondera, agora, é a informação.

Na qualidade de principal matéria-prima desse novo modelo capitalista, a informação se impõe como condição determinante para o desenvolvimento econômico e cultural da sociedade, daí o intensivo uso da tecnologia da informação – enquanto mecanismo facilitador da coleta, produção, processamento, transmissão e armazenamento – o que acarretam avassaladoras mudanças no mundo⁷⁵.

Hoje se assiste à chamada revolução da tecnologia da informação, a qual pode ser definida como um fenômeno que, apesar de evidenciar importância semelhante à revolução industrial do século XVIII, supera-a exponencialmente, porque induz a todos, e a tudo, um padrão de descontinuidade nas bases materiais da economia, da sociedade e da cultura e, diferentemente de qualquer outra revolução, desestrutura, na mais absoluta amplitude, os domínios da vida, não como fonte exógena de impacto, mas como elemento nuclear de um tecido que, desse elemento destituído, atualmente já não tem condições de se desenvolver⁷⁶.

⁷⁴ "Assim, no modo agrário de desenvolvimento, a fonte do incremento de excedente resulta aumentos quantitativos da mão de obra e dos recursos naturais(em particular a terra) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte e produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e circulação. No modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos"(grifos). CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000. Em sentido similar, SIQUEIRA JR., Paulo Hamilton, "A sociedade da informação tem como principal valor a informação, o conhecimento. Na era agrícola, a terra se configurava como o fator primordial da geração de riquezas. Na era industrial, a riqueza surge da máquina a vapor e da eletricidade. Na era do conhecimento, a informação e o conhecimento são os atores centrais da produção econômica"(grifos). **Teoria do Direito**. São Paulo: Saraiva, 2009, p. 218.

⁷⁵ VIEIRA, Tatiana Malta. **O Direito à privacidade na Sociedade de Informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação**.UNB, 2007. Disponível em: <https://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf>. Acesso em: 18 dez. 2022.

⁷⁶ CASTELLS, Manuel.**A sociedade em rede**. Op. cit., p.67.

Um aspecto adicional que se levanta, em relação à revolução da tecnologia da informação, é que, ao contrário das demais revoluções que ocorreram em uma área geográfica limitada do planeta, com lenta expansão para outras regiões, esta revolução se difundiu, celeremente, por todo o globo em menos de duas décadas⁷⁷.

Até mesmo os relacionamentos sociais foram fortalecidos por um fluxo informacional, e não encontram mais obstáculos físicos distanciais. Existe uma nova e mais abreviada compreensão entre tempo-espaço⁷⁸, o que outrora acarretava maior cadência às interações sociais⁷⁹.

Pode ocorrer que determinada informação possua um vínculo objetivo com uma pessoa, revelando algo sobre ela. Esse vínculo objetivo implica que a informação se refere às características ou ações dessa pessoa, as quais podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio ou, então, às informações provenientes de seus atos, como os dados referentes ao seu consumo, informações provenientes de suas manifestações, como as opiniões que manifesta, e tantas outras⁸⁰. Doneda esclarece que é importante estabelecer esse vínculo, pois ele afasta outras categorias de informações que, embora também façam referência a uma pessoa, não seriam consideradas, propriamente, informações pessoais, no sentido pretendido. Significa dizer que, as opiniões alheias, acerca dessas pessoas, a princípio não possuem esse vínculo objetivo, também sua produção intelectual não é considerada informação pessoal, embora o fato de sua autoria ter essa condição⁸¹. Sobre essa classificação, Pierre Catala identifica uma informação pessoal, quando o objeto da informação é a própria pessoa, com a seguinte análise:

[...]”Mesmo que a pessoa em questão não seja a ‘autora’ da informação, no sentido de sua concepção, ela é titular legítima dos seus elementos. Seu vínculo com o indivíduo é por demais

⁷⁷ CASTELLS, Manuel. **A sociedade em rede**. Op. cit., p. 69-70.

⁷⁸ PAESANI, Liliana Minardi(Coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007, p. XI (Apresentação): Vive-se hoje a era da mais importante revolução tecnológica jamais antes experimentada. Revolução pós-industrial, de dimensão planetária. Novo poder foi criado, o poder tecnológico, que encurta distâncias de tempo e espaço. São enormes e diferentes as consequências que produz sobre as concepções a respeito das relações entre território, política, economia e cultura e atinge áreas geográficas mais extensas e maior quantidade de pessoas”(grifos).

⁷⁹ BIONI, Bruno Ricardo. A proteção de Dados Pessoais: a função e os limites do consentimento.3. ed. Rio de Janeiro: Forense, 2021, p. 5.

⁸⁰ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 143.

⁸¹ *Ibidem*.

estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade”⁸²

Ademais, a sociedade experimenta uma grande quantidade de regras, as quais visam a influenciar o comportamento, em razão do avanço tecnológico. Na atual sociedade da informação e do conhecimento, as regras técnicas, contidas nos algoritmos digitais, estão se tornando cada vez mais importantes, além das regras legais e sociais. Quando se fala em algoritmos, trata-se não apenas da formação da ordem social, mas também do seu desenvolvimento econômico⁸³: eles mudam nossa percepção do mundo⁸⁴.

A ciência da computação tem aumentado as possibilidades pessoais e econômicas, a partir do desenvolvimento de algoritmos inteligentes, os quais são uma sequência de instruções codificadas que determinam, ao computador, o que fazer.

Eles podem ser pré-programados, mas hoje há também algoritmos chamados “aprendizes”(learners), os quais utilizam a técnica de *machine learning* e fazem previsões sobre fenômenos, desenvolvendo outros modelos (e até outros algoritmos), automaticamente⁸⁵, independentemente de uma nova programação humana. Existem, ainda, algoritmos para receber *feedbacks* sobre a precisão e eficiência dos resultados e, com isso, possibilitar a modificação do algoritmo originário para chegar aos resultados pretendidos, de forma mais rápida, barata e precisa⁸⁶.

O exponencial crescimento tecnológico, que se efetivou por meio da utilização desses algoritmos, da inteligência artificial, de técnicas de *profiling*, *data*

⁸² CATALA, Pierre. **Ebauche d’une théorie juridique de l’information**. In: *Informatica e Diritto*, ano IX, jan-abr., 1983, p. 22. Disponível em: <<https://mafr.fr/media/assets/publications/catalap-ebauche-dune-theorie-juridique-de-linformation-1998.pdf>>. Acesso em: 08 jan. 2023.

⁸³ HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital-desafios para o direito**. 2 ed. Rio de Janeiro: Forense, 2022, p. 11.

⁸⁴ HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital-desafios para o direito**. 2 ed. Rio de Janeiro: Forense, 2022, p. 12.

⁸⁵ FERRARI, Isabela; BECKER, Daniel; Wolkart, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. São Paulo: *Revista dos Tribunais*, 2018, vol.995, p 4. Disponível em: <<https://dspace.almg.gov.br/handle/11037/30128>>. Acesso em: 19 dez. 2022.

⁸⁶ FERRARI, Isabela; BECKER, Daniel; Wolkart, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. São Paulo: *Revista dos Tribunais*, 2018, vol.995, p 5. Disponível em: <<https://dspace.almg.gov.br/handle/11037/30128>>. Acesso em: 19 dez. 2022.

mining e todas as formas de processamento de dados, ampliou a sociedade de risco, por potencializar os danos que decorrem das armas de destruição matemática (*weapons of math destruction*)⁸⁷. Em razão de algoritmos sofisticados, os quais são desenhados para auxiliar, ou mesmo para substituir a intervenção humana, verifica-se a habilidade em construir tarefas para a tomada de decisões, tais como: reconhecimento facial, diagnóstico médico, direção autônoma de veículos e, até mesmo, planejamento de campanhas políticas, que outrora não seriam possíveis sem o desenvolvimento dessas ferramentas. Nessa mesma configuração, a *Big Data*⁸⁸ também pode ajudar a detectar fraudes financeiras, aumentando a margem de acertos, cujo esforço humano não conseguiria auferir alcance, velocidade ou eficiência⁸⁹.

Essa larga utilização de algoritmos, nas relações pessoais em uma *Sociedade da Informação*, evidencia verdadeira revolução tecnológica ocorrida nos meios de comunicação, cuja principal característica denota a facilidade de obtenção, troca e difusão de informações advindas de inúmeros lugares do globo, em tempo quase-real, nas quais “a integração e a ubiquidade” são as palavras-chave. A transgressão das fronteiras é seu corolário, quer sejam elas físicas ou funcionais⁹⁰, onde o local, o nacional e o global se interconectam, razão pela qual o impacto dos algoritmos é também objeto de análise de outros campos do conhecimento⁹¹. No campo cultural, é nítido percebermos o papel que desempenham os algoritmos do Google, Facebook e Amazon em sua construção; Ted Striphas⁹² assim os defende, em seu

⁸⁷ O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown, 2016(ebook), n.p.

⁸⁸ Conceituar *Big Data* é um trabalho complexo, pois não há fronteiras concretas acerca desse fenômeno. De acordo com Bart van der Sloot, Dennis Broeders e Erik Schrijvers, a definição de *Big Data* divide-se em três aspectos: (i) coleta de dados- o *Big Data* diz respeito à coleta de grandes quantidades de dados, a partir de fontes variadas e, muitas vezes, não estruturadas; (ii) análise de dados – o *Big Data* relaciona-se, também, à velocidade das análises e do uso de certos mecanismos como algoritmos, *learning machine* e correlações estatísticas; (iii) uso de dados – os resultados são muitas vezes de natureza preditiva e são formulados em nível geral ou de determinado grupo. In: VAN DER SLOOT, Bart; BROEDERS, Dennis; SCHRIJVERS, Erik (org.). **Exploring the boundaries of Big Data**. Amsterdam: WWR, 2016, p.11.

⁸⁹ VERMA, Shikha. **Weapons of mass destruction**: how big data increases inequality and threatens democracy. Book reviewer. New York: Crown, 2016(ebook), n.p. Disponível em: <https://appliedenergyscience.lbl.gov/sites/default/files/Weapons_of_Math_Destruction_How_Big_Data_Increases.pdf> Acesso em 18 dez. 2022.

⁹⁰ MATTELART, Armand. **História da sociedade da informação**. São Paulo: Edições Loyola, 2022, p. 151.

⁹¹ *Ibidem*, p.152.

⁹² Neste artigo, Ted Striphas relata, por meio de sua análise e observação, que os algoritmos estão se tornando decisivos e que empresas como Google, Amazon e Facebook estão, rapidamente, se transformando, apesar da retórica populista, em “os novos apóstolos da cultura”. Disponível em: <<http://journals.sagepub.com/doi/10.1177/1367549415577392>> Acesso em: 20 dez. 2022.

artigo “Algorithmic Culture”⁹³, o qual examina a influência dessas ferramentas na formação do que chamamos de cultura.

O diferencial que a informatização proporcionou ao tratamento de dados pessoais apresenta perfis quantitativo e qualitativo: o primeiro deles baseado na “força bruta”, no poder de processar mais dados em menos tempo e, o outro, na aplicação de técnicas sofisticadas a esse processamento, de forma a obter resultados mais valiosos⁹⁴. Quando combinados, representam a base técnica que, potencialmente, pode ser aplicada a toda coleta de dados pessoais e que deve ser levada em consideração em qualquer enfoque funcional dessa cadeia disciplinar de dados pessoais.

Entretanto, é provável que a informação relacionada à realidade não subjetivável seja tratada como dado pessoal, quando combinada com uma informação relativa a uma pessoa⁹⁵. Por exemplo: (i) um computador com número IP A conectou-se à rede X; (ii) o computador pertence a Luís. A informação (i) é relacionada a um objeto, não sendo, pois, dado pessoal. Todavia, quando conjugada à informação (ii), aquela (i) converte-se em dado pessoal: Luís conectou-se à rede X por meio do seu computador que detém número IP A⁹⁶. Há um exemplo prático e didático, trazido pelo Grupo de Trabalho do artigo 29⁹⁷: uma determinada empresa de táxis instala um sistema de localização por satélite para determinar, em tempo real, a posição dos carros disponíveis. Não obstante o objeto das informações colhidas ser os carros e a finalidade da coleta ser o fornecimento de melhor serviço aos usuários, tal tecnologia permite controlar o desempenho dos motoristas e verificar os limites de velocidade. Portanto, as informações colhidas têm impacto considerável nesses trabalhadores, de modo que podem ser

⁹³ STRIPHAS, Ted. *Algorithmic Culture*. Bloomington: Sage Journals, 2015. Disponível em: <<http://journals.sagepub.com/doi/10.1177/1367549415577392>> Acesso em: 20 dez. 2022.

⁹⁴ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 143.

⁹⁵ CORDEIRO, A. Barreto Menezes. **Direito da Proteção de dados**: à luz Do RGPD e da Lei n. 58/2019. Coimbra: Al Medina, 2020, p. 110.

⁹⁶ PAIVA, Eduarda Beutinger. **A reversibilidade do processo de anonimização e as suas repercussões no regime de proteção de dados pessoais**. Universidade Federal do Rio Grande.

⁹⁷ Este *Grupo de Trabalho GT 29* foi instituído com base no artigo 29 da Diretiva 95/46/EC. Esse grupo representa um corpo consultivo independente de proteção de dados e privacidade. Suas tarefas estão descritas no artigo 30 da Diretiva 95/46/EC e artigo 15 da Diretiva 2022/58/EC. Tradução livre. EUROPEAN UNION. Article 29 Data Protection Working Party. **Opinion 4/2007 on the concept of personal data**. Brussels, 20 jun. 2007, p. 09. Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 04 jan. 2023.

consideradas como dados pessoais, os quais são merecedores de proteção jurídica⁹⁸.

Conforme proposto no Working Party 29, hoje substituído pelo EDPB (European Data Protection Board), a expressão “relacionada à” pode alcançar três situações diversas, as quais configuram elementos alternativos e não cumulativos: (i) conteúdo, (ii) finalidade e (iii) resultado⁹⁹. A primeira constitui regra geral, na qual a informação é sobre determinada pessoa; o indivíduo é o objeto da informação. Esse elemento independe da circunstância e do objetivo do responsável pelo tratamento dos dados, para que a informação seja considerada pessoal. Nesse grupo estão incluídas, por exemplo, a anamnese¹⁰⁰ clínica e as fichas médicas, na qual as informações estão diretamente relacionadas a um sujeito: o paciente. Na segunda situação, a pessoa não é o objeto da informação. Sendo assim, os dados são utilizados para uma *finalidade específica*, que permite avaliar, tratar de determinada forma ou influenciar o comportamento de um indivíduo. Podem-se citar, nesse caso, os dados que constem em um registro de tempo de trabalho, alusivos ao período de serviço e ao período de descanso de determinado trabalhador¹⁰¹.

Para finalizar, situações que contenham elemento de resultado se referem àquelas que não tem o indivíduo como objeto (conteúdo), tampouco visam a avaliá-lo ou influenciá-lo (finalidade), mas que provocam impacto nos direitos ou nos interesses de determinada pessoa¹⁰². O próximo item se ocupará de apresentar características a respeito de pessoa natural identificada ou identificável, dentro do tema dados pessoais, para a análise do cumprimento do princípio da finalidade.

⁹⁸ WORKING PARTY. Article 29 Data Protection Working Party. **Opinion 4/2007 on the concept of personal data**. Brussels, 20 jun. 2007, p. 09. Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 04 jan. 2023.

⁹⁹ Ibidem.

¹⁰⁰ Anamnese é o histórico médico-clínico que vai desde os sintomas iniciais até o momento da observação clínica, realizado com base nas declarações espontâneas do paciente. O termo anamnese vem do grego *anamnesis*, e remete a “trazer de novo à memória”. No contexto da investigação médica, especialmente nos exames complementares para diagnóstico de doenças, alguns pontos relacionados à realização do exame são imprescindíveis, como a razão pela qual ele foi solicitado e o tempo que levou para ser feito. É seguro dizer que o emprego de uma simples pergunta ao paciente já pode auxiliar e fazer a diferença no diagnóstico da condição atual, e também futura, da sua saúde. Disponível em: <<https://portalelemedicina.com.br/blog/o-que-e-anamnese-e-como-e-feita>> Acesso em: 04 jan. 2023.

¹⁰¹ CORDEIRO, A. Barreto Menezes. **Direito da Proteção de dados**: à luz Do RGPD e da Lei n. 58/2019. Coimbra: Al Medina, 2020, p. 112.

¹⁰² PAIVA, Eduarda Beutinger. **A reversibilidade do processo de anonimização e as suas repercussões no regime de proteção de dados pessoais**. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2021, p. 19.

2.3 Aspectos do termo “pessoa natural identificada ou identificável

Com relação à LGPD, seu objeto de tutela não são os dados pessoais, mas sim a proteção do *titular* relacionado a esses dados¹⁰³, ou seja, a pessoa natural (inserida na definição de dado pessoal, consagrada na LGPD), a qual se apresenta como a única destinatária do direito fundamental a sua tutela, porquanto esse direito está fortemente vinculado à dignidade humana e à personalidade¹⁰⁴. Os direitos da personalidade são atributos essenciais à condição humana e as pessoas jurídicas não gozam dessa condição, conforme ensinamento de Schreiber:

[...] As sociedades, as associações, as fundações e todas as demais espécies de entes abstratos detêm personalidade em sentido subjetivo, ou seja, possuem aptidão para a aquisição de direitos e obrigações. Não gozam, apesar disso, da especial proteção que o ordenamento jurídico reserva ao núcleo essencial da condição humana¹⁰⁵.

Não podem ser titulares de dados pessoais as pessoas jurídicas¹⁰⁶, como já foi abordado no art. 5º, I da LGPD e no art. 4º(1) do GDPR, tampouco coisas ou animais (realidades jurídicas não subjetiváveis). A informação relativa à pessoa jurídica apenas poderá ser merecedora de tutela da LGPD quando se relaciona, direta ou indiretamente, com uma pessoa natural¹⁰⁷. Dados pessoais são prolongamentos e sujeições do direito à privacidade, destacado como direito fundamental no art. 5º da Constituição Federal e como direito da personalidade.

¹⁰³ Por meio dessa interpretação, Danilo Doneda ensina que “não se atribui um ‘direito aos dados pessoais’, porém a proteção desses; tal cuidado provoca implicações na inteira estrutura da disciplina de proteção de dados pessoais que segue. Ao afastar a ideia de um direito subjetivo que teria como objeto os dados pessoais, afastam-se, igualmente, as concepções patrimoniais sobre a proteção” In: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 213.

¹⁰⁴ MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 185.

¹⁰⁵ SCHREIBER, Anderson. **Direitos da Personalidade**. São Paulo: Atlas, 2011, p. 21-22.

¹⁰⁶ This regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established established as legal persons, including the name and the form of the legal person and the contact details of the legal person. EUROPEAN UNION. Recital 14. General Data Protection Regulation – GDPR. Disponível em: <<https://www.privacy-regulation.eu/en/recital-14-GDPR.htm>>. Acesso em: 04 jan. 2023.

¹⁰⁷ CORDEIRO, A. Barreto Menezes. **Direito da Proteção de dados**: à luz Do RGPD e da Lei n. 58/2019. Coimbra: Al Medina, 2020, p. 113.

De acordo com Schreiber¹⁰⁸, deve-se analisar o art. 52 do Código Civil com cautela. Argumenta o autor, que o centro gravitacional dos direitos da personalidade é a própria pessoa humana. Por terem uma estrita ligação subjetiva, as pessoas jurídicas não possuem aptidão para adquirirem direitos e obrigações nesta seara. Em razão desse entendimento, o art. 52 do Código Civil não assegura às pessoas jurídicas os direitos subjetivos da personalidade, admitindo, tão-somente, a extensão da técnica desses direitos para a proteção da pessoa jurídica¹⁰⁹. A rigor, a lógica fundante dos direitos da personalidade é a tutela da dignidade da pessoa humana. Ainda assim, provavelmente por conveniência de ordem prática, o legislador pretendeu estendê-los às pessoas jurídicas, o que não poderá significar que a concepção dos direitos da personalidade seja uma categoria conceitual neutra, aplicável indistintamente a pessoas jurídicas e a pessoas humanas. Entretanto, há discussões na doutrina acerca da possibilidade de o direito à proteção de dados ser estendido a pessoas jurídicas, tendo como fulcro o entendimento de que os atos negociais, praticados por essas pessoas, serão atribuídos à própria empresa e não ao sócio, de maneira que os dados advindos de contratações, sejam elas eletrônicas ou não, são prolongamentos da identidade econômica e social das pessoas jurídicas, merecendo proteção, ainda que relativa a elas¹¹⁰. Contudo, a LGPD, *a priori*, não se estende à pessoa jurídica¹¹¹; embora, em um sistema jurídico em que o diálogo das fontes se torna ferramenta indispensável ao operador do direito, interpretar a Lei Geral de Proteção de Dados com base na Constituição Federal e no Código Civil seja de premente necessidade, sob pena de a pessoa jurídica ser prejudicada pelo comportamento legislativo¹¹².

Na abordagem do sentido dos termos pessoa identificada ou identificável, há uma bipartição léxica que, ora retrai (reducionista), ora expande (expansionista) a moldura normativa da Lei Geral de Proteção de Dados.¹¹³ A LGPD não diferencia

¹⁰⁸ SCHREIBER, Anderson. **Direitos da Personalidade**. São Paulo: Atlas, 2011, p. 21-22.

¹⁰⁹ MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano Bruno Santos. **A proteção de dados da pessoa jurídica e a Lei 13.709/2018**: reflexões à luz dos direitos da personalidade. *Scientia Juris*, v. 23, n. 2, p.74-90, jul. 2019, p. 43.

¹¹⁰ MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano Bruno Santos. **A proteção de dados da pessoa jurídica e a Lei 13.709/2018**: reflexões à luz dos direitos da personalidade. *Scientia Juris*, v. 23, n. 2, p.74-90, jul. 2019, p. 43.

¹¹¹ MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano Bruno Santos. **A proteção de dados da pessoa jurídica e a Lei 13.709/2018**: reflexões à luz dos direitos da personalidade. *Scientia Juris*, v. 23, n. 2, p.74-90, jul. 2019, p. 43.

¹¹² *Ibidem*.

¹¹³ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p. 59.

essas duas expressões, proporcionando debates hermenêuticos. Contudo, o GDPR – quando conceitua dado pessoal, trata de definir o termo “identificável” dentro da seguinte baliza:

GDPR, art. 4º-Definições. Para efeito do presente regulamento, entende-se por: (1) “Dados pessoais”, informação relativa a uma pessoa singular identificada ou “identificável (“titular dos dados”); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular[...].”

Em relação a pessoas diretamente identificadas ou identificáveis, o nome da pessoa é, certamente, o identificador mais comum. Em razão desse consenso, na prática, a noção de “pessoa identificada” implica a referência ao seu nome próprio¹¹⁴.

Em razão de verificar essa identidade, o nome da pessoa, algumas vezes, tem que ser combinado com outras partes da informação (data de nascimento, nome dos pais, endereço ou fotografia do rosto) para evitar confusão entre aquela pessoa e possíveis homônimos¹¹⁵. Por exemplo, a informação de que a soma do dinheiro pertence a determinado indivíduo pode ser considerada, na identificação de uma pessoa, porque está vinculada ao seu nome. Ademais, o nome é uma parte da informação que revela que o indivíduo usa a combinação de letras e fonética para distinguir-se e ser distinguido de outras pessoas, com as quais ele estabelece relações. O nome pode ser, de igual forma, o ponto de partida para a informação a respeito da moradia da pessoa ou, até mesmo, onde pode ser encontrada; ele também pode dar informação acerca de seus familiares (por meio do sobrenome) e um número de relações legais e sociais distintas, associadas com o nome (registros de educação, registros médicos, contas bancárias). Nessa mesma linha, pode ser

¹¹⁴ WORKING PARTY. Article 29. Data Protection Working Party. **Opinion 4/2007 on the concept of personal data**. Brussels, 20 jun. 2007, p. 13 Disponível em < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em: 05 jan. 2023.

¹¹⁵ Ibidem.

possível conhecer a aparência da pessoa, se a foto for associada ao nome. Todas essas novas partes de informação, associadas ao nome, podem permitir que alguém construa o indivíduo de carne e osso e, portanto, por meio dos identificadores, a informação original estará associada com a pessoa natural, que pode ser singularizada em relação a outros indivíduos¹¹⁶.

Para adicionar aos exemplos supramencionados, o entendimento de ser ou não a pessoa natural identificável, o GDPR, em seu Considerando 26, acrescentou mais elementos, estabelecendo que:

[...] deve-se levar em conta todos os meios suscetíveis de serem razoavelmente utilizados, tais como a distinção, quer pelo responsável pelo tratamento, quer por outra pessoa, para identificar direta ou indiretamente a pessoa natural¹¹⁷.

Bruno Bioni¹¹⁸ sintetiza o vocabulário e a opção adotada pela Lei Geral de Proteção de Dados e pelas normas setoriais de proteção de dados pessoais e procede a uma análise ilustrativa de suas repercussões práticas:

Quadro I – Vocabulário analítico no conceito de dados pessoais

Expansionista	Reduccionista
Pessoa identificável	Pessoa identificada
Pessoa indeterminada	Pessoa específica/determinada
Vínculo mediato, indireto, impreciso ou inexato	Vínculo imediato, direto, preciso ou exato.
Alargamento da qualificação do dado como pessoal	Retração da qualificação do dado como pessoal

Fonte: Adaptado da tabela de BIONI, Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 60.

¹¹⁶ Ibidem.

¹¹⁷ Ibidem.

¹¹⁸ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p.59.

A partir da dinâmica de conceitos básicos de sistemas de informação e de banco de dados, poder-se-á entender as estratégias regulatórias possíveis e o conceito de dado pessoal. Para ilustrar, apresentar-se-á uma tabela de dados relacionais, para demonstrar as diferenças entre os conceitos reducionista e expansionista¹¹⁹.

Tabela 1 – Base de dados relacionais

A) Nome	B) CPF	C) CEP	D) Idade	E) Classificação
1. Amanda Duarte	297.456.032-77	42900-020	18	Jovem poupadora
2. Amanda Duarte	082.661.001-24	48456-999	24	Jovem consumista
3. Amanda Coelho	996.023.777-11	91234-331	31	Jovem executiva
4. Amanda Löwen	350.209.555-90	71234-990	56	Adulta ciclista

Fonte: Adaptado da tabela de BIONI, Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 61.

Hipótese 1 (reducionista): a presença de homônimas não permitiria que houvesse a individualização exata de uma parcela das pessoas inseridas no banco de dados acima, caso não houvesse outros dados-identificadores (únicos) como, por exemplo, o CPF. Apenas mediante tal associação foi possível identificar, exatamente, a(s) Amanda(s), tornando-as pessoas identificadas, ou seja, individualizadas de maneira precisa, exata e inequívoca¹²⁰.

Hipótese 2 (expansionista): caso houvesse a eliminação da coluna “B”, haveria incerteza sobre qual Amanda seria poupadora, consumista ou executiva (coluna “E”), pois não haveria outro dado para diferenciar cada uma das homônimas. No caso em tela, a incerteza gerada por um grupo de pessoas com o mesmo nome tende a ser eliminada pela agregação de informações, tornando-as pessoas identificáveis¹²¹.

¹¹⁹ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 60-61.

¹²⁰ Ibidem, p.61

¹²¹ Ibidem, p.61.

O dado pessoal é tutelado pela LGPD, de forma explícita, em seu art. 5º. Ele é fundamental para embasar o objeto desta pesquisa, a qual inclui *o princípio da finalidade*, que estabelece limites e fronteiras, objetivando proteger o *titular* desses dados contra o abuso de tratamentos posteriores, sem o seu consentimento ou, até mesmo, do seu conhecimento. O uso secundário de dados pessoais e seu fundamento no legítimo interesse passam pelo entendimento acerca do que é o uso secundário de dados, o que será tratado no próximo tópico.

2.4 Uso secundário de dados pessoais

O uso posterior ao tratamento originário dos dados pessoais, também conhecido como uso secundário de dados, tem seu conceito atrelado ao princípio da finalidade, pois a informação se torna muito mais valiosa ao longo do tempo¹²². Ademais, o conjunto de dados encontra uso secundário e novo valor quando é utilizado para uma finalidade completamente diferente. Nas lições de Mayer e Cukier¹²³, *“o sistema vale-se da informação obtida por uma finalidade e a reutiliza para um finalidade distinta – em outras palavras, o dado se move do uso primário ao uso secundário”*. Em síntese, o valor dos dados precisa ser considerado em termos de todas as possíveis maneiras que poderá ser empregado no futuro.

A reflexão construída por Solove¹²⁴ baseia-se no questionamento que indaga o motivo da preocupação do uso secundário de dados, além da finalidade coletada, e por que haveria tantas tentativas legais de limitar o seu uso posterior. O autor ainda conceitua uso secundário como sendo *“o uso de dados para finalidades não relacionadas àquelas para as quais os dados foram, originalmente, coletados, sem o consentimento do titular dos dados”*¹²⁵. A variedade de uso secundário de

¹²² MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work and think. First Mariner Books: New York, 2014, p. 103. No texto original: The system takes information generated for one purpose and reuses it for another-in other words, the data moves from primary to secondary uses. This makes it much more valuable over time.(...) [The] sets of data find secondary uses – and new value- when they are applied to a completely different purpose. (...) In short, data’s value needs to be considered in terms of all the possible ways it can be employed in the future”. Tradução livre.

¹²³ *Ibidem*.

¹²⁴ SOLOVE, Daniel J. **A taxonomy of privacy**. University of Pennsylvania Law Review, v. 154, jan. 2006, p. 477-560, p. 519.

¹²⁵ **“Secondary use”** is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject’s consent.(Grifei). SOLOVE, Daniel J. **A taxonomy of privacy**. University of Pennsylvania Law Review, v. 154, jan. 2006, p. 477-560, p. 520.

dados é, virtualmente, infinita, e elas variam do benigno ao maligno¹²⁶. Ademais, as pessoas podem não fornecer seus dados, se souberem de um potencial uso, após o tratamento originário deles. Com efeito, esse uso secundário tem a possibilidade de criar problemas, porque a informação pode não encaixar tão bem no novo uso. Isso acontece porque os dados são removidos do contexto primário, para o qual foram coletados; conseqüentemente, esses dados podem ser, facilmente, mal interpretados.

De acordo com o considerando 28 e o art. 6º, n.1, b) da Diretiva¹²⁷, as finalidades devem ser consideradas antes ou, em todo o caso, nunca depois do momento no qual ocorre a coleta de dados. Dessa forma, qualquer tratamento que se siga à coleta é considerado tratamento posterior e deve preencher o requisito da compatibilidade.

O critério da compatibilidade pode ser formal ou substantivo¹²⁸:

- (i) uma avaliação formal compara as finalidades que foram, inicialmente, indicadas pelo responsável pelo tratamento, habitualmente por escrito, com quaisquer finalidades adicionais para descobrir se essas estavam ou não cobertas[...];
- (ii) uma avaliação substantiva vai além das declarações formais para identificar, quer a finalidade original, quer a nova, dependendo do contexto e de outros fatores.

Conforme o Parecer 3 do Grupo de Estudos 29 (WP 29) da União Europeia, existem fatores-chave a serem considerados durante a avaliação de compatibilidade, entre eles: (i) a relação entre as finalidades pelas quais os dados foram coletados e as finalidades do seu uso secundário: quanto maior o afastamento entre as finalidades da coleta e as finalidades do uso secundário, mais problemática se torna a avaliação da compatibilidade; (ii) o contexto no qual os

¹²⁶ Ibidem.

¹²⁷ UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho** de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 06 mar. 2023.

¹²⁸ UNIÃO EUROPEIA. **Parecer 3 do Grupo de Estudos 29, 2013**. Disponível em: <https://www.gpdp.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC03_2013%20%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_%E7%9B%AE%E7%9A%84%E9%99%90%E5%88%B6_PT.pdf>. Acesso em: 10 abr. 2023.

dados foram coletados e as expectativas razoáveis das pessoas em causa quanto a sua utilização posterior: uma avaliação desta natureza deve incluir, também, uma investigação do equilíbrio de poderes entre a pessoa em causa e o tratamento e o responsável pelo tratamento;(iii) a natureza dos dados e o impacto do tratamento posterior sobre as pessoas em causa: avalia se o tratamento posterior envolve dados sensíveis, tais como dados biométricos, informação genética, dados de localização, e outros tipos de dados pessoais que exigem proteção especial e (iv) as garantias aplicadas pelos responsáveis pelo tratamento para assegurar um tratamento leal e para impedir quaisquer impactos indevidos sobre as pessoas em causa, ou seja, se as finalidades tiverem sido modificadas ou não tiverem sido determinadas com clareza, uma primeira condição necessária (mas nem sempre suficiente) para assegurar a compatibilidade é a nova determinação das finalidades. Em alguns casos, pedir um consentimento separado, específico, para o novo tratamento, pode ajudar a compensar a modificação da finalidade. Contudo, é importante reiterar que os requisitos da compatibilidade do art. 6º, n.1, b) da Diretiva¹²⁹ e o requisito da base legal, inserido neste mesmo documento, em seu art. 7º, são cumulativos. Dessa forma, uma nova base legal, por si só, não pode legitimar o uso secundário de dados que seja, de outro modo, incompatível.

O GDPR, em seu considerando 51, dispõe sobre a restrição de processamento, a qual prevê que os métodos para restringir o processamento de dados pessoais podem incluir, entre outros, mover temporariamente os dados selecionados para outro sistema de processamento, tornar os dados pessoais selecionados indisponíveis para os usuários, ou remover, temporariamente, os dados publicados de um site. Com efeito, nos sistemas de arquivo automatizados, a limitação do tratamento deve, em princípio, ser assegurada por meios técnicos de forma a que os dados pessoais não sejam sujeitos a operações de tratamento ulteriores e não possam ser alterados. O fato de o tratamento de dados pessoais ser restrito deve ser claramente indicado no sistema¹³⁰.

¹²⁹ UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho** de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 06 mar. 2023.

¹³⁰ EUROPEAN UNION. Regulation(EU) 2016/679. **General Data Protection Regulation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 out. 2022.

Contudo, o tratamento de dados pessoais deve ser considerado lícito quando for necessário para proteger um interesse essencial à vida do titular dos dados ou de outra pessoa singular. O tratamento de dados pessoais com base no interesse vital de outra pessoa singular deve, em princípio, ter lugar apenas quando o tratamento não puder ser manifestamente fundamentado em outra base jurídica.

Alguns tipos de processamento podem atender tanto a importantes motivos de interesse público quanto a interesses vitais do titular dos dados, como, por exemplo, quando o processamento é necessário para fins humanitários, e inclusive para monitorar epidemias e sua propagação, ou em situações de emergência humanitária, em particular as situações de desastres naturais e provocadas pelo homem. Nesses contextos, o uso secundário de dados não pode ser considerado ilícito, conforme considerando 46 do GDPR¹³¹.

Nesta mesma linha, o considerando 52 do GDPR¹³² trata das exceções à proibição de tratamento de categorias especiais de dados pessoais, apresentando algumas permissões, tais como: o processamento de dados pessoais no campo do direito do trabalho, direito da proteção social, incluindo pensões e, para segurança da saúde, monitoramento e alerta, prevenção ou controle de doenças transmissíveis e outras ameaças graves à saúde. Conforme esse considerando, tal derrogação pode ser feita para fins de saúde, incluindo a saúde pública e a gestão de serviços de saúde, especialmente a fim de garantir a qualidade e a relação custo-eficácia dos procedimentos utilizados para regularizar os pedidos de prestações e serviços no sistema de seguro de saúde, ou para fins de arquivo de interesse público, fins de pesquisa científica ou histórica ou fins estatísticos.

Como observado, o uso secundário de dados está vinculado ao princípio da finalidade, sujeita-se a avaliação da compatibilidade e apresenta exceções legais.

Na sequência do estudo, tratar-se-á do seu diálogo principiológico no uso secundário de dados e sobre a base legal do interesse legítimo.

¹³¹ Ibidem.

¹³² Ibidem.

3 DIÁLOGO PRINCIPIOLÓGICO NO USO SECUNDÁRIO DE DADOS: TESTE DA BASE LEGAL DO LEGÍTIMO INTERESSE

Primeiramente, faz-se necessário elucidar a semântica do gênero princípio jurídico, para analisar o uso secundário de dados. Princípios são aquelas normas que estabelecem fundamentos para que determinado mandamento seja encontrado¹³³. Karl Larenz¹³⁴ define os princípios como normas de grande relevância para o ordenamento jurídico, na medida em que estabelecem fundamentos normativos para a interpretação e a aplicação do Direito, deles decorrendo, direta ou indiretamente, normas de comportamento¹³⁵. A rigor, os princípios seriam pensamentos diretivos de uma regulação jurídica existente ou possível, mas que ainda não são regras suscetíveis de aplicação, pois lhes falta o caráter formal de proposições jurídicas, isto é, a conexão entre uma hipótese de incidência e uma consequência jurídica. Dessa forma, os princípios indicariam somente a direção em que está situada a regra a ser encontrada¹³⁶.

Para Humberto Ávila, em sua obra *Teoria dos Princípios*¹³⁷, existem três espécies normativas, as quais dependem da dimensão imediata que experimentam. Dessa forma, quando a dimensão for comportamental, está-se diante de uma regra; quando for finalística, de um princípio e quando for metódica, está-se diante de um postulado.

Essa reflexão acerca dos princípios leva em consideração as diretrizes para a sua análise, tendo em vista que os princípios são normas finalísticas, que exigem a delimitação de um estado ideal de coisas¹³⁸, a ser buscado por meio de comportamentos necessários a essa realização. Sendo assim, urge que se especifique os fins ao máximo, pois quanto menos específico for o fim, menos controlável será a sua realização; também necessário que se examinem os casos

¹³³ ESSER, Josef. **Grundsatz und Norm in der Richterlichen Fortbildung des Privatrechts**. 4 ed. Tübingen, Mohr, Siebeck, 1990. Disponível em <https://www.trans-lex.org/101900/_/esser-josef-grundsatz-und-norm-in-der-richterlichen-fortbildung-des-privatrechts-4th-ed-t%C3%Bcbingen-1990>. Acesso em: 26 dez. 2022.

¹³⁴ LARENZ, Karl. **Metodologia da Ciência do Direito**. Trad. José Lamego. 3 ed. Lisboa. Fundação Calouste Gulbenkian, 1997, p. 474.

¹³⁵ Ibidem, p. 475.

¹³⁶ ÁVILA, Humberto. **Teoria dos Princípios: da definição à aplicação dos princípios jurídicos**. 9 ed., rev. E atual. São Paulo: Malheiros, 2018, p. 34-36.

¹³⁷ Ibidem, p 40-51.

¹³⁸ Estado ideal de coisas é definido por Ávila como: “uma situação qualificada por determinadas qualidades. Dessa forma, o estado de coisas se transforma em fim quando alguém aspira conseguir, gozar ou possuir as qualidades presentes naquela situação”. Ibid., p. 92.

paradigmáticos, que iniciam o processo de esclarecimento das condições que compõem o estado ideal das coisas; relevante, da mesma forma, que se verifiquem as similaridades capazes de possibilitar a constituição de grupos de casos que giram em torno da solução de um mesmo problema central e que se verifique a existência de critérios capazes de possibilitar a delimitação de quais são os bens jurídicos que compõem o estado ideal das coisas. E, por último, que se realize o percurso inverso: descubra-se o estado ideal de coisas e os comportamentos necessários a sua promoção e se verifique a existência de outros casos que deveriam ter sido decididos, sempre com base no princípio em análise¹³⁹. Essas são algumas formas de especificação dos fins, segundo Humberto Ávila¹⁴⁰

Por consequência, os princípios estabelecem uma demanda prática, que nada mais é do que adotar o comportamento necessário para alcançar o estado ideal de coisas¹⁴¹.

Os princípios consistem em normas *primariamente complementares e preliminarmente parciais*¹⁴², na medida em que não têm a pretensão de gerar uma solução específica, mas de contribuir, ao lado de outras razões, para a tomada de decisão, pois abrangem somente parte dos aspectos relevantes para essa escolha. Como exemplo, apresenta-se o princípio da proteção dos consumidores, o qual não tem pretensão monopolista, no sentido de prescrever toda e qualquer medida de proteção aos consumidores, mas sim àquelas que possam ser harmonizadas com outras medidas necessárias à promoção de outros fins, como livre iniciativa e propriedade.

Dentro do arcabouço principiológico, extraímos o princípio da finalidade, o qual está inserido no ordenamento brasileiro de proteção de dados, por meio do art. 6º, I, da LGPD¹⁴³, e tem a seguinte redação:

“[...]”- finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, de

¹³⁹ Ibidem, p. 91-94.

¹⁴⁰ Ibidem, p. 94.

¹⁴¹ Ibidem, p. 97.

¹⁴² Humberto Ávila faz uma reflexão acerca dos princípios como critérios da medida de contribuição para a decisão. ÁVILA, Humberto. **Teoria dos Princípios**: da definição à aplicação dos princípios jurídicos. 9 ed., rev. E atual. São Paulo: Malheiros, 2018, p. 76.

¹⁴³ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**.

Brasília, 2018. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 27 dez. 2022.

acordo com o contexto do tratamento[...].”.

A LGPD tem sua construção sob fortes raízes europeias, advindas do GDPR ¹⁴⁴, o qual disciplina a matéria no seu art. 5º, 1., alínea e), como segue:

“[...]1. Os dados pessoais são:

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas, exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (‘imitação da conservação’)[...].”.

Segundo o GDPR, o princípio da limitação da finalidade é um dos seis princípios relativos ao tratamento de dados pessoais, o qual requer que esses sejam:

[...] coletados para finalidades determinadas, explícitas e legítimas e não podendo ser tratados, posteriormente, de uma forma incompatível com essas finalidades; o tratamento posterior, para fins de arquivo de interesse público, ou para fins de investigação científica, ou histórica, ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, n.1[...].

Por meio dessa definição, observa-se que o princípio da limitação da finalidade consiste em dois componentes : (i) a especificação da finalidade e (ii) a compatibilidade com os tratamentos posteriores de dados pessoais. Esse segundo componente, já referido no Item anterior, leva em consideração pressupostos definidos no artigo 6(4) do GDPR¹⁴⁵, o qual trata da licitude do tratamento, e prevê

¹⁴⁴ EUROPEAN UNION. Regulation(EU) 2016/679. General Data Protection Regulation. Disponível em: < <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>> Acesso em 27 dez. 2022.

¹⁴⁵ KOSTADINOVA, Zhasmina Radkova. **Purpose limitation under the GDPR**: can Article 6(4) be automated? Tilburg University. 2017. Disponível em: <https://arno.uvt.nl/show.cgi?fid=146471>>. Acesso em: 27 fev. 2023.

que quando existir tratamento para “fins que não sejam aqueles para os quais os dados pessoais foram recolhidos e não for realizado com base no consentimento do titular de dados[...], deve-se levar em conta”:

- a) qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
- b) o contexto em que os dados foram coletados[...];
- c) a natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9º¹⁴⁶[...];

Essas previsões do artigo 6(4) do GDPR já estavam dispostas no WP29¹⁴⁷, com exceção da letra “e”¹⁴⁸, a qual foi uma inovação do Regulamento Europeu. Entretanto, a legislação brasileira optou pelo desmembramento dos elementos (i) finalidade específica, a qual é composta pela especificidade e pela legitimidade e (ii) compatibilidade, a qual se entende como o processamento de forma compatível com a finalidade para qual os dados foram, originariamente, coletados. Com efeito, a compatibilidade está inserida no princípio da adequação¹⁴⁹.

Uma das mais relevantes bases legais é o consentimento dos titulares, a quem deve ser fornecida a alternativa de anuir sobre a coleta e demais atos englobados na atividade de tratamento. O consentimento pode ser fornecido por escrito ou outro meio, de maneira destacada das demais cláusulas e deve ser específico para as finalidades pretendidas, cabendo ao controlador o ônus da prova sobre a conformidade de sua obtenção, vedado o tratamento mediante vício de consentimento, conforme o art. 8º da LGPD.

Com efeito, o consentimento é um ato do titular cujo efeito será autorizar um determinado tratamento e fundamenta-se na possibilidade de autodeterminação em

¹⁴⁶ O artigo 9º do GDPR prevê o tratamento de categorias especiais de dados pessoais. In: <<https://gdpr-info.eu/>>. Acesso em: 27 fev. 2023.

¹⁴⁷ Substituído pelo EPDB – European Data Protection Board em maio de 2018. In: <<https://edpb.europa.eu/>>. Acesso em: 31 out. 2022.

¹⁴⁸ O art. 6(4) do GDPR, em sua letra “e” prevê a existência de salvaguardas adequadas, que podem ser a cifragem e a pseudonimização. In: <<https://gdpr-info.eu/>>. Acesso em: 27 fev. 2023.

¹⁴⁹ Art. 6º, II- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 27 fev. 2023.

relação aos dados pessoais, da qual ele é instrumento por excelência¹⁵⁰. Uma das preocupações fundamentais da disciplina da proteção de dados pessoais é que o indivíduo não seja manipulado e tenha o poder de decidir acerca da divulgação e utilização de seus dados¹⁵¹.

Contudo, há uma base legal que demanda maior esforço hermenêutico, representa o objeto desta pesquisa, suscita inúmeras dúvidas e reflexões e está disposta no inciso IX do artigo 7º: o legítimo interesse do controlador ou de terceiro.

Essa hipótese tem um caráter excepcional, não somente em razão da ausência de consentimento, mas também diante da ausência de determinação objetiva de seus contornos e efeitos práticos. A fiscalização, conforme a lei brasileira, é mais uma etapa no caminho para a análise do legítimo interesse¹⁵². Para a averiguação dessa base legal, faz-se necessário utilizar o teste de ponderação, que será tratado no item 3.4.

Observa-se um forte arcabouço principiológico contido tanto na LGPD quanto no GDPR, para a proteção ao tratamento de dados. Entretanto, a LGPD faculta a solicitação de um relatório de impacto à proteção de dados ao controlador pela ANPD, quando o tratamento tiver como fundamento o legítimo interesse, o qual será tratado posteriormente. Por outro lado, o artigo 37 da lei brasileira ratifica a necessidade do controlador e do operador manterem registro das operações de tratamento, principalmente quando baseado na hipótese do artigo 7º, inciso IX: “ o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses(...) IX- quando necessário para atender aos interesses legítimos

Bastante relevante para esta pesquisa é o princípio da finalidade, o qual está atrelado ao uso secundário de dados pessoais. O princípio da finalidade é trazido com essa nomenclatura pela lei brasileira e passa a ser analisado no item seguinte.

¹⁵⁰ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021. p. 307.

¹⁵¹ MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei geral de proteção de dados: aspectos relevantes*. Indaiatuba, SP: Editora Foco, 2021. p.13-22.

¹⁵² *Ibidem*, p.179.

3.1 Princípio da Finalidade

A finalidade é o corolário principiológico das leis de proteção de dados. Junto a ela, os princípios da necessidade¹⁵³ e da transparência¹⁵⁴ são fundamentais para entender as questões trazidas pelo uso secundário de dados pessoais¹⁵⁵, fundamentado no legítimo interesse.

Importante entender o papel da finalidade, na proteção de dados, que é uma condição essencial para o tratamento e um requisito prévio à aplicação dos restantes requisitos em matéria de qualidade dos dados. Dessa forma, a *determinação da finalidade* e o conceito de *utilização compatível* contribuem para a transparência, certeza e segurança jurídicas¹⁵⁶; destinam-se a proteger a pessoa, estabelecendo limites para que os responsáveis pelo tratamento utilizem esses dados com lealdade. A limitação da finalidade deverá, por exemplo, evitar a utilização dos dados pessoais dos indivíduos de forma, ou para finalidades adicionais, para que os titulares não deparem com um tratamento inesperado, inadequado ou objetável. Neste ponto, o Parecer 3 da União Europeia já apontava para o cuidado com o uso secundário de dados. Por outro lado, a noção de utilização compatível também oferece algum grau de flexibilidade aos responsáveis pelo tratamento.

Quando se trata de determinação da finalidade, a alínea b) do n. 1 do artigo 6º da Diretiva 95/46/CE dispõe que os dados pessoais podem somente ser recolhidos para finalidades “determinadas, explícitas e legítimas”. Dessa forma, os

¹⁵³ O artigo 6º da LGPD, em seu inciso III, define a necessidade como “a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”. Disponível em: < **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

¹⁵⁴ A LGPD traz, em seu artigo 6º, VI, o conceito de transparência, que nada mais é do que “ a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”. Disponível em:<**Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

¹⁵⁵ GARCIA, Rafael Scaroni. A mercadoria é você: o uso secundário de dados pessoais. UFRGS. Porto Alegre, 2020. Disponível em<<https://www.lume.ufrgs.br/bitstream/handle/10183/248468/001125855.pdf?sequence=1&isAllowed=y>>. Acesso em: 10 abr. 2023.

¹⁵⁶ UNIÃO EUROPEIA. Parecer n. 3, 2013. Disponível em:<https://www.gdpd.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC03_2013%20%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_%E7%9B%AE%E7%9A%84%E9%99%90%E5%88%B6_PT.pdf>. Acesso em: 10 abr. 2023.

dados são recolhidos para certos fins, os quais são a razão de ser das operações de tratamento.

Em primeiro lugar, qualquer finalidade deve ser determinada, ou seja, definida de forma suficiente para permitir a aplicação de quaisquer garantias de proteção de dados necessárias e para delimitar o âmbito da operação de tratamento¹⁵⁷. Em segundo lugar, a finalidade deve ser explícita. Ela deve ser suficientemente inequívoca e claramente expressa. Em terceiro lugar, as finalidades também têm que ser legítimas. A determinação da finalidade ao abrigo do art. 6º¹⁵⁸ da Diretiva e o requisito de um fundamento legal, ao abrigo do art. 7º¹⁵⁹ são, assim, dois requisitos separados e cumulativos¹⁶⁰.

Com relação à finalidade *determinada*, o responsável pelo tratamento deve considerar para qual finalidade os dados serão recolhidos e, conseqüentemente, não poderá recolher dados pessoais que não sejam necessários, adequados ou relevantes para a finalidade da qual pretende se servir.

A determinação da finalidade exige que o responsável pelo tratamento efetue uma avaliação interna, a qual é uma condição necessária de sua responsabilidade¹⁶¹. Por meio dessa análise, o responsável pelo tratamento tem que identificar quais são as finalidades e deve documentar e ser capaz de demonstrar que efetuou uma avaliação interna. Com efeito, por meio do art. 6º, n. 1, alínea b) da Diretiva¹⁶², as finalidades devem ser inferidas, anteriormente, e nunca após o momento em que ocorra o recolhimento dos dados pessoais.

¹⁵⁷ Ibidem, p. 14.

¹⁵⁸ “Os Estados-membros devem estabelecer que os dados pessoais serão objeto de um tratamento leal e lícito, recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades”. UNIÃO EUROPEIA. Diretiva 95/46/CE do PARLAMENTO Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 10 mar. 2023.

¹⁵⁹ “Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se a pessoa, em causa, tiver dado, de forma inequívoca, o seu consentimento ou o tratamento for necessários para prosseguir interesses legítimos do responsável pelo tratamento ou pelo terceiro[...]. UNIÃO EUROPEIA. Diretiva 95/46/CE do PARLAMENTO Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 10 mar. 2023.

¹⁶⁰ Ibidem, p.15.

¹⁶¹ Ibidem, p.15

¹⁶² UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho** de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 06 mar. 2023.

A finalidade deve ser clara e específica, por isso, uma finalidade vaga ou geral, tal como “melhorar a experiência do usuário”, “finalidade de comercialização”, “finalidade de segurança de tecnologia de informação”, sem mais detalhes, em geral não preencherá o critério de ser determinada. Dessa forma, o grau de detalhe no qual uma finalidade deve ser determinada depende do contexto particular da coleta de dados e dos dados pessoais envolvidos. Em alguns casos, será suficiente o recurso a uma linguagem clara para dar uma determinação adequada e, em outros, poderá ser exigido maiores detalhes¹⁶³.

Os dados podem, evidentemente, ser coletados para mais de uma finalidade. Essas finalidades podem estar relacionadas ou não. A questão que se suscita é saber até que ponto o responsável pelo tratamento deve determinar cada uma dessas finalidades distintas, em separado, e que grau de detalhe adicional deve ser indicado. Pode ser útil o conceito de uma finalidade conjunta, para operações de tratamento *relacionadas*, nas quais diversas operações separadas de tratamento podem ter lugar. Dessa forma, os responsáveis pelo tratamento devem evitar a identificação de uma única finalidade alargada, para justificar várias possibilidades de tratamento posterior que, na realidade, só remotamente se relacionam com a finalidade inicial. Em síntese, cada finalidade separada deve ser determinada em detalhe suficiente para permitir avaliar se a coleta de dados pessoais para essa finalidade é ou não conforme à lei e para estabelecer quais as garantias de proteção de dados que se aplicam¹⁶⁴.

Os dados pessoais devem ser recolhidos para finalidades *explícitas*. O objetivo desse requisito é assegurar que a finalidade seja definida sem vaguidão ou ambiguidade quanto ao seu significado ou intenção¹⁶⁵. Em especial, a determinação da finalidade deve ser expressa de um modo tal que possa ser entendido da mesma forma, não apenas pelo responsável pelo tratamento e por terceiros subcontratantes, mas também pelas autoridades de proteção de dados, e pelas pessoas em causa. Esse atributo contribui para a transparência e para a previsibilidade. Além disso, quando o responsável pelo tratamento não cumpre a exigência da Diretiva, em seu art. 6º, n. 1, alínea b)¹⁶⁶, não significa que possa tratar

¹⁶³ Ibidem, p.20.

¹⁶⁴ Ibidem, p.21.

¹⁶⁵ Ibidem, p.21.

¹⁶⁶ UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho** de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva->

os dados pessoais para toda e qualquer finalidade à sua discricção¹⁶⁷ Nem significa que um documento, cuidadosamente elaborado por advogados do responsável pelo tratamento (por exemplo, avisos de proteção de dados enganadores ou contendo termos contratuais desleais) possa legitimar o tratamento para finalidades descritas nessas situações. Em tais casos, será necessário reconstruir as finalidades do tratamento, tendo em mente os fatos do caso.

Com relação ao requisito da legitimidade, significa que a finalidade deve estar conforme à lei, no sentido mais lato. Contudo, dentro dos limites da lei, outros elementos tais como o costume, códigos de ética, cláusulas contratuais, o contexto geral e os fatos do caso podem também ser considerados para determinar se uma determinada finalidade é legítima. Com efeito, isso inclui a natureza da relação subjacente entre o responsável pelo tratamento e as pessoas em causa, seja ou não uma relação comercial. Por consequência, a legitimidade de uma dada finalidade também pode mudar com o tempo, dependendo dos desenvolvimentos científicos e tecnológicos, das mudanças da sociedade e das atitudes culturais¹⁶⁸.

Além dos princípios da LGPD e, principalmente para esta pesquisa, além do princípio da finalidade, as atividades de tratamento de dados pessoais devem observar a boa-fé, a qual será analisada na sequência.

3.2 Boa-fé no tratamento de dados

O art. 7º, § 3º da LGPD¹⁶⁹, refere que o tratamento de dados pessoais, cujo acesso é público, deve considerar a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização. Dessa forma, o elemento boa-fé, que é tratado

[europeia.pdf](#)> Acesso em: 06 mar. 2023.

¹⁶⁷ GRUPO DE TRABALHO DO ARTIGO 29 PARA PROTEÇÃO DE DADOS. **Parecer 03/2023 sobre limitação da finalidade**. Abr. 2013. Disponível em: https://www.gdpd.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC03_2013%20%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_%E7%9B%AE%E7%9A%84%E9%99%90%E5%88%B6_PT.pdf > Acesso em 14 abr. 2023.

¹⁶⁸ Ibidem.

¹⁶⁹ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados(LGPD)**. Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 27 dez. 2022.

no art. 113 do Código Civil¹⁷⁰, promulgado em 2002, conecta, textualmente, boa-fé e usos, havendo, ainda, referência à habitualidade da conduta seguida.

Em similar sentido, o art. 187 do Código Civil estabelece que, quando se trata de limites: "também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes". Efetivamente, boa-fé objetiva significa uma atuação "refletida", pensando no outro, no parceiro contratual, respeitando-o, assim como seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, informando-o, aconselhando-o, cuidando, sem causar lesão ou desvantagem excessiva¹⁷¹.

O princípio geral da boa-fé objetiva, hoje previsto como cláusula geral nos arts. 113, 187 e 422 do Código Civil¹⁷², tem fundamento constitucional na cláusula maior de tutela da dignidade da pessoa humana¹⁷³, chancelando a alteração de mudança de foco do indivíduo isolado e independente para um ser social, integrante da comunidade e que, portanto, deve manter relações sociais de cooperação e solidariedade, a fim de conservar a sua própria subsistência¹⁷⁴.

Não se trata de inovação do Código Civil de 2002, pois essa normatização já estava presente, no ordenamento jurídico, no Código de Defesa do Consumidor¹⁷⁵ de 1990. Essa mudança de paradigma, a que se refere Cláudia Lima Marques¹⁷⁶,

¹⁷⁰ O artigo 113 do Código Civil disciplina que: "os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração". Neste mesmo artigo, em seu parágrafo primeiro, há a previsão de que "a interpretação do negócio jurídico deve lhe atribuir o sentido que (...) corresponder a boa-fé(...).

¹⁷¹ MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 4. ed. revista atualizada e ampliada, incluindo mais de 1.000 decisões jurisprudenciais. Revista dos Tribunais, 2002.

¹⁷² O Código Civil Brasileiro apresenta, em seu art. 422, a seguinte disposição: "os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios da probidade e boa-fé". BRASIL, Lei nº 10.406, de 10 de janeiro de 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em 28 dez. 2022.

¹⁷³ BRASIL. Constituição Federal. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 28 dez. 2022.

¹⁷⁴ BARBOSA, Elisandra Cristina. **A Boa-Fé na Relação Contratual e o Princípio da Confiança**. São Paulo: Pontifícia Universidade Católica de São Paulo, 2008. Disponível em: <<https://repositorio.pucsp.br/bitstream/handle/8274/1/Elisandra%20Cristina%20Barbosa.pdf>> Acesso em: 28 dez. 2022.

¹⁷⁵ BRASIL. Lei 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%Aancias.&text=Art.48%20de%20suas%20Disposi%C3%A7%C3%B5es%20Transit%C3%B3rias> Acesso em: 28 dez. 2022.

¹⁷⁶ MARQUES, Cláudia Lima. **Confiança no Comércio Eletrônico e a Proteção do Consumidor**: um estudo dos negócios jurídicos de consumo no comércio eletrônico). São Paulo: Editora Revista dos Tribunais, 2004.

com a incidência do princípio da boa-fé, está inserida na moldura civil constitucionalista da Política Nacional das Relações de Consumo, no art. 4º, III, o que justifica a aplicação desse princípio para além dos campos do direito do consumidor.

Na linha de observação, análise e reflexão sobre a boa-fé e os usos, as práticas auxiliam a perceber o que é legitimamente esperado. A expectativa do destinatário da manifestação negocial se torna objetiva ou objetivável¹⁷⁷. Como esclarece a autora¹⁷⁸, não se trata da crença subjetiva (o estar de boa-fé), do exame de elementos subjetivos, tal como a íntima convicção (o comportar-se segundo o Direito), mas de uma crença cuja legitimação (expectativa legítima) pode ser averiguada por elementos objetivos, o que normalmente acontece no mercado.

Efetivamente, a conexão entre a boa-fé e os usos (ou as práticas) auxilia a minimizar a tensão entre a segurança jurídica e os traços da informalidade e atipicidade. Faz-se necessário averiguar as práticas e os usos, na medida em que há intensa relação entre a conduta dos agentes e as pautas orientadoras da *ratio* da prática comercial¹⁷⁹. Além disso, constitui fator de segurança considerar o que é considerado habitual, correto e regular, ou seja, aquilo que seria o esperável entre os contraentes, de forma a não causar surpresas desleais.

Além disso, originariamente, o ordenamento alemão já apresentara o mesmo espírito, em seu Bürgerliches Gesetzbuch-BGB¹⁸⁰ (Código Civil), que data de 1896, quando se estipulou o princípio da boa-fé, em seu § 242:

Atuação para boa-fé e confiança: **O devedor é obrigado, na atuação da relação obrigacional, a comportar-se com boa-fé e confiança, como é exigido no tráfego privado**¹⁸¹. (Grifei)

¹⁷⁷ MARTINS-COSTA, Judith. **Mercado e Solidariedade Social entre Cosmos e Taxis**: a boa-fé nas relações de consumo. MARTINS-COSTA, Judith(Org.) **A Reconstrução do Direito Privado**. São Paulo: Revista dos Tribunais, 2002, p. 611-661.

¹⁷⁸ Em sua obra “A Boa-Fé no Direito Privado: critérios para a sua aplicação”, Judith Martins-Costa, em seu capítulo IV, trata da boa-fé em vários segmentos do Direito, tais como: Direito de família, Direito empresarial e Direito do Consumidor. MARTINS-COSTA, Judith. **A Boa-Fé no Direito Privado**: critérios para a sua aplicação. 2 ed. São Paulo: Saraiva, 2019, p. 280-291.

¹⁷⁹ REGO, Anna Lygia Costa. **Confiança & Investimento Estrangeiro**: uma análise do ambiente jurídico brasileiro. São Paulo: Singular, 2013, p. 47.

¹⁸⁰ DEUTSCHLAND. Bürgerliches Gesetzbuch-BGB. 1896, p. 58. Disponível em < <https://www.gesetze-im-internet.de/bgb/BGB.pdf> > Acesso em: 27 dez. 2022.

¹⁸¹ Código Civil alemão, em seu § 242: Der Schuldner ist verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern. Tradução livre.

No General Data Protection Regulation – GDPR- a boa-fé aparece como princípio sob nomenclaturas diversas, conforme a tradução: *lealdade*, *Treu und Glauben* e *fairness*, nas versões portuguesa, alemã e inglesa, respectivamente (art. 5º/1 [a])¹⁸².

Muito frequente é a abordagem conjunta da confiança e da boa-fé, em razão da origem comum na *fides*¹⁸³, contudo não significa que sejam sinônimas. A confiança, enquanto princípio (*Vertrauensprinzip*) é mais ampla do que a boa-fé¹⁸⁴. Entretanto, a boa-fé concretiza e protege a confiança por meio da cláusula geral¹⁸⁵ da boa-fé objetiva.

Nessa mesma linha, destaca Judith Martins-Costa¹⁸⁶ que na vigência do Código Civil de 1916, não obstante a escassez do texto escrito, a boa-fé já vigorava no direito positivo, fosse por força do art. 131 do Código Comercial, fosse por ter sido largamente acolhida por via jurisprudencial, razão pela qual é axiomático que o Direito deva tutelar as condutas segundo a boa-fé. Impensável, atualmente, um código sem a inclusão de preceitos análogos à boa-fé objetiva, eis que esta representa verdadeira mola de acesso a decisões mais flexíveis, que não encontram solução às normas postas, pois impossível ao Direito, enquanto sistema, prever todas as possibilidades de acontecimentos da vida humana, principalmente se for considerada a sua principal tarefa: regulação e pacificação de situações futuras.

Os princípios da boa-fé e da confiança estão entrelaçados e detêm uma relação de complementaridade um para com o outro¹⁸⁷. É do dever de cooperação,

¹⁸² Como bem observado na nota de rodapé n. 12, "(...) o Considerando 38 da Diretiva, na versão em alemão, continha a expressão "Treu und Glauben" que, como se sabe, significa boa-fé objetiva:(...). Na versão em português da Diretiva, todavia, a expressão empregada é de um tratamento de dados que deve ser realizado "de forma lícita e leal". A não utilização da expressão boa-fé ou boa fé objetiva, mas sim de "tratamento leal", repete-se na versão em língua português do GDPR e da Carta Europeia de Direitos Fundamentais". (MENKE, Fabiano; GOULART, Guilherme Damasio. **Segurança da Informação e vazamento de dados**. In: BIONI, Bruno et al. (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN, 2020(ebook), n.p.).

¹⁸³ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraiva, 2018, p. 254.

¹⁸⁴ LARENZ, Karl. **Methodenlehre der Rechtswissenschaft**. 6.ed. Springer, 1991, p. 424; LARENZ, Karl. **Metodologia da ciência do direito**. Tradução de José Lamego. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 1997, p. 603.

¹⁸⁵ MENKE, Fabiano. **A interpretação das cláusulas gerais**: a subsunção e a concreção dos conceitos. Revista de Direito do Consumidor, v. 50, abr.-jun., 2004, p. 9-35.

¹⁸⁶ MARTINS-COSTA, Judith. **Mercado e solidariedade social entre cosmos e taxis**: a boa-fé nas relações de consumo, p. 611/661. In MARTINS-COSTA, Judith (org.). A Reconstrução do Direito Privado: reflexos dos princípios, diretrizes e direitos fundamentais constitucionais no direito privado. São Paulo: Editora Revista dos Tribunais, 2002. p. 95-96.

¹⁸⁷ LISBOA, Roberto Senise. **Confiança contratual**. São Paulo: Atlas, 2012, p.151.

lealdade, de uma conduta proba, que se extraem situações de confiança que devem ser tuteladas, pois o próprio art. 422 do Código Civil coloca a probidade ao lado da boa-fé:” os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé”¹⁸⁸.

Desde o dever-direito de informação até as figuras parcelares da boa-fé e da confiança é como se houvesse a aceitação e a internalização de uma conduta correta e adequada¹⁸⁹: a crença de que os outros- parceiro contratual e terceiro- não se comportarão contraditoriamente ao longo da relação obrigacional e cooperarão para o seu adimplemento.

A privacidade nesse contexto reside, justamente, na fidelidade depositada pelo emissor de uma informação ao seu recipiente, na expectativa de que seus dados serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foram publicizados; particularmente, na esperança de que o trânsito das suas informações pessoais não comprometerá a sua capacidade de livre desenvolvimento da personalidade e de participação social¹⁹⁰.

É exatamente essa confiança que é capaz de reduzir a complexidade¹⁹¹ do fluxo informacional, em substituição à abordagem tradicional da autodeterminação informacional (consentimento específico). A privacidade (consentimento) contextual é como se fosse o óleo das engrenagens de um mercado e de uma série de relações sociais movimentadas e altamente dependentes da troca intensa e dinâmica de dados.

E para construir a reflexão sobre o uso secundário de dados pessoais, faz-se relevante também refletir sobre uma das bases legais de extrema importância, a qual consta do art. 7º ao art. 11 da LGPD: o consentimento no uso secundário de dados, com um olhar para a lei brasileira e para o GDPR.

¹⁸⁸ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021.

¹⁸⁹ LISBOA, Roberto Senise. **Confiança contratual**. São Paulo: Atlas, 2012, p.149.

¹⁹⁰ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p.235.

¹⁹¹ MENEZES CORDEIRO, Antônio Manuel da Rocha. **Da boa-fé no direito civil**. Coimbra: Almedina, 2011, p.1242.

3.3 Consentimento no uso secundário dos dados

O consentimento do titular para o tratamento de dados pessoais¹⁹² é um dos pontos mais sensíveis de toda a disciplina de proteção de dados; por meio dele, o direito civil tem a oportunidade de estruturar, a partir da consideração da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão¹⁹³.

A qualificação jurídica do consentimento para o tratamento de dados pessoais não deve ser tomada como uma tarefa que visa ao enquadramento da sua disciplina em um esquema preconcebido, no qual o tratamento de dados pessoais deva submeter-se aos modelos de uma determinada concepção da autonomia privada¹⁹⁴. Ou seja, a especificidade do consentimento, no caso da proteção dos dados pessoais, pede uma funcionalização de sua própria natureza jurídica, e ao intérprete cabe integrar essa disciplina do consentimento com os efeitos que dela são pretendidos¹⁹⁵. Dessa forma, não parece apropriada a caracterização de uma natureza puramente negocial a esse consentimento. Se fosse dessa maneira, seria legitimada a inserção do consentimento em estruturas contratuais, dificultando a sua valoração em função dos atributos da personalidade que estão em jogo. Ou seja, o consentimento para o tratamento de dados pessoais atinge, diretamente, uma série de elementos da própria personalidade, ainda que não no sentido exato da disposição desses elementos. O consentimento assume com mais propriedade as vestes de um ato do titular, cujo efeito será de autorizar um determinado tratamento para os dados pessoais¹⁹⁶. Conforme afirma a doutrina¹⁹⁷, “quem consente não exprime, propriamente, a ausência de interesse na proteção de seus dados, nem a ela renuncia, porém lança mão de um verdadeiro ato de exercício do direito de autodeterminação na esfera das escolhas pessoais(...)”. Esse exercício de direito se manifesta, mais que no momento do consentimento em si, que teria o efeito de

¹⁹² “O consentimento, nas matérias que envolvem diretamente a personalidade, assume hoje um caráter bastante específico. A evolução tecnológica é responsável por um crescimento das possibilidades de escolha que podem ter reflexos diretos para a personalidade, visto que várias configurações possíveis, referentes tanto à privacidade quanto à imagem, identidade pessoal, disposições sobre o próprio corpo e outras, dependem, em alguma medida, de uma manifestação da autonomia privada”. GORMLEY, Ken. **One hundred years of privacy**. Wisconsin Law Review, n. 1335, 1992, p. 1396.

¹⁹³ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 143.

¹⁹⁴ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 315.

¹⁹⁵ *Ibidem*.

transmudar a informação pessoal em um bem jurídico, na possibilidade de concedê-lo ou negá-lo e reside, exatamente, nesse poder que, caso limitado de alguma forma em uma estrutura negocial, perderia sua razão de ser¹⁹⁸.

Portanto, verifica-se que a fundamentação desse consentimento reside na possibilidade de autodeterminação em relação aos dados pessoais, e que essa deve ser levada em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos desse consentimento¹⁹⁹. Com efeito, existem dois planos de análise possíveis: no primeiro, o consentimento é o instrumento por excelência dessa autodeterminação e, portanto, de um aspecto da tutela da pessoa. Contudo, em outro plano, o consentimento representa o papel de instrumento de legitimação para que esses dados sejam, em alguma medida, utilizados por outra pessoa²⁰⁰.

Esse balanceamento não é simples. Sendo assim, mesmo em uma perspectiva de proteção da pessoa como valor preponderante, é forçoso reconhecer que existem efeitos de naturezas diversas que dependem, diretamente, do consentimento. Dessa forma, Davide Messinetti, quando descreve esse fenômeno, propõe separar esse consentimento em dois aspectos ou momentos²⁰¹: (i) consentimento como condição de acesso na esfera privada, o qual estaria ligado ao poder de autodeterminação e (ii) consentimento como fonte da regra que confirma a *fattispecie* circulatória, quando legitima a inserção desses dados pessoais no mercado²⁰².

Quando se trata do contexto da lei brasileira²⁰³, a (LGPD), em seu art. 5º, XII, define o conceito do consentimento como sendo “a *manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus*

¹⁹⁶ MESSINETTI, Davide. **Circolazioni dei dati personali e dispositivi di regolazioni dei poteri individuali**. Rivista Critica del Diritto Privato, 1998, p.339-407.

¹⁹⁷ RESTA, Giorgio. **Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali**. Rivista Critica del Diritto Privato. 2000, p. 307.

¹⁹⁸ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 315.

¹⁹⁹ Ibidem, p.316.

²⁰⁰ Ibidem, p.316.

²⁰¹ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 316.

²⁰² MESSINETTI, Davide. **Circolazioni dei dati personali e dispositivi di regolazioni dei poteri individuali**. Rivista Critica del Diritto Privato, 1998, p.351-342.

²⁰³ A Lei Geral de Proteção de Dados, em seu art. 9º, dispõe que “o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I- finalidade específica do tratamento[...]”.

dados pessoais para uma finalidade determinada". Pela análise da lei, observa-se que esse consentimento é realizado para uma finalidade precisa e única.

Outro comando da LGPD, em seu art. 9º, § 2º, prevê que "na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais, não compatíveis com o consentimento original, o controlador deverá informar, previamente, ao titular, sobre as mudanças da finalidade, podendo o titular revogar o consentimento, caso discorde das alterações". Contudo, no que se refere ao tratamento de dados pessoais de crianças, conforme art. 14, §3º da LGPD, esses poderão ser coletados *sem a necessidade do consentimento de um dos pais ou pelo responsável legal*, quando a coleta for necessária para contatá-los; e serão utilizados uma única vez, sem armazenamento, ou para a sua proteção. Entretanto, mesmo com essa ressalva, em nenhum caso os dados das crianças poderão ser repassados a terceiro, sem o consentimento dos pais ou do responsável legal.

Consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com fundamento na expressão da sua vontade. Sua utilização como instrumento paradigmático, para a tutela de dados pessoais, deve ser observada a partir de seus efeitos na sua concreta aplicação ao caso dos dados pessoais e seus efeitos – o que já foi denominado como *mito do consentimento*²⁰⁴ e deve ser analisado sob dois aspectos. O primeiro é que o consentimento se apresenta como um elemento acessório, sempre ligado a uma situação que o fundamenta, a qual pode ser a realização de um contrato, a inscrição em um concurso, o registro em um hospital, entre outras²⁰⁵. Um outro fator é que o consentimento para o tratamento de dados pessoais pode se apresentar como um procedimento, aparentemente, inócuo, ou seja, as consequências que dele podem advir podem ser pouco nítidas e difíceis de serem identificadas.

Atualmente, quase todas as coisas a que os indivíduos se arriscam, especialmente online, apresentam avisos de privacidade longos e complexos, escritos por advogados e para advogados, os quais exigem, no final da nota de esclarecimento, o '*consentimento*' ou o '*abandono*' do uso dos serviços desejados. Essa escolha binária não é o que a arquitetura da privacidade imaginou há quatro décadas atrás, quando essa interface foi desenvolvida, com o intuito de empoderar

²⁰⁴ RODOTÀ, Stefano. **Elaboratori Elettronici e controllo sociale**. Bologna. Il Mulino, 1973, p. 341.

²⁰⁵ DONEDA, Danilo. **Da Privacidade à Proteção de Dados**: fundamentos da lei geral de proteção de dados. 3 ed. São Paulo: Thomson Reuters Brasil, 2021, p. 312.

os indivíduos, fazendo-os tomar decisões informadas sobre o processo de seus dados pessoais. Na prática, certamente, não foi o melhor mecanismo para garantir que a privacidade da informação ou o fluxo livre da informação estivesse protegido²⁰⁶.

Igualmente, o desafio está no fato de que na era do 'Big Data'²⁰⁷, muito do valor da informação pessoal não está visível no momento da coleta, quando o *aviso* e o *consentimento* são, normalmente, apresentados. Em razão de que os usos futuros exigem contatar com os indivíduos para um novo consentimento, muitos desses usos, os quais têm benefícios sociais e individuais significantes, podem ser extremamente valiosos. Com efeito, os usuários acabam por não implementar uma forma de garantir a segunda ou terceira anuência do titular desses dados. Além disso, o que costumava ser uma relação relativamente simples entre os indivíduos, agentes de tratamento e usuários dos dados pessoais, tem se tornado complicada quando um conjunto de dados são combinados e os processadores e usuários se modificam. Essa ordem lógica se torna ainda mais obscura para os titulares, quando necessitam compreender a complexidade da transação na qual eles são solicitados a consentir. Para Cate e Mayer-Schönberger, 'Big Data' não é apenas grande, mas também coleta e processa com tanta velocidade que transforma as oportunidades de consentir em um fardo inaceitável para a maioria das pessoas.

Tendo em vista esse panorama²⁰⁸, a realidade desafia o atual e dominante mecanismo de privacidade do *aviso* e *consentimento*. Esse processo pode deixar a privacidade dos indivíduos seriamente exposta, pois os titulares dos dados são forçados a tomar decisões excessivamente complexas, baseadas em informações

²⁰⁶ CATE, Fred H. and MAYER-SCHÖNBERGER, Viktor. **Notice and Consent in a World of Big Data**. Indiana: Maurer School of Law, 2013, p. 67-73. Disponível em: <<https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3662&context=facpub>>. Acesso em: 18 jan. 2023.

²⁰⁷ "Big data é um termo para configuração abundante de dados, os quais têm a mais variada e complexa estrutura, a qual apresenta dificuldade de armazenamento, análise e visualização para processos e resultados futuros. Big data e sua análise são o centro das ciências modernas e dos negócios. Seus dados são gerados por meio de transações online, e-mails, vídeos, áudios, imagens, registros em rede, posts, sites de busca, registros médicos, interações sociais de networking, dados científicos, sensores, celulares e seus aplicativos. Eles são armazenados em banco de dados e crescem enormemente, tornando-se difícil capturá-los, armazená-los, gerenciá-los, analisá-los e visualizá-los via ferramentas de software de banco de dados". Definição em: **Big Data: A Review**. SAGIROGLU; Seref; SINANC, Duygu. Turkey Gazy University, 2014. Disponível em: <https://academics.uccs.edu/~ooluwada/courses/datamining/ExtraReading/Big_data_A_review.pdf>. Acesso em: 18 jan. 2023.

²⁰⁸ CATE, Fred H. and MAYER-SCHÖNBERGER, Viktor. **Notice and Consent in a World of Big Data**. Indiana: Maurer School of Law, 2013, p. 67-73. Disponível em: <<https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3662&context=facpub>>. Acesso em: 18 jan. 2023.

limitadas, enquanto os processadores de dados podem, talvez muito facilmente, apontar para a formalidade do *aviso e consentimento* e, desse modo, tentar se eximir muito de sua responsabilidade. Ao mesmo tempo, mecanismos de privacidade corrente podem, indevidamente, interferir no potencial de inovação do uso dos dados. Esses desafios requerem uma reavaliação racional do panorama da privacidade, tão bem como uma avaliação da combinação ideal de mecanismos aptos a proteger a privacidade da informação em uma sociedade mundial, a qual está começando a perceber o valor latente do ‘Big Data’.

Quando se observa o GDPR, esse conceito de consentimento, em seu art. 4º, nº 11, é, relativamente, mais estendido:

[...]“uma manifestação de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”.

Com relação à natureza voluntária da base legal do consentimento²⁰⁹, o art. 7º, §4º do Regulamento Geral de Proteção de Dados europeu declara que “ao avaliar se o consentimento é dado, livremente, há que se verificar, com a máxima atenção se a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais, o qual não é necessário para a execução desse contrato”.

Com efeito, os considerandos do GDPR tratam de algumas questões mais específicas da exigência do consentimento²¹⁰. Como exemplo, pode-se citar a terceira frase do nº 42 dos considerandos, a qual esclarece que “só se deve assumir que o titular deu seu consentimento, voluntariamente, se ele fizer uma escolha genuína ou livre e está, portanto, em condições de recusar ou retirar o consentimento, sem sofrer desvantagens”. Além disso, o considerando 43 adiciona o seguinte:

“A fim de assegurar que o consentimento é dado, de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados

²⁰⁹ HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**: transformação digital-desafios para o direito. 2 ed. Rio de Janeiro: Forense, 2022, p. 83-92.

²¹⁰ Ibidem.

e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução”.

Com relação ao carácter voluntário do consentimento, ele é um elemento importante para a proteção da autonomia dos usuários-titulares²¹¹. Entretanto, se determinados serviços são, praticamente, indispensáveis aos titulares, por razões profissionais e pessoais importantes, como - por exemplo - atuar no mundo do trabalho ou nas autoridades públicas ou para a participação social na comunicação, e se não existem serviços concorrentes da qualidade comparável, os titulares de dados não têm, praticamente, outra escolha senão dar seu consentimento. O pressuposto de que esse consentimento é voluntário é algo ficcional.

Também sobre esse tema, o Tribunal Constitucional Alemão identificou esse dilema, e elaborou a seguinte formulação: “serviços básicos para o público em geral estão sendo cada vez mais prestados por empresas privadas, muitas vezes poderosas, em todas as áreas da vida, com base em extensas coletas de dados pessoais e medidas de processamento de dados. Dificilmente, os indivíduos terão outra escolha senão a de revelar, em grande medida, seus dados pessoais para as empresas, caso não queiram ser excluídos desses serviços básicos. Diante da capacidade de manipulação, reprodução e de possibilidades de divulgação, praticamente ilimitadas dos dados, tanto em termos de tempo como de espaço, bem como sua imprevisível capacidade de recombinação em procedimentos de processamento não transparentes, por meio de algoritmos incompreensíveis, os indivíduos podem se tornar amplamente dependentes ou ficar expostos a condições contratuais impositivas”²¹². Mesmo que não se trate dos pressupostos para a

²¹¹ Ibidem.

²¹² BverfG- **Tribunal Constitucional Federal da Alemanha**. Decisão de 6 de novembro de 2019, nº 88. Disponível em: < https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html >. Acesso em 16 jan. 2023.

validade do consentimento de um titular, a importância das circunstâncias citadas devem ser levadas em consideração para a avaliação da natureza voluntária de um consentimento²¹³.

Com efeito, é curioso notar que o progresso geracional das leis de proteção de dados pessoais é marcado pela gradual adjetivação empregada ao consentimento, como sendo uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada²¹⁴; mas, ao mesmo tempo, verifica-se que há um certo *descaso normativo* com relação à forma pela qual ele deveria ser operacionalizado²¹⁵. Trata-se, assim, de uma espécie de *hipertrofia do consentimento* junto ao restante do corpo normativo de proteção de dados pessoais, o que é diagnosticado por um *desenvolvimento incompleto* dos seus outros membros que preencheriam a citada adjetivação e dariam concretude à prometida esfera de controle dos dados pessoais.

Em meio a esse descompasso, o próprio mercado se autorregulou. O surgimento das políticas de privacidade²¹⁶ é uma resposta a essa demanda regulatória. Ocorre que tal mecanismo tem se mostrado falho por inúmeras razões, seja porque ele reforça a assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais²¹⁷.

Em relação às políticas de privacidade, nota-se que são, por excelência, um contrato de adesão²¹⁸. A massificação²¹⁹ das relações contratuais ordinárias de consumo é também característica marcante no mercado informacional.

²¹³ HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital**: transformação digital - desafios para o direito. 2 ed. Rio de Janeiro: Forense, 2022, p. 83-92.

²¹⁴ Conceito inserido na LGPD, em seu art. 5º, XII. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

²¹⁵ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p.166.

²¹⁶ Correlacionando a autorregulação, por meio do surgimento das políticas de privacidade, no mercado americano, com o padrão normativo da autodeterminação informacional advindo das FIIPs: SOLOVE, Daniel; HARTZOG, Woodrow. **The FTC and the New Common Law of Privacy**. **Columbia Law Review**, 114, p. 583-676, 2014. Disponível em: <<https://dx.doi.org/20.2139/ssrn.2312913>> Acesso em 10 nov. 2023.

²¹⁷ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p.166.

²¹⁸ MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime nas relações contratuais. São Paulo: Revista dos Tribunais, 2011, p.74-75;86-87.

²¹⁹ MIRANDA, Custódio da Piedade Ubaldino. **Contrato de Adesão**. São Paulo: Atlas, 2002, p.13-16.

Essa dinâmica dos contratos de adesão assinala, sobretudo, a assimetria de forças das relações de consumo, na medida em que o seu elo mais forte fixa, unilateralmente, o programa contratual²²⁰. Em termos de proteção de dados pessoais, isso significa que será o fornecedor quem determinará os rumos do fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada²²¹. Sendo assim, e de acordo com essa dinâmica contratual, os usuários não têm o poder de barganhar para colocar em curso as suas preferências de privacidade. Essa conjuntura, somada à proeminência de uma série de plataformas que condicionam a própria participação social do cidadão, acaba por tornar falaciosa a prometida esfera de controle dos dados pessoais²²². É nesse contexto que a lógica do “tudo” ou “nada”²²³ das políticas de privacidade acaba por mistificar a autodeterminação informacional²²⁴. As políticas de privacidade, ora escoradas nessa dinâmica dos contratos de adesão, têm sido uma ferramenta inapropriada para garantir ao consumidor o controle dos seus dados pessoais.

A especificidade do consentimento, no caso da proteção dos dados pessoais, pede igualmente uma funcionalização de sua própria natureza jurídica e ao intérprete cabe integrar essa disciplina do consentimento com os efeitos que dela são pretendidos²²⁵.

Nesse sentido, a atualização contínua dos termos de uso causa instabilidade e retira qualquer perspectiva de controle já que, na maioria das vezes, eles se tornam mais invasivos em relação as suas versões anteriores. Com efeito, é elucidativo o estudo da *Electronic Frontier Foundation/EFF* que criou uma *timeline* – para usar o próprio termo da rede social em questão – das políticas de privacidade do *facebook*, constatando-se que houve uma erosão de uma série de funcionalidades da plataforma e das garantias contratuais contidas nas antigas políticas de privacidade, que possibilitavam aos seus usuários um maior controle

²²⁰ MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime nas relações contratuais. São Paulo: Revista dos Tribunais, 2011, p.74-75;86-87.

²²¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p.167.

²²² *Ibidem*.

²²³ MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime nas relações contratuais. São Paulo: Revista dos Tribunais, 2011, p.79.

²²⁴ SCHWARTZ, Paul M. **Privacy and democracy in cyberspace**. *Vanderbilt law review*, v.52, 1999, p.825.:”In this fashion, privacy consent

²²⁵ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021. p. 315.

sobre os seus dados pessoais²²⁶. Esse exemplo demonstra que essa ferramenta contratual tem sido utilizada para o esvaziamento de qualquer esfera de controle dos dados pessoais²²⁷. Com efeito, tais termos contratuais sujeitam o usuário, muitas vezes, a dar um cheque em branco, cujo “preenchimento”, ou seja, a utilização de dados, fica ao arbítrio daquele que estipulou, unilateralmente, as suas cláusulas contratuais e, nesse contexto, questiona-se a possibilidade da proteção contratual do consumidor. Seria viável? Por meio do Código de Defesa do Consumidor, a resposta é não²²⁸. A razão da negativa é porque a proteção contratual do consumidor tem sido, por excelência, um controle *ex post*, mediante a declaração de nulidade das cláusulas contratuais abusivas²²⁹.

Por essas razões, a proteção contratual do consumidor, no âmbito das políticas de privacidade, não deve ser vista como o mecanismo ideal para a proteção da dados pessoais. Ao contrário, deve ser encarada como uma ação paliativa se a causa regulatória primária falhar, qual seja, o empoderamento *ex ante* do cidadão, para exercer um controle genuíno sobre os seus dados pessoais. Também nesse sentido, tal ferramenta contratual está longe de ocasionar o empoderamento. Com efeito, os seus textos longos e de difícil compreensão são incapazes sequer de estabelecer uma comunicação adequada²³⁰ para que o titular dos dados possa racionalizar um processo de tomada de decisão²³¹.

²²⁶ BAROCAS, Solon; NISSENBAUM, Helen. **Big Data’s End Run Around Consent and Anonymity**. In: LANE, J.; STODDEN, V.; BENDER, S.; NISSENBAUM, H. (Ed.) *Privacy, Big Data and the Public Good*. CAMBRIDGE: Cambridge University Press, 2014.,. 44-75.

²²⁷ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p.168.

²²⁸ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p.169.

²²⁹ O rol exemplificativo de cláusulas abusivas está contido no Código de Defesa do Consumidor, em seu art. 51. Lei 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%Aancias.&text=Art..48%20de%20suas%20Disposi%C3%A7%C3%B5es%20Transit%C3%B3rias> Acesso em: 28 dez. 2022.

²³⁰ BIONI, Bruno Ricardo. **O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo ‘Lulu’**. *Revista de Direito do Consumidor*, v. 94, p.283-326, 2014.

²³¹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p.169.

Há um famoso estudo de pesquisadoras da *Carnegie Mellon University*²³² que avaliaram que os usuários despenderiam, ao menos, 201 horas²³³, o que seria equivalente a U\$3,354 – para que pudessem ler os termos de uso dos *websites*, que são, em média, acessados por um usuário americano.

Por outro lado, ao fornecedor e prestador de produtos e serviços não cabe analisar, singularmente, cada instrumento contratual, já que ele é o mesmo para toda a sua base de consumidores. Já o consumidor precisa analisar todos os instrumentos contratuais das suas relações, uma vez que eles variam de acordo com cada fornecedor. A massificação dos instrumentos contratuais é, portanto, unilateral, sendo esta a razão pela qual a suscitada externalidade negativa do seu custo de leitura atinge somente os consumidores²³⁴.

Deve-se pensar, nesse contexto, como a massificação de tais relações poderia ser inversa ou, ao menos, uma via dupla. Relevante seria investigar como a tecnologia poderia massificar as escolhas dos consumidores sobre o trânsito dos dados pessoais para toda a miríade de atores do mercado informacional²³⁵. Diferentemente das relações ordinárias de consumo, essas novas relações são estruturadas sobre um mesmo objeto de troca: os dados pessoais, que são o *trade-off*²³⁶ desses novos modelos de negócio; ao contrário da relação *off-line*, em que a contrapartida de um bem de consumo é fixada, individual e pecuniariamente, para cada relação de consumo²³⁷.

Importante perquirir se há novas formas de concretizar a prometida esfera de controle sobre os dados pessoais, se há novas ferramentas que sejam tão líquidas e fluidas quanto é o fluxo de dados pessoais, e que percorram, universalmente, todo o ambiente on-line. Isso porque toda a técnica contratual off-line das políticas de privacidade é uma ferramenta sólida que se presta para, estaticamente, exercer um controle dos dados para cada espaço e relação singular

²³² MACDONALD, Aleecia M.; CRANOR, Lorrie Faith. **The Cost of Reading Privacy Policies**. *Journal of Law and Policy for Information Society*, v.4, 2008, p. 565.

²³³ *Ibidem*, p.564.

²³⁴ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p.169.

²³⁵ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p.170.

²³⁶ Trade-off é a análise daquilo que se perde em comparação com aquilo que se ganha ao fazer determinada escolha. Esse conceito pode ser aplicado em diferentes situações em que haja agentes econômicos diante de escolhas. Disponível em: <<https://www.ibccoaching.com.br/portal/coaching-e-financas/trade-off-o-que-e-e-qual-a-sua-importancia/>>. Acesso em: 24 abril. 2023.

²³⁷ *Ibidem*.

do ambiente eletrônico²³⁸. Por essa razão, esse ferramental não se ajusta à complexidade do fluxo informacional das renovadas relações de consumo, sobrecarregando o cidadão do século XXI²³⁹.

Recentemente, em 24 de fevereiro de 2023, foi publicada uma resolução da Autoridade Nacional de Proteção de Dados²⁴⁰ - Resolução CD/ANPD nº 4²⁴¹ - a qual trata sobre uso secundário não consentido. Essas infrações são classificadas em leve, média ou grave, conforme os critérios previstos no Regulamento de Dosimetria e Aplicação de Sanções Administrativas e, também segundo a natureza e a gravidade das infrações e dos direitos pessoais afetados. O art. 26 da Seção XII da Resolução²⁴² trata da “proibição parcial ou total do exercício de atividades relacionadas a tratamentos de dados”, a qual inclui, entre outras determinações, sanções referentes ao tratamento com fins ilícitos, ou sem amparo em hipótese legal.

Depois de analisar o *consentimento* no uso secundário de dados, o item seguinte tratará do legítimo interesse e a autorização legal ao uso posterior de dados, apresentando disposições legais, na LGPD e no GDPR, e comandos normativos que precedem essas leis.

²³⁸ LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. **A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo art. 7, incisos VIII e IX do Marco Civil da Internet a partir da human computer interaction e da privacy by default.** In: DE LUCCA, Newton; SIMÃO FILHO, A dalberto; LIMA, Cíntia Rosa Pereira de (COORD.). Direito e Internet III: marco civil da internet. São Paulo: Quartier Latin, 2015, t. I, p.263-290.

²³⁹ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento.** 3. ed., Rio de Janeiro: Forense, 2021, p.171.

²⁴⁰ A ANPD é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. In: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/perguntas-frequentes-2013-anpd#c1> >. Acesso em: 07 mar. 2023.

²⁴¹ ANPD. **Resolução CD/ANPD nº4.** Disponível em:<<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucao4CDANPD24.02.2023.pdf/view> >. Acesso em: 07 mar. 2023.

²⁴² Está previsto na Resolução CD/ANPD nº 4, Seção XII, a seguinte disposição: Da Proibição Parcial ou Total do Exercício de Atividades Relacionadas a Tratamento de Dados e, mais especificamente, no art. 26: “A sanção de proibição do exercício de atividades relacionadas a tratamento de dados pessoais consiste no impedimento parcial ou total das operações de tratamento de dados pessoais, e poderá ser aplicada nos casos em que: I - houver reincidência em infração punida com suspensão parcial do funcionamento do banco de dados ou suspensão do exercício da atividade de tratamento dos dados pessoais; II - ocorrer tratamento de dados pessoais com fins ilícitos, ou sem amparo em hipótese legal; ou III - o infrator perder ou não atender as condições técnicas e operacionais para manter o adequado tratamento de dados pessoais. In: ANPD. **Resolução CD/ANPD nº4.** Disponível em:<<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucao4CDANPD24.02.2023.pdf/view> >. Acesso em: 07 mar. 2023.

3.4 O legítimo interesse e a autorização legal ao uso posterior de dados

A base legal legítimo interesse pode justificar o uso posterior de dados, por criar algumas possibilidades de tratamento.

Fundamental se faz abordar os textos legais da Diretiva 95/46/CE e do GDPR, em razão da influência direta do processo legislativo europeu na lei brasileira, devido ao longo processo de construção de um consenso transnacional acerca dos princípios básicos, que regem a matéria de proteção de dados pessoais.

A previsão do legítimo interesse, em relação à Diretiva 95/46/CE, é trazido pelo legislador tanto no preâmbulo da norma, em seu considerando 30²⁴³, quanto na Seção II, art. 7º, f, intitulada “princípios relativos à legitimidade do tratamento de dados”. Contudo, essa legislação não trouxe detalhes sobre como se daria a análise da correta aplicação do legítimo interesse, em caso concreto, o que gerou aplicações divergentes desta base legal em estados membros da União Europeia, uma vez que a diretiva necessitava ser transposta para cada estado-membro para ser vinculante. Dessa forma, a execução do art. 7º, alínea f, divergiu, substancialmente, de um estado para o outro²⁴⁴.

²⁴³ [...] (30) Considerando que, para ser lícito, o tratamento de dados pessoais deve, além disso, ser efetuado com o consentimento da pessoa em causa ou ser necessário para a celebração ou execução de um contrato que vincule a pessoa em causa, ou para o cumprimento de uma obrigação legal, ou para a execução de uma missão de interesse público ou para o exercício da autoridade pública, ou ainda para a realização do interesse legítimo de uma pessoa, desde que os interesses ou os direitos e liberdades da pessoa em causa não prevaleçam; que, em especial, para assegurar o equilíbrio dos interesses em causa e garantir, ao mesmo tempo, uma concorrência real, os Estados-membros são livres de determinar as condições em que os dados pessoais podem ser utilizados e comunicados a terceiros no âmbito de atividades legítimas de gestão corrente das empresas e outros organismos que, do mesmo modo, podem precisar as condições em que a comunicação a terceiros, de dados pessoais, pode ser efetuada para fins de mala direta ou de prospecção feita por uma instituição de solidariedade social ou outras associações ou fundações, por exemplo de caráter político, desde que respeitem as disposições que permitem à pessoa em causa opor-se, sem necessidade de indicar o seu fundamento ou de suportar quaisquer encargos, ao tratamento dos dados que lhe dizem respeito; [...] Artigo 7º Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se: [...] f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n. 1 do artigo 1º. In: UNIÃO EUROPEIA. Diretiva 95/46/CE do PARLAMENTO Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 06 mar. 2023.

²⁴⁴ BALBONI, Paolo; COOPER, Daniel; IMPERIALI, Rosario; MACENAITE, Milda. Legitimate interest of the data controller: New Data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law*, Oxford, v.3, n.4, p. 244-261, 2013.

O legítimo interesse, historicamente, tem sido encarado como a mais flexível²⁴⁵ das bases legais de tratamento de dados no regime do direito europeu. Essa base legal ganhou ainda mais relevância diante da emergência de tecnologias e no contexto de uma economia baseada no uso intensivo de dados²⁴⁶. Tal como o consentimento, no início do progresso geracional das leis de proteção de dados, o legítimo interesse ganhou o status de uma nova “carta coringa regulatória”, para abraçar uma miríade de possíveis usos de dados²⁴⁷.

A antiga diretiva europeia de proteção de dados, ao prever o legítimo interesse, não detalhava os critérios para a sua aplicação. Foi essa situação que levou à realização de estudos pelo Grupo de Trabalho do art. 29, os quais confirmaram a falta de harmonização na interpretação e no uso do legítimo interesse. Com efeito, passou-se a defender a necessidade de criação de uma orientação adicional para uso entre os países membros da União Europeia, especialmente considerando que o interesse legítimo poderia suplantiar os direitos e liberdades fundamentais dos titulares dos dados²⁴⁸.

Nessa conjuntura, o GT 29 divulgou, em 09 de abril de 2014, um estudo compilado no documento intitulado como Parecer 06/2014²⁴⁹, o qual contém diretrizes e orientações para a aplicação do interesse legítimo como fundamento para o tratamento para dados pessoais. A partir do documento foi apresentada uma definição sobre o legítimo interesse, nos seguintes termos²⁵⁰:

O conceito de “interesse está estreitamente relacionado ao conceito de “finalidade”, referido no artigo 6º da diretiva, embora se trate de conceitos distintos. Em matéria de proteção

²⁴⁵ UK Information Commissioner’s Office. Guide to the general data protection regulation(GDPR). Disponível em:<<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>>. Acesso em: 06 mar. 2023.

²⁴⁶ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed.,Rio de Janeiro: Forense, 2021, p. 238.

²⁴⁷ Ibidem, p. 239.

²⁴⁸ BALBONI, Paolo; COOPER, Daniel; IMPERIALI, Rosario; MACENAITE, Milda. Legitimate interest of the data controller: New Data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law*, Oxford, v.3, N.4, P. 244-261, 2013.

²⁴⁹ GRUPO DE TRABALHO DO ARTIGO 29º DA DIRETIVA 95/46/CE. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento do dados da aceção do artigo 7º da Diretiva 95/46/CE. Disponível em:<https://www.gdpd.gov.mo/pt/references_detail/article/l3mqmkcr.html>. Acesso em: 09 mar. 2023.

²⁵⁰ JOELSONS, Marcela. **O interesse legítimo do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu**: desafios e caminhos para uma aplicação no cenário brasileiro. In: MENKE, Fabiano; VALLE DRESCH, Rafael de Freitas(Org.).LEI GERAL DE PROTEÇÃO DE DADOS. Ed. Foco, 2021, p.123.

de dados, a “finalidade” é a razão específica pela qual os dados são tratados. Por outro lado, um interesse é o objetivo mais abrangente que o responsável pelo tratamento pode ter no tratamento, ou o benefício que o responsável pelo tratamento retira - ou que a sociedade pode retirar do tratamento²⁵¹.

Ao prever a possibilidade de tratamento de dados, quando necessário para atender aos interesses da pessoa natural ou jurídica que tem o poder de decisão, a lei entrega um termo amplo, um conceito jurídico indeterminado. É uma hipótese flexível cujo conteúdo e limites não são determinados *a priori* e sua caracterização depende da avaliação de sua conformidade. Seus efeitos jurídicos, entretanto, já estão previstos na lei e o aplicador deve apenas utilizar, no fato concreto, o elemento semanticamente vago para individualizar a hipótese abstrata. De forma diversa se apresentam as cláusulas gerais, as quais são normas que funcionam como válvulas de segurança, conferindo ao intérprete o poder de construir o significado da norma²⁵².

A LGPD estabeleceu as figuras do controlador²⁵³ e do operador²⁵⁴, denominados como agentes de tratamento. O que os diferencia é o poder decisório sobre o tratamento que se dará aos dados pessoais: enquanto o primeiro decide, o segundo cumpre as suas determinações²⁵⁵. Em outras palavras, o responsável por enquadrar o tratamento de dados pessoais em uma base jurídica é o controlador, que poderá “terceirizar” esse tratamento aos operadores de sua confiança.

²⁵¹ Ibidem.

²⁵² MIRAGEM, Bruno. **Teoria Geral do Direito Civil**. Rio de Janeiro. Forense, 2021, p. 87.

²⁵³ Conforme a LGPD, “controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. Disponível em: < **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

²⁵⁴ Operador é “a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

²⁵⁵ OLIVEIRA, Ricardo; COTS, Márcio (org.). **O legítimo interesse e a LGPD: Lei Geral de Proteção de Dados Pessoais**. Revista dos Tribunais, 2ª ed., 2021, p. 63.

O legítimo interesse do controlador²⁵⁶ ou de terceiros é trazido pelo legislador brasileiro no capítulo II da LGPD, intitulado: “do tratamento de dados pessoais”, na seção I, denominada “dos requisitos para o tratamento de dados pessoais”, a qual traz essa hipótese autorizativa no inciso IX do artigo 7^o²⁵⁷ e, depois, no artigo 10 e incisos:

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não limitam a:

- I- apoio e promoção de atividades do controlador; e
- II- proteção, em relação ao titular, do exercício de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da Lei²⁵⁸.

Uma indagação que acompanha o tema legítimo interesse é a seguinte: quais os atributos que concedem ao interesse a qualidade de legítimo? O artigo 10 da LGPD estabelece que o legítimo interesse do controlador somente poderá fundamentar o tratamento de dados para finalidades legítimas, consideradas a partir de situações concretas²⁵⁹.

O legislador tratou de usar o termo finalidades legítimas, conceito aberto, com a necessidade de justificativa legal, ou por outras fontes do direito, tais como:

²⁵⁶ Conforme a LGPD, em seu art. 5º, VI, controlador pode ser definido como: “a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 28 fev. 2023.

²⁵⁷ Art 7º: “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses[...]IX- quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 28 fev. 2023.

²⁵⁸ **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

²⁵⁹ O artigo 7º da LGPD refere o “legítimo interesse do controlador ou de terceiros” e o artigo 10 apenas menciona o “legítimo interesse do controlador”. Apesar da lacuna, deve-se entender pela aplicação do artigo 10 aos terceiros seguindo a linha da própria LGPD e do GDPR, que considera o terceiro.

analogia, jurisprudência, usos e costumes e doutrina²⁶⁰. Com efeito, o tratamento de dados pessoais pode ter diversas finalidades, como a emissão de nota fiscal e entrega de produtos. Entretanto, não significa que seja possível modificar, unilateralmente, a finalidade original para outra ou outras. Essa mudança da finalidade original depende de revalidação da base jurídica empregada. Além disso, a análise depende das situações concretas²⁶¹.

O termo *situações concretas* coloca um limitador temporal no tratamento de dados pessoais ou impõe urgência no seu enquadramento em base jurídica específica. Dessa forma, seria possível armazenar dados pessoais, sob o argumento do legítimo interesse sem que tenha sido determinada a finalidade do tratamento? Não, não é possível, pois o legítimo interesse exige uma finalidade lícita, que só se revela em uma situação concreta²⁶². Como exemplo de *situações concretas*, cita-se o comércio eletrônico quando trata dados pessoais para oferecimento de produtos relativos ao dia dos pais ou, ainda, a indústria que trata dados pessoais de ex-empregados temporários, para atuarem em um determinado pico de produção²⁶³.

A aplicação do legítimo interesse, por meio da concreção, consistirá em uma “atividade volitiva complexa” do julgador, “por meio da qual as consequências jurídicas concretas resultam da polaridade entre os valores sistemáticos e problemáticos”²⁶⁴. Com relação aos valores da LGPD, extraídos da justificativa de seu projeto, é possível afirmar a existência de dois eixos principais: dar proteção à individualidade e à privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação. É a polaridade entre esses dois valores - privacidade e livre iniciativa - e a consequente escolha, pelo aplicador, no caso concreto, de qual vai prevalecer, que marcará a aplicação do legítimo interesse²⁶⁵. E não apenas isso, a ponderação deverá ser marcada pela análise do interesse do controlador, ou de terceiro, em contraste com a verificação do impacto às liberdades e direitos fundamentais do titular, bem como com suas legítimas expectativas, conforme

²⁶⁰ OLIVEIRA, Ricardo; COTS, Márcio (org.). **O legítimo interesse e a LGPD: Lei Geral de Proteção de DADOS Pessoais**. Revista dos Tribunais, 2ª ed., 2021, p. 63.

²⁶¹ Ibidem, p.77.

²⁶² OLIVEIRA, Ricardo; COTS, Márcio (org.). **O legítimo interesse e a LGPD: Lei Geral de Proteção de DADOS Pessoais**. Revista dos Tribunais, 2ª ed., 2021, p. 63.

²⁶³ Ibidem, p.78.

²⁶⁴ ÁVILA, Humberto. **Subsunção e concreção na aplicação do direito**. In: MEDEIROS, Antônio Paulo Cachapuz de (Org.). Faculdade de Direito da PUC-RS: o ensino jurídico no limiar do novo milênio. Porto Alegre:Edipuc-RS, 1997,P.413-465, P.413.

²⁶⁵ Ibidem.

previsão do art. 10, II da LGPD. Essa regra de ponderação encontra previsão, também, no art. 7º, IX da LGPD “ao referir-se à prevalência de direitos para syndicar a aplicação do interesse legítimo²⁶⁶”.

O art 10 da LGPD ainda traz um breve rol exemplificativo que engloba o "apoio e promoção das atividades do controlador e a proteção do exercício regular dos direitos dos titulares ou a prestação de serviços que o beneficiem, respeitadas as legítimas expectativas e direitos fundamentais". É uma sequência de conceitos subjetivos que compõe a base legal do tratamento de dados justificado pelo legítimo interesse do controlador.

Com relação à legítima expectativa do titular, observa-se que, em uma relação jurídica, na qual o titular informe o número de seu CPF a um caixa de supermercado, visando a participar de uma premiação vinculada ao Governo Estadual, o qual pretende fazer um controle de notas fiscais, com objetivo arrecadatário, nota-se que a expectativa do consumidor é, no máximo, compartilhar seus dados com o Governo Estadual. Contudo, se esse estabelecimento coleta dados com uma tecnologia capaz de analisar os hábitos desse consumidor, consultar seu *scoring* creditício ou, até mesmo, criar *mailing* utilizando os dados do titular para disparo de promoções, esse tratamento viola a expectativa do cliente, que apenas imagina compartilhar o seu CPF com o Governo Estadual.

Além da necessária reflexão sobre o legítimo interesse e seus atributos, e analisando a principiologia no tratamento de dados pessoais, essas atividades, nos termos do artigo 6º da LGPD, deverão observar a boa-fé e os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas²⁶⁷. Para o recorte desta pesquisa, interessa-nos os princípios da finalidade, da necessidade e da transparência, os quais estão, expressamente, elencados nos parágrafos 1º e 2º do artigo 10 da lei, e estabelecem que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, e que o controlador deverá adotar

²⁶⁶ BUCAR, Daniel; VIOLA, Mario. **Tratamento de dados pessoais por “legítimo interesse do controlador”**: primeiras questões e apontamentos. FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro. São Paulo: Thomson, 2019, p.475.

²⁶⁷ Todos esses princípios estão contidos no art. 6º da LGPD. Disponível em:< **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm²⁷². Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deverá ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível, uma útil perspectiva geral do tratamento previsto. Se forem apresentados por via eletrônica, os ícones deverão ser de leitura automática.

De acordo com Laura Schertel Mendes, a base legal do legítimo interesse se afigura como uma espécie de cláusula geral, na qual se opera um teste de proporcionalidade entre os interesses na utilização dos dados pessoais, que são do controlador ou de terceiros, e os direitos do titular, sendo um dos pontos mais delicados da nova legislação²⁷³.

Dessa forma, a opinião do Grupo de Trabalho do Artigo 29 estabeleceu critérios para a sua aplicação, com os objetivos de (i) trazer previsibilidade e segurança jurídica na aplicação dessa base legal em todo o bloco econômico europeu; e (ii) evitar que o legítimo interesse fosse uma “porta aberta”²⁷⁴ para contornar os direitos e princípios da diretiva, em especial as outras bases legais para o tratamento de dados. Com efeito, no documento, o achado mais importante é a elaboração de um teste “multifatorial”²⁷⁵ a ser considerado pelos reguladores e pelos próprios agentes da cadeia de processamento de dados (os controladores), respectivamente, ao interpretarem e se valerem dessa base legal. Dessa forma, havia a previsão de um teste multifatorial, composto por quatro passos:(i) avaliação do legítimo interesse;(ii) impacto sobre o titular do dado;(iii) equilíbrio entre “a” e “b” e (iv) salvaguardas a cargo de quem processa dados para prevenir consequências negativas sobre o titular do dado²⁷⁶. Esse teste se denominou *legitimate interest assessment*(LIA)²⁷⁷.

²⁷² Ibidem, p.178.

²⁷³ MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016. Revista de Direito Civil Contemporâneo, v.9, p.35-48, out-dez 2016.

²⁷⁴ GRUPO DE TRABALHO DO ARTIGO 29º DA DIRETIVA 95/46/CE. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento do dados da aceção do artigo 7º da Diretiva 95/46/CE. Disponível em:<https://www.gdpd.gov.mo/pt/references_detail/article/l3mqmkcr.html>. Acesso em: 09 mar. 2023.

²⁷⁵ Ibidem, p. 11.

²⁷⁶ Ibidem, p. 12.

²⁷⁷ ICO–Information Commissioner’s Office. Disponível em:<<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>

O LIA, no contexto do GDPR, possui variações quanto a sua estruturação, de modo que há versões, como a do Information Commissioner's Office, que subdivide o teste em 3 fases (teste de legitimidade, necessidade e balanceamento), e versões como a do antigo grupo de trabalho do artigo 29, que determinam existir quatro fases, sendo a última delas a de salvaguardas²⁷⁸.

Para melhor investigar o uso secundário dos dados fundamentado no legítimo interesse, é relevante interligar a finalidade legítima e lícita como um dos juízos de valor do controlador ou terceiro.²⁷⁹

Para isso, apresenta-se a tabela abaixo:

Fase/Teste	Europa (ICO)	Europa (WP 29)	Brasil
Fase 1- Legitimidade Juízo de valor do controlador ou terceiro	Art. 6(4),b, RGPD; Recital 47 e 50,= da Diretiva 95 -Situação concreta -Finalidade lícita	Art. 6(4),b, RGPD; Recital 47 e 50 da Diretiva 95 -Situação concreta -Finalidade lícita	Art. 10, caput, da LGPD -Situação concreta -Finalidade lícita
Fase 2- Necessidade Requisitos constitutivos do legítimo interesse pelo controlador ou terceiro.	Art. 6(4),b, RGPD; Recital 47, 49, 50, da Diretiva 95 -Adequação -Minimização -Outras bases legais	Art. 6(4),b, RGPD; Recital 47 e 50, da Diretiva 95 -Avaliação do impacto -Natureza dos dados -Tipo de tratamento -Legítimas expectativas	Art. 10, §1º da LGPD -Adequação -Minimização -Outras bases legais
Fase 3 – Balanceamento Requisitos constitutivos do legítimo interesse pelo controlador ou terceiro.	Art. 6,(4),c, d, e; 6(1), f do RGPD -Legítima expectativa -Direitos e liberdades fundamentais -Salvaguardas: medidas de transparência, direito de oposição, pseudonimização	Art. 6,(4),c, d; 6(1), f do RGPD; Recital 47 da Diretiva 95 -Direitos e liberdade fundamentais -Transparência -Proporcionalidade	Art. 6º, I, 7º, IX e art. 10, II da LGPD -Legítima expectativa- Direitos e liberdades fundamentais
Fase 4 – Salvaguardas Garantias necessárias quando da aplicação da hipótese e contraditório		Salvaguardas: art. 6(4), e do RGPD, Recital 50 da Diretiva 95 -Medidas de transparência	Salvaguardas: art. 10, § 2º e 3º da LGPD -Medidas de transparência -Direito de oposição

[legitimate-interests/](#). Acesso em: 09 mar. 2023.

²⁷⁸ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p. 243.

²⁷⁹ Ibidem.

pelo titular ou entidades representativas dos seus interesses		-Direito de oposição -Pseudonimização -Portabilidade	-Pseudonimização
---	--	--	------------------

Fonte: Extrato da obra de BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 244.

O Brasil optou por um teste do legítimo interesse de quatro fases²⁸⁰, no qual o mérito dessa distribuição é arquitetar um circuito decisório que considera não apenas o juízo de valor a ser realizado pelo agente de dados, mas, também, pelo próprio titular ou representantes de seu direito. Nesse ponto da pesquisa, que objetiva avaliar o uso secundário de dados pessoais com fundamento no legítimo interesse, depreende-se a importância de ter uma fase dedicada a destacar e reforçar os princípios que dariam voz a quem deve ter seus direitos sopesados²⁸¹. Importante analisar e observar sobre como esses quatro passos refletem a estrutura do art. 10 da LGPD e uma escolha do legislador em não fazer um transplante legal do contexto europeu²⁸².

Bruno Bioni comenta sobre a sistematização do teste, levando em consideração a LGPD, o qual apresenta as etapas de:

(i) *verificação da legitimidade do interesse*: situação concreta e finalidade legítima (art. 10, caput e I, da LGPD), na qual o interesse do controlador deve ser contornado por uma finalidade legítima. Deve-se perquirir se há uma situação em concreto que lhe dê suporte, para não ser meramente especulativo²⁸³;

(ii) *necessidade*: minimização e outras bases legais (art. 10, § 1º da LGPD), cuja reflexão a ser feita é se os dados coletados são realmente necessários para se atingir a finalidade pretendida, e se seria possível atingir o mesmo resultado por meio de uma quantidade menor de dados, sendo menos intrusivo²⁸⁴ e impactando menos o indivíduo;

(iii) *balanceamento*: impacto sobre o titular dos dados e legítimas expectativas (art. 10, II da LGPD). Além das condicionantes do caput do art. 10 (finalidade legítima e concreta), o inciso II traz novos elementos, que devem ser

²⁸⁰ Ibidem.

²⁸¹ Ibidem.

²⁸² Ibidem.

²⁸³ ARTICLE 29, **Data Protection Working Party**. Opinion on 06/2014. Disponível em: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf>. Acesso em: 10 mar. 2023.

²⁸⁴ Ibidem.

observados quando a finalidade for de “ proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem”. Com efeito, a essa finalidade é acoplado um novo fator: o respeito às “legítimas expectativas do titular e os direitos e liberdades fundamentais, nos termos da LGPD”²⁸⁵. De acordo com Bruno Bioni, a legítima expectativa tem relação com o princípio da boa-fé, presente no caput do art. 6º da Lei, o qual é um norte para todos os outros princípios previstos neste dispositivo²⁸⁶. Dessa forma, quando o incluiu, o legislador brasileiro amarrou os conceitos jurídico-indeterminados da legítima expectativa e do “legítimo interesse” ao princípio da boa-fé, tratado no item 2.5 deste trabalho.

Assim, a inclusão da boa-fé no caput do art. 6º é indicativa da centralidade do princípio, inclusive em relação aos demais princípios, que são desdobramento do caput, expresso em incisos²⁸⁷. Como princípio, a boa-fé está inserida na seção de disposições preliminares da lei, que também conta com fundamentos (art. 2º), escopo de aplicação da Lei (arts. 3º e 4º) e definições (art. 5º)²⁸⁸.

O GT 29, ao analisar, especificamente, a hipótese do legítimo interesse, afirmou que essa modalidade de tratamento de dados estipula que o responsável faça um balanceamento (balancing test) entre seus legítimos interesses no tratamento dos dados e os interesses e direitos fundamentais do titular dos dados. O resultado desse balanceamento determina se os dados podem ou não ser lícitamente tratados sem o consentimento do titular²⁸⁹. Além disso, assegura aos responsáveis a flexibilidade necessária para efetuar o tratamento de dados, nos casos em que não haveria impactos indevidos sobre o indivíduo em decorrência desse tratamento, estabelecendo o necessário equilíbrio entre proteção à privacidade e à intimidade e o desenvolvimento econômico e inovação, criando uma esperada sustentabilidade dos sistemas²⁹⁰.

²⁸⁵ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 245.

²⁸⁶ A boa-fé seria um “princípio dos princípios”, inserido no art. 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:[...]. In: BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 245.

²⁸⁷ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 246.

²⁸⁸ Ibidem.

²⁸⁹ EUROPEAN UNION. **Guidelines on Automated Individual decision-making and Profiling for the purpose of Regulation 2016/679**-Adopted on 3 October 2017-As last Revised and Adopted on February 2018. Disponível em:< https://www.ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826>. Acesso em: 25 abr. 2023.

²⁹⁰ OLIVEIRA, Ricardo; COTS, Márcio (org.). **O legítimo interesse e a LGPD: Lei Geral de Proteção de DADOS Pessoais**. Revista dos Tribunais, 2ª ed., 2021, p. 63.

Em relação ao balanceamento, além do interesse privado do responsável, existem interesses coletivos que reforçam a necessidade do tratamento de dados, além de se certificar de que nenhuma das outras hipóteses previstas poderia melhor se encaixar ao caso concreto²⁹¹.

Trata-se da principal fase do teste de proporcionalidade, na qual são sopesados os interesses do controlador e de terceiros diante dos do titular dos dados²⁹². Necessário se faz examinar se o novo uso atribuído ao dado está dentro das legítimas expectativas do seu titular, o que é determinado pela compatibilidade²⁹³ entre o uso adicional e aquele que originou a coleta dos dados pessoais²⁹⁴, implicando uma análise contextual para verificar se esse uso secundário seria esperado pelo titular dos dados²⁹⁵. Por essa razão, a escolha do termo legítimo não só qualifica a base legal do interesse legítimo, como também o princípio da finalidade. Além disso, deve-se analisar de que forma os titulares de dados serão impactados, mais especificamente repercussões negativas em termos de discriminação e sobre a sua autonomia (liberdades e direitos fundamentais)²⁹⁶. Caso o tratamento de dados também os beneficie, a balança tende a ser equilibrada;

(iv) salvaguardas: art. 10§§ 2º e 3º da LGPD. Nesse item, Bioni reflete a ideia do dever de transparência na atividade de tratamento de dados, embora o legítimo interesse prescindia do consentimento do titular. Como salvaguarda, encontra-se a possibilidade do titular se opor ao tratamento, pela ferramenta do

²⁹¹ Ibidem, p.132.

²⁹² Ibidem, p.247.

²⁹³ Compatibilidade está inserida no princípio da adequação e está relacionada, na LGPD, com as finalidades informadas ao titular, de acordo com o contexto do tratamento. In: BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 19 jan. 2023.

²⁹⁴ KUNER, Christopher. **Regulation of Transborder Data Flows under Data Protection and Privacy Law**. OECD Digital economic papers, Paris, n. 187, p. 1-40. Disponível em: <<http://dx.doi.org/10.1787/5kg0s2fk315f-en>>. Acesso em: 13 mar. 2023.

²⁹⁵ De acordo com o art. 29 do Working Party, opinião 03/2016:"The second factor focuses on the specific context in which the data were collected an the reasonable expectations of the data subjects as o their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situation would expect his or her data to be used for based on the context of the collection". In: Article 29 Data Protection Working Party. **Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)**. Disponível em:<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf> Acesso em: 13 mar. 2023.

²⁹⁶ Ibidem.

*opt-out*²⁹⁷, podendo decidir por estar fora do que considera ser incompatível com as suas legítimas expectativas e podendo controlar seus dados a posteriori²⁹⁸.

Em síntese, em relação ao teste da base legal do legítimo interesse, pode-se afirmar que o primeiro passo é a avaliação do interesse da pessoa responsável pelo tratamento; o segundo, é a verificação do impacto nas pessoas envolvidas; o terceiro, o exame do equilíbrio entre os interesses, e o último é a análise de existência de garantias complementares para evitar impactos indevidos.²⁹⁹

Além dessas técnicas, o controlador deve adotar ações que mitiguem os riscos do titular dos dados (por exemplo, anonimização), sendo esse o sentido da previsão da eventual necessidade de elaboração de *relatório de impacto à proteção de dados pessoais (RIPD)*³⁰⁰, registro que tem previsão no art. 5º, XVII da LGPD, com o seguinte texto:

“documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos”.

Por sua vez, o art. 38 da LGPD esclarece qual é o âmbito de aplicação do relatório, bem como, de modo extremamente sucinto, os elementos básicos que devem compô-lo³⁰¹, além de não ser obrigatório. Entretanto, em relação ao GDPR, o nº 3 do art. 35 dispõe sobre a obrigatoriedade da avaliação de impacto sobre a proteção de dados, dentro daquelas previsões legais, manifestamente entre as

²⁹⁷ Nas abordagens promocionais, baseadas no legítimo interesse, as respectivas mensagens devem conferir ao cliente a opção de *opt-out*, isto é, de solicitar a remoção dos seus dados da lista de e-mails comerciais/spam da empresa remetente. In: MARTINS, Ricardo Maffei; GUARIENTO, Daniel Bittencourt. **LGPD impõe às empresas revisão de suas estratégias de marketing**. Disponível em: <<https://www.migalhas.com.br/coluna/impressoes-digitais/353608/lgpd-impoe-as-empresas-a-revisao-de-suas-estrategias-de-marketing>>. Acesso em: 13 mar. 2023.

²⁹⁸ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 248.

²⁹⁹ DILL, Amanda Lemos. **A delimitação dogmática do legítimo interesse para tratamento de dados pessoais**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). *Lei geral de proteção de dados: aspectos relevantes*. Indaiatuba, SP: Editora Foco, 2021. p. 95- 118.

³⁰⁰ *Ibidem*.

³⁰¹ O art 38 da LGPD prevê que “A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comerciais industrial. In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 13 mar. 2023.

alíneas a), b) e c). Como exemplo, cita-se a alínea a), que trata da “avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição e perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem, significativamente, de forma similar”.

Com efeito, o ordenamento jurídico brasileiro trata do RIPD em três momentos: no art. 5º XVII, o qual apresenta a definição de relatório de impacto de proteção de dados; também no art. 38, que trata da faculdade da ANPD em determinar ao controlador a elaboração do relatório de impacto e, por último, no art 55-J, XIII, que estabelece a competência da ANPD em editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD. Pela observação e análise da pesquisa, identifica-se uma lacuna na LGPD em estabelecer uma obrigatoriedade do RIPD para situações de maior risco no seu tratamento. Na última parte, tratar-se-á do relatório de impacto da proteção de dados, o qual é muito relevante para mitigar riscos e garantir maior segurança jurídica. No tópico seguinte, serão apresentadas questões controvertidas na aplicação do legítimo interesse.

3.5 Questões controvertidas na aplicação do legítimo interesse

Ainda há discussão, no âmbito do GDPR, se os agentes de tratamento de dados deveriam documentar o teste de ponderação do legítimo interesse sempre que as suas atividades de tratamento de dados estivessem apoiadas nesta base legal. Isso porque a própria estrutura do LIA- legitimate interest assessment- não está esquematizada no texto duro da lei³⁰² mas, tão somente, nas diretrizes para a sua interpretação. Além disso, o regulamento europeu apenas reforçou o dever de informação junto aos titulares dos dados, nos artigos 13º e 14º, mas não o dever de

³⁰² O GDPR contém 99 artigos e 173 considerandos. Esses são definidos como as razões para a adoção dos artigos do GDPR propriamente dito: “considering the following reasons the articles of the GDPR have been adopted. These are the latest and final recitals of April 27th 2016”. Assim, os considerandos apresentam a racionalidade do regulamento, mas não se confundem com ele. Disponível em: <EUROPEAN UNION. Regulation(EU) 2016/679. **General Data Protection Regulation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 out. 2022.

documentação acerca das atividades de tratamento de dados, lastreadas no legítimo interesse³⁰³.

Alguns doutrinadores³⁰⁴ já têm se posicionado acerca da obrigatoriedade do LIA, pois, a partir do princípio da *accountability*³⁰⁵, alega-se que os controladores de dados deveriam demonstrar a sua responsabilidade em balancear seus interesses frente aos dos titulares por meio dessa documentação, em específico.

Contudo, no âmbito da LGPD esse desenho é distinto, porque as fases do LIA estão talhadas no próprio texto duro da lei e distribuídas ao longo dos incisos e parágrafos do art. 10. Dessa forma, não se trata de uma diretriz interpretativa, mas do próprio conteúdo normativo em torno da licitude da base legal³⁰⁶. Além disso, não apenas o dever de informação é reforçado como corolário do princípio da transparência³⁰⁷, mas, principalmente, o dever de registro das atividades de tratamento de dados. Para Bioni³⁰⁸, a LGPD aponta para uma documentação especial que parece ser justamente o LIA.

Dessa forma, o desenho normativo descrito da LGPD, somado ao princípio da *accountability* conduz, necessariamente, à obrigação de execução e de documentação do LIA, uma vez que a interpretação sistemática dos arts. 6º, X, 10 e 37 da lei brasileira condiciona o uso responsável da base legal do legítimo interesse ao referido teste, sob pena dos agentes de tratamento não demonstrarem a adoção de medidas eficazes para tanto³⁰⁹.

Outra questão controvertida na aplicação do legítimo interesse está na previsão, pela LGPD, do direito de oposição frente às outras nove bases legais como uma maneira do titular obstruir o tratamento de seus dados à semelhança da

³⁰³ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p. 248.

³⁰⁴ FERRETI, Frederico. Data Protection and the Legitimate Interest of Data Controllers: Much Ado or About Nothing or the Winter of Rights? *Common Market Law Review*, n. 51(3):843-868. Acesso em: 25 abr. 2023. KAMARA, Irene; DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: a Pragmatic Approach. *Brussels Privacy Hub Working Paper*, vol.4, n.12, 2018. Acesso em: 20 abr. 2023.

³⁰⁵ *Accountability* aqui entendida como prestação de contas.

³⁰⁶ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p. 248.

³⁰⁷ Por meio do art. 6º, VI, da LGPD, temos que “art. 6º: As atividades de tratamento de dados pessoais deverão observar a boa fé e os seguintes princípios:(...) VI- transparência: garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

³⁰⁸ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p. 248.

³⁰⁹ *Ibidem*, p.25.

hipótese de revogação do consentimento³¹⁰. Entretanto, diferentemente da revogação do consentimento, que se apresenta como um direito potestativo e sem limitações estabelecidas, a LGPD condicionou o exercício do direito de oposição à hipótese de violação a uma das suas normas. Com efeito, levando em consideração uma primeira interpretação, o exercício desses dois direitos de objeção teria alcances distintos, visto que o legítimo interesse não dependeria, única e exclusivamente, da vontade do titular em exercê-lo. Contudo, não pode haver assimetria³¹¹ entre duas bases legais. Deve-se colocar em igualdade as hipóteses de legitimação para o tratamento de dados.

O legítimo interesse deve levar em consideração as legítimas expectativas do titular de dados. Tal análise é feita, objetivamente, de acordo com os padrões sociais e pelo próprio agente de tratamento de dados o qual se coloca na posição do titular para avaliar se a sua conduta não frustraria a confiança nele depositada. Contudo, a última fase do teste tem como um dos seus pilares a adoção de medidas de transparência, de modo que o cidadão possa ter voz sobre o que considera ser um uso inadequado das suas informações pessoais³¹².

A forma pela qual foi estruturado o legítimo interesse, na LGPD, também confere uma posição jurídica ao titular de objeção ao tratamento de seus dados, lastreado em tal base legal³¹³. A expressão legítima expectativa, nesse sentido, tem uma conotação subjetiva, vinculada ao que o próprio titular deseja e espera que seja feito com seus dados. Se não fosse assim, a última fase do LIA, que se refere ao dever de transparência acerca do tratamento de dados, não aplicaria um dos fundamentos da lei, que é a autodeterminação informativa. Ou seja, quando é dada a transparência acerca do tratamento de dados com base no legítimo interesse e o titular a ele se opõe, caso o agente de tratamento de dados não o acate, estará violando uma das normas da LGPD. Com efeito, trata-se de uma interpretação sistemática entre os arts. 10, II e §2º, combinado com o art. 18, §2º³¹⁴. Entretanto, é

³¹⁰ De acordo com o art. 8º, §5º da LGPD: "o consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei". In: **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 13 mar. 2023.

³¹¹ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 258.

³¹² Ibidem, p.259.

³¹³ Ibidem, p.259.

³¹⁴ Ibidem, p.259.

necessário observar e analisar que esse direito não é absoluto. Se, por um lado, a posição jurídica de processar dados sem o consentimento prévio não pode ser abusada a ponto de lhe retirar, por completo, a sua capacidade de autodeterminação informativa, por outro lado, tal direito de objeção também deve ser contornado pela figura de abuso de direito³¹⁵. Essa cláusula geral contida no Código Civil brasileiro limita quem pode cometer ato ilícito ao se valer dessa prerrogativa em circular uma informação pessoal, caso “exceda manifestamente os limites impostos pelo seu fim econômico e social, pela boa-fé e pelos bons costumes”³¹⁶. Com efeito, para além de pura e simplesmente apontar que o instituto do abuso de direito pode ser uma ferramenta de delimitação de juridicidade da privacidade contextual no cenário brasileiro, é importante verificar em que a lei geral de proteção de dados agrega, teleologicamente, essa análise³¹⁷. O novo marco regulatório estabelece uma dialética normativa de conciliação entre a proteção de direitos e liberdades fundamentais do titular do dado e o livre desenvolvimento econômico e tecnológico. Entretanto, ao fazê-lo, eleva, expressamente, a proteção de dados como um novo direito de personalidade e que tem como fundamento a autodeterminação informativa³¹⁸. Sendo assim, o fim econômico e social em torno da circulação de dados pessoais deve, necessariamente, ser recortado pelo grau de empoderamento do seu titular em visualizá-lo e controlá-lo. Quem se vale da posição jurídica de tratar dados pessoais, sem o consentimento prévio do seu respectivo titular, não pode dela abusar a ponto de gerar ou agravar a assimetria de informação e de poder, frente a quem tem o livre desenvolvimento da sua personalidade condicionado pelo uso de suas informações pessoais. Se, por acaso, isso ocorrer, acontece a ilegitimidade, que é o problema de qualificação acerca do exercício de uma prerrogativa, a qual o instituto do abuso de direito endereça³¹⁹.

³¹⁵ Ibidem, p.259.

³¹⁶ Código Civil Brasileiro. Disponível

em<https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm Acesso em: 2 abr. 2023.

³¹⁷ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed.,Rio de Janeiro: Forense, 2021, p. 258.

³¹⁸ Conforme o art. 2º, II, da LGPD:”A disciplina da proteção de dados tem como fundamento (...) II-a autodeterminação informativa. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

³¹⁹ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed.,Rio de Janeiro: Forense, 2021, p. 237-238.

Em um exemplo prático, na hipótese em que o tratamento de dados pessoais sirva ao propósito de combate a incidentes de segurança na rede, esse é um cenário no qual há uma finalidade econômico-social que sobrepõe o direito individual do próprio titular. Dessa forma, se tal atividade de tratamento de dados está em conformidade com os princípios e demais normas de proteção de dados, em especial com aqueles que são reforçados nas fases de aplicação do legítimo interesse (necessidade, transparência e prevenção), o direito de oposição tende a ser relativizado frente a um interesse coletivo³²⁰. Essa é uma discussão normativa que coteja a autodeterminação informativa³²¹ frente aos demais fundamentos da LGPD³²².

Diferentemente do GDPR, a LGPD não procedimentalizou, minimamente, o direito de oposição, especialmente frente a base legal do legítimo interesse. Contudo, a aplicação e interpretação do direito de oposição não deve ter como resultado um regime jurídico assimétrico³²³, especialmente frente ao direito correspondente de revogação do consentimento³²⁴.

Outro ponto controvertido na aplicação do legítimo interesse é o da publicidade direcionada. É nesse cenário que o LIA se apresenta e é capaz de fornecer pistas sobre os principais pontos de atenção acerca da mitigação dos riscos de eventual não conformidade com a base de dados do legítimo interesse³²⁵. Seja quem já mantém uma relação previamente estabelecida com o titular dos dados, seja no caso de terceiros que compõem uma rede de publicidade

³²⁰ Ibidem, p.259.

³²¹ Ibidem, p.259.

³²² O art. 2º da LGPD trata dos fundamentos da proteção e dados pessoais, que são eles: "I- o respeito à privacidade; II- a autodeterminação informativa; III- a liberdade de expressão, de informação, de comunicação e de opinião; IV- a inviolabilidade da intimidade, da honra e da imagem; V- o desenvolvimento econômico e tecnológico; VI- a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII_ os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais". **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

³²³ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed.,Rio de Janeiro: Forense, 2021, p. 237-238.

³²⁴ Conforme art. 8º, §5º da LGPD: "O consentimento poder ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei". **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados(LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

³²⁵ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed.,Rio de Janeiro: Forense, 2021, p. 260.

comportamental³²⁶, ambos têm o legítimo interesse em processar tais dados para viabilizar as suas atividades comerciais. Para esta pesquisa de uso secundário de dados com fundamento no legítimo interesse, listam-se quatro variáveis com o intuito de compor uma matriz de risco. A primeira variável do contexto da abordagem publicitária leva em consideração: (i) a relação estabelecida entre o titular do dado e o agente de tratamento de dados. A ideia de legítima expectativa é muito mais aderente quando já há uma relação preestabelecida entre o titular de dados e o agente de tratamento de dados. O tipo de abordagem e reunião de informações pode trazer mais ou menos riscos no uso da base legal do legítimo interesse. Com efeito, existem abordagens publicitárias com *marketing direto*³²⁷ e *indireto* nessa variável. Em transações que envolvam o marketing direto, o titular do dado já mantém essa relação com o controlador, como no caso dele já ter adquirido seus produtos e serviços. A partir desse histórico de compras, é possível lhe direcionar anúncios publicitários que sejam condizentes com o seu padrão de consumo, como a oferta de livros de um determinado autor, por meio de uma loja procurada pelo consumidor. No marketing direto são utilizados o first-party tracking, o qual nada mais é do que o rastreamento realizado pelo próprio aplicativo³²⁸, cujo perfil pode ser construído não só através de compras, mas também do que despertou interesse do consumidor, em sentido amplo. Nesses casos, há um contexto que favorece a aplicação do legítimo interesse, na medida em que essa relação preestabelecida é um indicativo de que tal uso de dados é compatível com o que originou a sua coleta. Já o marketing indireto é realizado por terceiros e pelo third-party tracking³²⁹. No marketing indireto há uma rede de publicidade comportamental composta por uma série de atores que trocam dados entre si e exibem esses anúncios em diferentes plataformas, ou seja, o mesmo anúncio

³²⁶ ARTICLE 29, **Data Protection Working Party. Opinion 2/2010.**

Disponível: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf>. Acesso em: 10 abr. 2023.

³²⁷ O Considerando 47 do GDPR prevê o marketing direto como uma das possíveis aplicações do legítimo interesse, no texto: "O tratamento de dados para fins de marketing direto pode ser considerado efetuado para um legítimo interesse". EUROPEAN UNION. Regulation(EU) 2016/679.

General Data Protection Regulation. Disponível em:

<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 out. 2022.

³²⁸ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento.** 3. ed., Rio de Janeiro: Forense, 2021, p. 261.

³²⁹ O third-party tracking é o rastreamento realizado por terceiros, que não a própria aplicação acessada pelo usuário. BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento.** 3. ed., Rio de Janeiro: Forense, 2021, p. 261.

percorre diferentes websites visitados ou aplicativos acessados. Com efeito, nesses casos, há não somente o ingresso de terceiros no fluxo informacional, mas também o acúmulo de dados de diferentes esferas da vida do titular do dado. Dessa forma, o GT 29, em seu parecer 2, já se posicionava no sentido de que o legítimo interesse não seria aplicável nesses casos, concluindo que não estaria dentro das legítimas expectativas do titular dos dados e seria necessário recorrer à base legal do consentimento; outra variável é (ii) o nível de intrusão (minimização), o qual analisa e observa que a lógica da publicidade comportamental³³⁰ é a reunião de informações, o máximo possível, sobre o consumidor em potencial, mediante a criação do retrato mais completo de sua personalidade. Essa publicidade tem prevalecido em razão de ser mais efetiva do que a publicidade direcionada. A esse respeito, é relevante considerar que a proibição dos provedores de conexão em armazenar *logs* de aplicação já estava previsto no Marco Civil da Internet³³¹, visto que a racionalidade do legislador foi impedir um mapeamento completo da vida digital das pessoas, o que seria tecnicamente possível por quem é a porta de entrada e saída da internet; outra variável é relativa a (iii) inferências e usos: que também são o fiel da balança. Em razão da tecnologia, tornou-se possível mapear as emoções do consumidor³³² e, até mesmo, precificar o consumidor de acordo com o seu perfil. Nesses casos, a balança tende a estar em desequilíbrio por ser algo que foge das legítimas expectativas do titular dos dados, como no caso de uma precificação dinâmica, e impacta, negativamente, a sua própria autodeterminação de forma ampla. Nessa situação, por exemplo, o seu poder de tomada de decisão, para a aquisição de um

³³⁰ WORKING PARTY. Article 29 Data Protection Working Party. **Opinion 2/2010 on behavioural advertisement**. Brussels, 22 jun. 2010. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf>. Acesso em: 30 jan. 2023.

³³¹ Em seu art. 14, caput, o Marco Civil da Internet proíbe que os provedores de conexão armazenem *logs* de acesso à aplicação, além dos logs de conexão a que estão obrigados, legalmente. Por parte do legislador, houve a preocupação de que a ausência de tal proibição implicaria sério prejuízo à privacidade dos usuários, isso porque os provedores de conexão poderiam rastrear toda a navegação do usuário, na medida em que eles são a porta de entrada e de saída da internet para os usuários. Por estarem situados nas camadas física e lógica da rede, eles poderiam mapear todo o conteúdo acessado por seus consumidores, o que seria extremamente invasivo. BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 217.

³³² Há uma vigilância imperativa das pessoas, em especial do consumidor em potencial, o qual varia desde os seus hábitos de navegação e comportamento na internet até as suas próprias emoções, tornando-o, totalmente transparente, como um *consumidor de vidro*. MENDES, Laura Schertel. **Transparência e Privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação. Faculdade de Direito da Universidade de Brasília, 2008, p.81-85.

bem de consumo, em termo volitivos e econômicos, é impactado negativamente³³³. Será útil estabelecer, nesse sentido um diálogo entre a LGPD e o Código de Defesa do Consumidor, com o intuito de analisar e verificar se tal prática também não seria abusiva³³⁴. Por fim, a última variável são as (iv) salvaguardas. A principal delas é a adoção de mecanismos de transparência que permitam ao titular dos dados se opor a tal tipo de tratamento, na figura do *opt-out*³³⁵. Com efeito, quanto mais visível for tal prática e mais fácil for o exercício do opt-out, maiores serão as chances de a aplicação da base legal do legítimo interesse ser válida. Além disso, a aplicação de PETs³³⁶ (privacy-enhancing technologies) é um fator-chave, principalmente as que facilitam que o titular do dado barre ou personalize o seu monitoramento diante da multidão de atores que compõem uma rede de publicidade comportamental. Deve-se considerar, também, que havendo uma série de atores que cooperam para a entrega da publicidade comportamental, é importante verificar qual é o seu nível de cooperação para a proteção de dados pessoais. Com efeito, além da necessidade de estabelecer contratos que definam a responsabilidade e os deveres de um dos agentes da cadeia de tratamento de dados pessoais, esse deve ser complementado

³³³ BIONI, Ricardo Bruno. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed., Rio de Janeiro: Forense, 2021, p. 263.

³³⁴ Artigo 39 do CDC dispõe do seguinte texto: "Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:(...) III- enviar ou entregar ao consumidor, sem solicitação prévia, qualquer produto, ou fornecer qualquer serviço; IV- prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços(...).Lei 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%Aancias.&text=Art.48%20de%20suas%20Disposi%C3%A7%C3%B5es%20Transit%C3%B3rias> Acesso em: 10 mai. 2023.

³³⁵ Opt-out se refere à possibilidade dada pela empresa de que os internautas não estejam mais presentes nas listas do chamado e-mail marketing. Sendo assim, essa ação serve tanto para quem foi cadastrado de maneira incorreta como então para aqueles que não possuem mais interesse em receber os e-mails de determinada instituição. Dessa forma, o público não autoriza mais que sejam enviados novos conteúdos e materiais desde o momento em que o cliente clica no link do Opt-out que, normalmente, fica logo abaixo do corpo do e-mail. Disponível em<<https://www.certifiquei.com.br/opt-out/>. Acesso em 12 mai. 2023.

³³⁶ As tecnologias de aprimoramento da privacidade (PET) são tecnologias que incorporam princípios fundamentais de proteção de dados, minimizando o uso de dados pessoais, maximizando a segurança dos dados e capacitando os indivíduos. Os PETs permitem que os usuários protejam a privacidade de suas informações de identificação pessoal, que geralmente são fornecidas e manipuladas por serviços ou aplicativos. Os PETs usam técnicas para minimizar a posse de dados pessoais por um sistema de informação sem perder a funcionalidade. De um modo geral, os PETs podem ser categorizados como tecnologias de privacidade rígidas e flexíveis. Disponível em: <https://en.wikipedia.org/wiki/Privacy-enhancing_technologies. Acesso em: 12 mai. 2023.

pela elaboração de relatórios de impacto à proteção de dados pessoais, códigos de boas condutas e outras iniciativas que reforcem esse comprometimento.³³⁷

4. PROPOSTA LEGISLATIVA DA LEGE LATA A LEGE FERENDA

Entre os instrumentos que a LGPD oferece para gerir riscos à privacidade com o propósito de prevenir danos e demonstrar conformidade, destaca-se o relatório de impacto à proteção de dados pessoais (RIPD) ou, como é denominado no GDPR, *data protection impact assessment*. O regulamento europeu já previu essa avaliação de impacto, no seu considerando 84, o qual trata da possibilidade do tratamento estar suscetível a um elevado risco para os direitos e liberdades das pessoas singulares, encarregando o responsável da realização de uma avaliação de impacto à proteção de dados, para a determinação da origem, natureza, particularidade e gravidade desse risco. Por meio desse considerando, sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco e o responsável pelo tratamento não puder atenuá-lo através de medidas adequadas, será necessário consultar a autoridade de controle *antes* de se proceder ao tratamento de dados pessoais.

Outro instrumento de gestão de risco à privacidade é a avaliação de legítimo interesse (*legitimate interest assessment-LIA*), a qual, embora não esteja expressamente prevista no GDPR, e na LGPD está, constitui boa prática para o controlador avaliar em que medida a utilização da base legal legítimo interesse impacta os direitos, as liberdades e as expectativas razoáveis dos titulares em relação ao tratamento de seus dados pessoais, de modo a auxiliá-lo na escolha ou não desse fundamento, para determinada operação de tratamento³³⁸. Com efeito, o *ICO – Information Commissioner’s Office* (órgão público não departamental do

³³⁷ A autoridade de proteção de dados do Reino Unido (Information Commissioner’s Office-ICO) posiciona-se nesse exato sentido ao observar a insuficiência de salvaguardas baseada apenas em contratos e cláusulas contratuais. Essa abordagem deveria ser acompanhada por outras medidas como relatórios de impacto, códigos de boas condutas e outros tipos de ferramentas para demonstrar *compliance* à legislação e promover accountability. INFORMATION COMMISSIONER’S OFFICE (ICO). Update report into adtech and real time bidding, 2019. Disponível em <<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>>. Acesso em: 12 mai. 2023.

³³⁸ BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. **Relatório de Impacto à Proteção de Dados e Avaliação de Legítimo Interesse**. In: BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. **Data Protection Officer (Encarregado): Teoria e Prática de Acordo com a LGPD e o GDPR**. São Paulo (SP): Editora Revista dos Tribunais, 2022. Disponível em <<https://thomsonreuters.jusbrasil.com.br/doutrina/1481212764/data-protection-officer-encarregado-teoria-e-pratica-de-acordo-com-a-lgpd-e-gdpr>>. Acesso em: 14 abr. 2023.

Reino Unido), dispõe que o legítimo interesse é a base legal mais flexível para processamento de dados. De acordo com o ICO, se houver a opção pelo legítimo interesse, o controlador estará assumindo uma responsabilidade extra por considerar e proteger os direitos e interesses das pessoas singulares³³⁹.

O ICO elaborou um modelo de avaliação dos legítimos interesses, o qual se divide em três partes:(i) teste da finalidade,(ii) teste da necessidade e (iii) teste do equilíbrio³⁴⁰.

O teste da finalidade é composto por uma gama de perguntas, as quais podemos citar, como exemplo:

- a) por que é necessário tratar esses dados?
- b) que benefício se espera alcançar com esse tratamento?
- c) o quanto importante são os benefícios identificados no tratamento?
- d) estão sendo cumpridas outras leis relevantes?

Com relação ao teste da necessidade³⁴¹, a avaliação considera se esse tratamento é necessário para a finalidade identificada. Para este teste, algumas sugestões de perguntas:

- a) esse tratamento realmente ajudará você a alcançar a sua finalidade?
- b) pode-se alcançar a mesma finalidade sem esse tratamento?
- c) pode-se alcançar a mesma finalidade tratando menos dados ou tratando-os de uma maneira menos intrusiva?
- d) é possível atingir a mesma finalidade sem o tratamento?

E por fim, para completar o modelo, aplica-se o teste de equilíbrio³⁴², no qual é necessário considerar o impacto nos interesses, direitos e liberdades dos indivíduos e avaliar se isso justifica o legítimo interesse. Para este teste é essencial que sejam feitas algumas perguntas, tais como:

- a) são dados de categoria especial ou dados criminais?
- b) são dados que as pessoas consideram, particularmente, privados?
- c) estão sendo tratados dados de crianças ou de pessoas vulneráveis?
- d) são dados pessoais ou profissionais?

³³⁹ ICO-Information Commissioner's Office. Disponível em:<<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>>. Acesso em: 16 abr. 2023.

³⁴⁰ Ibidem, p.1

³⁴¹ Ibidem, p.1

³⁴² Ibidem, p.2

Quanto à legislação brasileira, o relatório de impacto à proteção de dados tem sua ocorrência, na LGPD, em seu art. 5º, XVII³⁴³, art. 10, §3º³⁴⁴ (quando o tratamento for baseado no legítimo interesse do controlador) e art. 38, caput, sendo que este último estabelece “que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referentes as suas operações de tratamento de dados, em termos de regulamento, observados os segredos comercial e industrial”. Neste ponto, a lei brasileira faculta a autoridade nacional que determine ao controlador a elaboração do relatório de impacto. Em contrapartida, o GDPR, em seu art. 35º, n.3, alíneas “a”, “b” e “c” prevê critérios e situações, nas quais o relatório de impacto é obrigatório:

3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n. 1³⁴⁵ é obrigatória, nomeadamente, em caso de:

a) avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem, significativamente, de forma similar;

b) operações de tratamento em grande escala de categorias especiais de dados a que se refere o art. 9º, n.1, ou de dados

³⁴³ Conforme a LGPD, o relatório de impacto à proteção de dados pessoais é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

³⁴⁴ A LGPD prevê, em seu art. 10, §3º que “a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

³⁴⁵ O art. 35º, n1 do GDPR prevê que “quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Um conjunto de operações de tratamento que apresentar riscos elevados semelhantes pode ser analisado numa única avaliação”. EUROPEAN UNION. Regulation (EU) 2016/679. **General Data Protection Regulation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 mar. 2023.

personais relacionados com condenações penais e infrações a que se refere o art. 10º ou;

c) controlo sistemático de zonas acessíveis ao público em grande escala.

Quando se analisa o relatório de impacto à proteção de dados, e sua parcial importação do regulamento europeu, a lei brasileira revela-se problemática e desafiadora por diversos fatores que serão abordados. O primeiro deles está no seu glossário, no qual a LGPD estabelece que o relatório é uma “documentação do controlador que contém a descrição nos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”³⁴⁶. A lei brasileira ainda apresenta o conteúdo do relatório, em outro dispositivo³⁴⁷: “(...) o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados”.

Na definição dada pela LGPD, por meio do conteúdo do relatório, e analisando apenas a letra fria da lei, podemos perceber que ele se distancia bastante da definição dada pelo GDPR, com relação aos conceitos-chave de processo de “alto risco”, da avaliação de necessidade do tratamento, entre outros, inicialmente ignorados pela lei brasileira. A única menção ao “alto risco”, o que é elemento central do RIPD, encontra-se no art. 55-J, inciso XIII da lei:

“Art. 55-J. Compete à ANPD: XIII -editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei”.

³⁴⁶ Art. 5º, XVII da LGPD. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

³⁴⁷ Ibidem, art. 38, parágrafo único.

Traçando um paralelo com o GDPR, a lei brasileira apresenta algumas características de identidade própria: a abordagem excessivamente formalista, que é possível extrair do texto da LGPD; uma possível amplitude ou ausência das suas hipóteses de elaboração, sem uma proporcionalidade aparente, despregada das reais funções da ferramenta, e a ausência de critérios claros para quando elaborá-lo, o que não passou incólume a críticas. Matheus Sturari³⁴⁸, a título de exemplo, explorou tais pontos problemáticos extraídos da lei. Com efeito, ele observa que, por dedução à definição do art. 5º, XVII, o RIPD será exigido para atividades de tratamento que gerem riscos *às liberdades civis e direitos fundamentais*. Entretanto, o autor levanta uma série de questionamentos, entre eles: (i) se toda a hipótese de tratamento fundamentado em legítimo interesse deve ser acompanhada de um RIPD; (ii) quais são os tratamentos considerados como geradores de risco a ponto de demandarem um RIPD; (iii) a despeito de uma lista, quais critérios devem ser considerados para analisar a existência de risco e considerar a necessidade de um RIPD e, por último, todo e qualquer risco deve ensejar um RIPD ou apenas um “alto risco”, como no inciso XII, do art. 55-J da LGPD?

Para Sturari³⁴⁹, tais dúvidas parecem surgir em razão de uma preocupação da LGPD sob aspecto formal relacionado ao RIPD, isto é, estabelecer o que deveria ser considerado em seu instrumento (relatório); em contrapartida, carece de elucidações referentes ao seu aspecto processual, ou seja, não como um mero documento, mas como um processo de análise que deve ser desencadeado de acordo com critérios claros e, preferencialmente, dotados de certo aspecto objetivo. A LGPD parece focar no *resultado* do relatório, mas pareceu silenciar acerca de todo o processo necessário para se chegar a tal relatório, inclusive o principal: quando tal processo deve ser desencadeado. Acontece que a existência de tais dúvidas, e de um cenário de incertezas envolvendo o tema, tem gerado o seguinte efeito negativo: a possível banalização do RIPD e consequente excessiva oneração dos agentes de tratamento³⁵⁰.

³⁴⁸ STURARI, Matheus. **O DPIA na LGPD: interpretação nacional ou banalização do instrumento?** Perfil do LinkedIn. Publicado em 29 de outubro de 2020. Disponível em: <https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-ou-banaliza%C3%A7%C3%A3o-do-matheus/> > Acesso em 13 mai. 2023.

³⁴⁹ Ibidem.

³⁵⁰ Ibidem.

Em um outro trabalho acadêmico, acerca do tema, de Filipe Fonteles Cabral³⁵¹, o pesquisador levanta uma crítica sobre o risco de que o RIPD se torne um instrumento de controle em casos isolados ou, ainda mais grave, que seja um documento elaborado para fins formais, mas que não consiga guiar uma atividade real de gerenciamento de riscos, o que pode comprometer a eficácia do sistema de proteção de dados pessoais no Brasil.

Na evolução das ferramentas, houve um constante esforço para otimizar a atuação das autoridades de proteção de dados nos casos realmente necessários e para não onerar, excessivamente, o controlador de dados com o processo complexo de análise que é uma avaliação de impacto³⁵².

Ocorre que, a mera possibilidade de o relatório ser requisitado diretamente por uma autoridade, para além do critério de alto risco, vai na contramão do controle prévio do GDPR, e até mesmo da checagem prévia da Diretiva. A presença do encarregado de dados e as suas garantias de independência existem justamente para que esse realize a comunicação com a ANPD, e não o inverso. Além disso, um eventual cenário de frequente requisição direta de elaboração do relatório pela ANPD demonstra dois sintomas: o primeiro, os critérios para a sua obrigatoriedade não são claros o suficiente, o que pode ser corrigido via ato normativo da autoridade; o segundo, o fracasso completo do RIPD como ferramenta, visto que se os critérios para a sua obrigatoriedade são obscuros, tampouco impedem a implementação de processamento: prossegue-se com a atividade de alto risco, para elaborar o relatório apenas quando solicitado diretamente. Em suma, uma verdadeira carta-branca para o não cumprimento da obrigação de *compliance*. A Autoridade Nacional teria que, às cegas, identificar os controladores cujas atividades atraíam a necessidade de *enforcement*, requisitar a elaboração do relatório, dar um prazo específico, receber o relatório, avaliar se ele foi elaborado, corretamente, se há altos riscos iniciais, e se há altos riscos residuais, para, então, conseguir auxiliar o controlador e verificar a conformidade. Esse tipo de abordagem

³⁵¹ CABRAL, Filipe F. **O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais** –Lei nº 13.709/18. (2019) Tese (Mestrado em Direito) –Faculdade de Direito. Universidade Estadual do Rio de Janeiro. Rio de Janeiro. p. 82.

³⁵² GRASSO, Ian Matiello. **Relatório de impacto à proteção de dados pessoais na Lei Geral de Proteção de Dados: uma banalização?** Cadernos Jurídicos da Faculdade de Direito de Sorocaba, v. 3, n.1, 2021, p.142-174.

dissipará o tempo e esforço da recém-criada ANPD para onde ela é realmente necessária.

O momento mais adequado para a identificação, pela ANPD, se o controlador cumpriu com as suas obrigações de elaborar o RIPD (avaliar conformidade, identificar riscos e mitigá-los) é em uma notificação de vazamento de dados. Além de estar sujeito à pura discricionariedade, ou na melhor das hipóteses, de uma discricionariedade vinculada, a requisição pode onerar os controladores que não possuem atividades de alto risco, apenas porque uma autoridade requisitou o relatório, que será feito às pressas, apenas para ser entregue, desprovido de todas as suas funções principais³⁵³.

Dentro desse cenário brasileiro, e analisando e observando o problema do uso secundário de dados com fundamento no legítimo interesse, percebe-se a obscuridade na definição da necessidade do relatório de impacto à proteção de dados na LGPD. Com um olhar crítico e atento ao GDPR, o qual dedicou uma seção inteira para o tema (seção 3), que trata da avaliação de impacto sobre a proteção de dados e consulta prévia, identifica-se a necessidade de uma alteração legislativa na LGPD, em seu art. 38, o qual deve acrescentar um rol obrigatório para a elaboração do RIPD, para que haja mais segurança jurídica, mitigação de riscos e definição do conceito de “tratamento de alto risco”, para maior e melhor controle da ANPD.

Para refletir sobre o tema do uso secundário de dados pessoais e o fundamento no legítimo interesse, analisando possíveis salvaguardas e mitigações de risco, tratar-se-á de apresentar uma proposta legislativa de alteração do RIPD na LGPD, como sugestão final para esta pesquisa.

³⁵³ GRASSO, Ian Matiello. **Relatório de impacto à proteção de dados pessoais na Lei Geral de Proteção de Dados: uma banalização?** Cadernos Jurídicos da Faculdade de Direito de Sorocaba, v. 3, n.1, 2021, p.142-174.

4.1 Uso secundário de dados pessoais com legítimo interesse e a proposta legislativa de alteração da LGPD

O possível uso secundário de dados pessoais com fundamento no legítimo interesse, tratado no capítulo 3, assusta todos os titulares de dados pessoais à medida que essa base legal se apresenta com conceito amplo e, por seu grau de subjetividade, gera discussão.

Historicamente, o legítimo interesse tem sido encarado como a mais flexível das bases legais no regime comunitário europeu³⁵⁴. Essa premissa vai ao encontro da declaração do ex-diretor do Google, Marcel Leonardi, o qual afirmou que 70% do tratamento de dados, declarados pelas empresas, tem como base legal o legítimo interesse³⁵⁵. Esse é um número bastante significativo, principalmente se comparado ao consentimento, que representa apenas 5% do tratamento de dados declarado³⁵⁶.

Uma das possíveis soluções, acerca do tema dessa pesquisa, com o intuito de tentar mitigar o uso secundário de dados pessoais, baseado no legítimo interesse, é uma alteração legislativa no art. 38 da LGPD, o qual, hoje, prevê, apenas, a “possibilidade” da autoridade nacional determinar ao controlador que elabore relatório de impacto à proteção e dados pessoais, inclusive os sensíveis, nos termos de regulamento. Com efeito, a LGPD deverá ter previsão de situações cujo RIPD é obrigatório, sempre com um olhar atento a essa matéria, tratada no GDPR.

Em nível de comparação, a primeira diferença relevante entre as legislações é que no GDPR há um capítulo específico sobre o relatório de impacto, porém na LGPD o tema está disperso entre os capítulos. No capítulo que trata das disposições preliminares há disposição no sentido de que a ANPD deverá solicitar relatórios de impacto em relação às exceções previstas no inciso III do artigo 4º e há também a definição de relatório de impacto no artigo 5º, XVII.

Na sequência, no capítulo intitulado “Do tratamento de dados pessoais”, especificamente no artigo 10, que fala sobre a base legal do legítimo interesse, há

³⁵⁴ BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed., Rio de Janeiro: Forense, 2021, p. 248-249.

³⁵⁵ BERBERET, Lúcia. **“Interesse legítimo” supera “consentimento” no tratamento de dados pessoais pelas empresas**. Disponível em: <<https://telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>>. Acesso em: 16 mai. 2023.

³⁵⁶ DILL, Amanda Lemos. **A delimitação dogmática do legítimo interesse para tratamento de dados pessoais**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). Lei geral de proteção de dados: aspectos relevantes. Indaiatuba, SP: Editora Foco, 2021. p. 95- 118.

menção sobre a *possibilidade* de a ANPD solicitar a elaboração do relatório de impacto. No capítulo que trata “Do tratamento de dados pessoais pelo poder público” (art. 32, seção II, capítulo IV), a lei fala que a ANPD poderá solicitar, aos agentes do poder público, a publicação do relatório de impacto. Novamente, apresenta-se a faculdade da elaboração do RIPD.

No capítulo “Dos agentes de tratamento de dados pessoais”, no artigo 38, a lei traz os requisitos mínimos que devem conter no relatório de impacto e, por fim, no artigo 55-J, dentro do capítulo “Da autoridade nacional de proteção de dados (ANPD) e do conselho nacional de proteção de dados pessoais e da privacidade”, o legislador fala sobre a responsabilidade da ANPD na edição de regulamentos sobre o relatório de impacto.

Observa-se, dessa forma, que a maior parte das menções sobre o relatório de impacto à proteção de dados pessoais referem-se à possibilidade de a ANPD solicitar a elaboração do documento, e a menor parte demonstra as definições e requisitos mínimos necessários.

Ao contrário do que ocorre na LGPD, no GDPR há um capítulo denominado avaliação de impacto sobre a proteção de dados, dedicado às exposições específicas sobre a avaliação e o relatório de impacto à proteção de dados, nos artigos 35º e 36º. É possível encontrar, nesses artigos, as definições, a indicação da pessoa responsável pelo documento, o momento indicado para a elaboração, os casos em que é obrigatória a elaboração do relatório de impacto, os papéis das autoridades de proteção de dados, entre outros tópicos.

Outra diferença observada na análise das duas legislações é a especificação do momento em que o relatório deve ser elaborado. No GDPR há previsão, no artigo 35, 1, de que o relatório de impacto deve ser realizado antes do início do tratamento; na LGPD, encontra-se, entre as competências da ANPD no art. 55-J, inciso XIII, a previsão da edição de regulamentos e procedimentos sobre a proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais. É importante destacar que no GDPR há definição do que seria um tratamento de dados pessoais de *alto risco* e das atividades que ensejam a obrigatoriedade de elaboração do relatório de impacto, ao contrário da LGPD que apenas menciona a necessidade de elaborar o documento quando os processos de tratamento podem gerar riscos às

liberdades civis e aos direitos fundamentais, sem especificar quais seriam esses tratamentos de alto risco.

No GDPR, o responsável pelo tratamento deve solicitar o parecer do encarregado de proteção de dados, quando ele tiver sido designado. Também poderá solicitar a opinião dos titulares de dados, quando for adequado. Na LGPD não há menção sobre essas questões acima descritas.

Quanto às semelhanças, as duas legislações trazem os procedimentos para elaboração do relatório de impacto. O GDPR informa que a avaliação de impacto deve possuir, pelo menos, a descrição, a finalidade, a necessidade e a proporcionalidade do tratamento, também uma avaliação de riscos para direitos e liberdades dos titulares e as medidas a serem tomadas frente aos riscos, como forma de demonstração de conformidade com a lei. A partir da análise do artigo 38 da LGPD, depreende-se apenas que o relatório de impacto deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Diante do exposto, fica claro que a descrição desses procedimentos é bem mais completa no GDPR. Outro ponto a ser analisado é que, tanto a LGPD quanto o GDPR trazem previsões sobre o papel das autoridades nacionais na regulamentação do tema nos países, ocorre que na LGPD há apenas a descrição dos momentos em que a ANPD poderá solicitar o RIPD e a sua responsabilidade em regulamentar a matéria, já no GDPR existe uma orientação mais completa, de que o responsável pelo tratamento de dados pessoais deverá consultar a autoridade nacional antes de iniciar o tratamento quando houver elevado risco, da possibilidade de a autoridade elaborar e tornar públicas listas das operações de tratamento indicando quando é necessário e quando não é necessário elaborar o relatório de impacto. Para elucidação desse ponto, segue a tabela abaixo, apresentando uma comparação entre o GDPR e a LGPD, no que se refere ao relatório de impacto à proteção de dados:

Características	LGPD	GDPR
Capítulo específico sobre o tema	Não	Sim
Momento da elaboração	Não	Sim
Definição de alto risco	Não	Sim
Solicitação de parecer do encarregado de dados	Não	Sim
Solicitação de opinião do titular de dados	Não	Sim
Procedimentos para a elaboração	Sim	Sim
Autoridades nacionais vinculadas ao RIPD	Sim	Sim

Fonte: MIRANDA, Lara Soares. Relatório de Impacto à proteção de dados: um estudo comparado entre o direito brasileiro e o europeu. Universidade Federal de Uberlândia. 2021.

Quanto ao processo prático de elaboração do relatório de impacto, já houve na Europa regulamentação do tema pelo EDPS, porém no Brasil a ANPD ainda está em processo de análise do tema.

No momento dessa pesquisa, a Autoridade Nacional de Proteção de Dados se ocupa de esclarecer à sociedade e às organizações acerca das salvaguardas protetivas, mais especificamente sobre a elaboração do relatório de impacto à proteção de dados, visando a mitigar os riscos que podem surgir no tratamento dos dados pessoais. Com efeito, o processo de regulamentação do tema está em andamento, com agenda prevista para os biênios de 2023/2024.

Dentro dessa pesquisa de proteção de dados, com salvaguardas e mitigações de risco no tratamento de dados, em razão do uso secundário com fundamento no legítimo interesse, é essencial observar, verificar e analisar o relatório de impacto à proteção de dados elaborado pelo Tribunal de Contas da União, com sua elaboração baseada em probabilidades, impacto e nível de risco, o qual será abordado a seguir.

4.2 Análise do Relatório de Impacto à Proteção de Dados no TCU

Para analisar a relevância de um relatório de impacto em matéria de proteção de dados, com o objetivo de mitigar o risco do uso secundário de dados com fundamento no legítimo interesse, toma-se como exemplo o documento

desenvolvido pelo Tribunal de Contas da União. O TCU elaborou um relatório de impacto à proteção de dados no âmbito das contratações do Tribunal, em 2021. Como observação desse modelo de boas práticas, verifica-se que são imprescindíveis ações contínuas, consistentes e abrangentes, como salvaguarda à mitigação de riscos na proteção de dados.

O TCU conhece a necessidade de monitoramento e reavaliação permanente em prol da proteção de dados pessoais³⁵⁷. Essas práticas devem estar inseridas em um sistema de governança eficiente e integrado³⁵⁸. Não é demais lembrar, a esse propósito, que a LGPD dedicou sessão específica para tratar das Boas Práticas e da Governança, arts. 50 e 51, seção II), o que reforça a responsabilidade atribuída às instituições na garantia da proteção aos dados pessoais, agora direito fundamental expressamente consagrado na Constituição federal.

Preliminarmente, o RIPD do TCU apresenta pressupostos teóricos e metodológicos, com requisitos essenciais para a elaboração do RIPD, como transposto a seguir³⁵⁹:

Item	Requisito	Fundamento
1	Descrição do Relatório de Impacto à Proteção de Dados	Art. 5º, XVII, da LGPD
2	Descrição dos tipos de dados pessoais coletados	Parágrafo único do art. 38 da LGPD
3	Método de coleta dos dados pessoais	Parágrafo único do art. 38 da LGPD
4	Riscos na proteção e dados pessoais	Não há fundamento legal direto, mas esse requisito é mero corolário da necessidade de indicar medidas de mitigação de riscos (não é possível indicar medidas de mitigação de riscos sem a identificação de tais riscos)

³⁵⁷ TRIBUNAL DE CONTAS DA UNIÃO. Relatório de impacto à proteção de dados. Disponível em: <https://portal.tcu.gov.br/data/files/FD/20/E4/CA/202128102DFE0FF7F18818A8/Relatorio%20de%20Impacto%20a%20Protecao%20de%20Dados%20Pessoais_web.pdf>. Acesso em: 15 mai. 2023.

³⁵⁸ Ibidem.

³⁵⁹ Ibidem.

5	Medidas de salvaguarda e mitigação de riscos e metodologia para garantir a segurança das informações	Art. 5º, XVII, c/c parágrafo único do art. 38, da LGPD
6	Análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados	Parágrafo único do art. 38 da LGPD.

Fonte: Portal do TCU.

Para a elaboração e planejamento desse documento, o TCU contou com a atuação da Secretaria de Licitações, Contratos e Patrimônio (Selip), a qual elaborou algumas planilhas de boas práticas. Com efeito, o Tribunal seguiu o regramento da ISO 31000.³⁶⁰

Como a LGPD expressamente estabelece que os riscos devem ser mitigados (art. 5º, XVII, e parágrafo único do art. 38), foi adotado o conceito de risco pelo *viés negativo*, segundo o qual o risco é um evento que pode afetar adversamente o alcance dos objetivos relacionados à proteção de dados pessoais.

Segundo a ISO 31.000, “escopo, contexto e critérios envolvem a definição do escopo do processo, a compreensão dos contextos externo e interno”. Faz parte do processo, também, a definição da forma de mensuração da probabilidade e do impacto dos riscos. Tanto na probabilidade quanto no impacto foi utilizada a sequência de Fibonacci³⁶¹ (3, 5, 8, 13 e 21), de probabilidade muito alta para muito baixa, considerando as vantagens apontadas por Benedito Antônio da Costa.

Existem várias fases relativas ao desenvolvimento do RIPD no TCU, entre elas: (i) descrição dos tipos de dados pessoais coletados, (ii) riscos na proteção de dados, (iii) medidas de salvaguarda e mitigação de riscos, (iv) classificação da informação, (v) descarte de dados pessoais pelos fiscais de contratos, (vi) revisão das regras de acesso ao sistema áurea e as suas funcionalidades, (vii) fixação de critérios de temporalidade para guarda de documentos eletrônicos no sistema e-TCU, (viii) expedição formal de orientação aos agentes de tratamento de dados, (ix) obrigação de as empresas terceirizadas enviarem dados pessoais ao TCU de forma criptografada e contendo apenas dados de funcionários em exercício no TCU, (x) avaliação das medidas de mitigação de riscos e (xi) classificação da informação .

³⁶⁰ Associação Brasileira de Normas Técnicas, **NBR ISO 31.000**: Gestão de Riscos: Diretrizes. Rio de Janeiro: 2018. Disponível em: <<https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf>>. Acesso em: 15 mai. 2023.

³⁶¹ BRASIL. **Tribunal Regional Eleitoral de Mato Grosso**. Revista Democrática. Costa, Benedito Antônio. Utilização da Escala de Fibonacci na avaliação de riscos: vantagens, aplicações e didática. Volume 5. Cuiabá: 2019.

Relevante, neste ponto da pesquisa, apresentar, na prática, a forma como os dados são coletados no TCU. Para isso, segue a tabela abaixo, com algumas adaptações:

Fase do Processo de Contração	Categoria	Tipos de dados coletados	Método de coleta dos dados
Licitação	Dados cadastrais do representante da empresa	Nome, CPF e RG	Extração de sistemas governamentais
Fiscalização	Dados referentes aos funcionários terceirizados, para acompanhamento previdenciário, fiscal e trabalhista	Nome, CPF, RG, carteira de trabalho, exames médicos admissionais e demissionais, cópias de contracheques, comprovantes de transferências bancárias, cópias de extratos do INSS e FGTS (...)	Recebimento via e-mail ou documento encaminhado pela empresa (comunicação, proposta) endereçado aos fiscais de contrato

Fonte: Adaptação da tabela 2.2 do RIPD do TCU³⁶².

Para a identificação, análise e avaliação dos riscos associados ao tratamento dos dados pessoais foi criada uma tabela, produto da oficina realizada por especialistas³⁶³, que atribuíram nota de probabilidade e impacto para cada risco identificado, considerando a escala fornecida. A escala utilizada tem os valores possíveis de 3, 5, 8, 13 e 21, sendo 3 o menor valor a ser atribuído para probabilidade/impacto dos riscos e 21 o maior valor possível de atribuição. Os resultados foram validados em discussões e reflexões em grupo. Dentro desse estudo, o nível do risco é o produto da multiplicação da probabilidade com o impacto.

A tabela leva em consideração vários itens, entre eles:

³⁶² TRIBUNAL DE CONTAS DA UNIÃO. Relatório de impacto à proteção de dados. Disponível em: <https://portal.tcu.gov.br/data/files/FD/20/E4/CA/202128102DFE0FF7F18818A8/Relatorio%20de%20Impacto%20a%20Protecao%20de%20Dados%20Pessoais_web.pdf>. Acesso em: 15 mai. 2023.

³⁶³ Ibidem.

Risco	Probabilidade	Impacto	Nível do risco
Acesso aos dados pessoais por pessoa não autorizada	13	8	104
Utilização dos dados pessoais para outra finalidade que não a informada ao titular	5	13	65
Vazamento de dados pessoais	5	13	65
Reidentificação de dados anonimizados	8	8	64
Acesso aos dados pessoais fora das hipóteses previstas na LGPD (finalidade, adequação, necessidade)	5	18	40
Utilização de informações desatualizadas no tratamento de dados pessoais	3	3	9

Fonte: Adaptado do RIPD do TCU

Do quadro acima, infere-se que apenas o risco “acesso aos dados pessoais por pessoa não autorizada” representa risco “alto”. Os demais se apresentam como riscos “médios”, “baixos” ou “muito baixos”.

Com os riscos avaliados, segue-se a fase de tratamento dos riscos. Como a LGPD expressamente prevê, com a mitigação dos riscos relacionados à proteção de dados pessoais, tem-se a imposição de implementação de controles internos, ou seja, medidas de salvaguarda para redução e prevenção de tais riscos. As medidas de salvaguarda em privacidade de dados têm o objetivo de reduzir o nível de risco suportado pelo processo de trabalho. Usualmente, os controles são aplicados somente para os riscos de nível “alto” ou “muito alto”. No entanto, os controles relativos à privacidade de dados têm por característica serem transversais, isto é, capazes de mitigar simultaneamente mais de um risco. Por exemplo, um controle lógico de criptografia tem a capacidade de mitigar não só o risco de acesso aos

dados pessoais por pessoa não autorizada, mas também os de vazamento de dados pessoais e divulgação não autorizada desses dados, na medida em que, mesmo que os dados sejam vazados/divulgados, o receptor de tais dados não consegue acessá-los. Desta forma, apesar de as medidas propostas no relatório terem como objetivo principal a mitigação do risco “acesso aos dados pessoais por pessoa não autorizada”, considerado neste trabalho como de nível “alto”, elas também têm a capacidade de mitigar os demais riscos à proteção de dados pessoais relacionados ao processo de contratação. Outro fator considerado na proposição dos controles foram as balizas legais que delimitam toda a atividade de contratação e sua correspondência com a base principiológica da LGPD, o que já foi estudado no capítulo 3 desta pesquisa.

Ainda neste relatório, recomenda-se que seja expedida orientação formal em que constem cuidados e controles no tratamento de dados pessoais, de fácil implementação. A orientação deve ser balizada pelos princípios que regem o tratamento de dados, sobretudo os da *finalidade, necessidade e transparência*.

Nesse sentido, pode-se, por exemplo, instruir os agentes a: (i) reduzir a quantidade de dados pessoais coletados em seus processos de trabalho ao mínimo necessário ao propósito de tratamento; (ii) evitar propagar cópias de e-mails que contenham dados pessoais; (iii) evitar duplicar e armazenar, sem que seja necessário, documentos que contenham dados pessoais; (iv) orientar as empresas contratadas a encaminhar somente os documentos dos prestadores de serviços alocados aos contratos fiscalizados; (v) dispensar dados pessoais em documentos e informações que não sejam absolutamente necessários e (vi) estabelecer rotinas de controle de acompanhamento dos vínculos contratuais e descarte de registros de dados pessoais do sistema Contrata, de modo que nele não fiquem armazenados dados desnecessários.

Outras medidas, objeto de orientação, podem ser avaliadas, em conjunto com as unidades responsáveis pela área de TI do Tribunal. Cita-se, como exemplo, a possibilidade de que os agentes sejam instruídos a intensificar o uso de soluções já contratadas e disponíveis, como a criptografia nas mensagens de e-mail.

Seguindo as etapas da ISO 31000, com suas ferramentas de projetos, processos e atividades, o RIPD do TCU ainda prevê: padronização de cláusulas contratuais que estabeleçam a obrigação de as empresas terceirizadas enviarem os dados pessoais ao TCU de forma criptografada, contendo, exclusivamente, os

dados de funcionários em exercício no TCU, avaliação das medidas de mitigação de riscos, classificação da informação, descarte de dados pessoais pelos fiscais de contratos e pela comissão de licitação ou pelo pregoeiro, revisão de acesso ao sistema “áurea”³⁶⁴ e a suas funcionalidades, fixação de critérios de temporalidade para guarda de documentos de fiscalização de contratos no sistema e-TCU e, por fim, expedição formal de orientação para agentes que atuam nos processos de contratação e gestão contratual.

Considerando o momento desta dissertação, o TCU publicou, em 21 de junho de 2022, uma auditoria³⁶⁵ realizada com base no risco de dados pessoais coletados e tratados pela Administração Pública Federal. Por meio dela, avaliou as ações governamentais e os riscos à proteção de dados pessoais.

A análise abrangeu 382 organizações e abordou a condução de iniciativas governamentais para providenciar a adequação à Lei Geral de Proteção de Dados (LGPD) e às medidas implementadas para o cumprimento das exigências estabelecidas na Lei. O trabalho também comparou as organizações auditadas quanto ao nível de adequação à LGPD e concluiu que 17,8% estão no nível inexpressivo; 58,9% estão no nível inicial; 20,4% estão no nível intermediário e 2,9% estão no nível aprimorado. O diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD apresentou, portanto, situação de alto risco à privacidade dos cidadãos que têm dados pessoais coletados e tratados pela Administração Pública Federal.

Dessa forma, analisando o relatório de impacto à proteção da dados do TCU, observa-se que esse documento é uma grande garantia para as organizações. Seu objetivo é a avaliação sistemática e completa dos aspectos pessoais relacionados a pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, e que resultam em decisões que produzem efeitos jurídicos relativos a essas pessoas ou que as afetem, significativamente, de forma similar.

³⁶⁴ Sistema “áurea” é o sistema da plataforma do TCU.

³⁶⁵ BRASIL, Tribunal de Contas da União. TCU verifica alto risco à privacidade de dados pessoais coletados pelo governo. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em: 06 jun. 2023.

5 CONCLUSÃO

Em razão do risco permanente do uso secundário de dados pessoais baseado no legítimo interesse, observou-se a necessidade de utilizar salvaguardas para antecipar e mitigar riscos no tratamento de dados, assim como subsidiar a interpretação e aplicação de novos institutos. Para tanto, a compreensão do objeto proteção de dados na tutela civilista e os valores subjacentes à disciplina permitem refletir acerca das principais características e de algumas condições que conduziram à necessidade de um olhar para o ordenamento jurídico estrangeiro, principalmente para o GDPR, para enfrentar algumas inconsistências que se apresentam na LGPD.

Conforme apontado ao longo desta dissertação, o uso secundário de dados pessoais e seu fundamento no legítimo interesse potencializou a preocupação dos Estados em proteger os dados pessoais, com vista a caminhar para um tratamento de dados compatível com a sua coleta e finalidade originárias.

Em sede introdutória, o trabalho abordou as escolhas metodológicas e recortes temáticos da pesquisa sobre o uso secundário de dados e seu fundamento no legítimo interesse. Em razão da escolha por analisar, estritamente, a legislação brasileira e a europeia, em proteção de dados, não foram abordados casos materiais ou conflitos específicos de leis ou jurisdição. Dessa forma, a condução da pesquisa se estabeleceu pelas lentes do Direito Civil brasileiro e considerou a influência do instrumento regulatório europeu, em nível de experiência e maturidade jurídica.

A presente pesquisa se propôs a atenuar as divergências doutrinárias acerca do uso secundário de dados e seu fundamento no legítimo interesse. Para tanto, levantou-se a hipótese de que o legítimo interesse, por ser um conceito jurídico indeterminado ou uma cláusula geral, representa, de fato, uma grande justificativa para o uso secundário de dados.

A resposta desta dissertação perpassa pela análise do valor e da dimensão dos dados pessoais enquanto informação relacionada a pessoa natural identificada ou identificável e seu entrelaçamento com o direito da personalidade. O uso secundário de dados pessoais, o qual é uma preocupação da pesquisa, necessita da baliza do princípio da finalidade, o qual prevê a realização do tratamento para

propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Para tanto, o trabalho foi dividido em 3 partes, conforme a estrutura do sumário, que são elas: (i) tratamento de dados pessoais e uso secundário de dados, (ii) diálogo principiológico no uso secundário de dados: teste da base legal do legítimo interesse e, por fim, uma (iii) proposta legislativa da *lege lata* a *lege ferenda*.

A primeira parte abordou os fundamentos mais relevantes à proteção de dados na LGPD, entre eles, a autodeterminação informativa (*informationelles Selbstbestimmungsrecht*). Na sequência, tratou-se de analisar as diferenças entre dado pessoal e informação, com um olhar para o uso secundário de dados pessoais, levando em consideração o conteúdo do dado pessoal como sendo uma informação relacionada à pessoa natural identificada ou identificável. Além disso, ainda na primeira parte, ingressou-se no uso secundário de dados pessoais, apresentando o seu liame com o princípio da finalidade, pois a informação se torna muito mais valiosa ao longo do tempo³⁶⁶. Nas lições de Mayer e Cukier³⁶⁷, o “sistema vale-se da informação obtida por uma finalidade e a reutiliza para uma finalidade distinta - em outras palavras, o dado se move do uso primário ao uso secundário”, ou seja, o valor dos dados precisa ser considerado em termos de todas as possíveis maneiras que poderá ser empregado no futuro.

A segunda parte desta dissertação trabalhou o diálogo principiológico no uso secundário de dados e o teste da base legal do legítimo interesse. O legítimo interesse é uma das dez bases legais previstas na LGPD para tratamento de dados pessoais (art.7º,IX). Foram analisadas, nesta pesquisa, duas bases legais – legítimo interesse e consentimento - as quais são hipóteses autorizativas de tratamento de dados pessoais, e englobam um grande número de operações realizadas com tais dados pessoais, incluindo a coleta, sua classificação, utilização, acesso, transmissão, processamento, armazenamento, eliminação, entre outros (art. 5º, X da LGPD).

Ao longo do trabalho foi demonstrado que não existe hierarquia entre as bases legais, mas sim base legal mais ou menos adequada a determinado tratamento de dados. O recorte desta dissertação tratou do legítimo interesse, o

³⁶⁶ MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: a revolution that will transform how we live, work and think. First Mariner Books: New York, 2014, p. 103.

³⁶⁷ Ibidem.

qual justifica o uso posterior de dados, por criar algumas possibilidades de tratamento. Foi observado que a LGPD estabeleceu as figuras do controlador e do operador, denominados como agentes de tratamento. O que os diferencia é o poder decisório sobre o tratamento que se dará aos dados pessoais, ou seja, enquanto o primeiro decide, o segundo cumpre as suas determinações. Dessa forma, foi fundamental abordar os textos legais da Diretiva 95/46/CE e do GDPR, em razão da influência direta do processo legislativo europeu na lei brasileira, devido ao longo processo de construção de um consenso transnacional acerca dos princípios básicos que regem a matéria de proteção de dados pessoais.

Por fim, a última parte do presente estudo propôs uma alteração legislativa no artigo 38 da LGPD em razão da observação e da análise, por toda a pesquisa, da necessidade de a Lei exigir o relatório de impacto à proteção de dados em algumas situações específicas, quando o tratamento envolve a avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem, significativamente, de forma similar; da mesma forma, quando houver operações de tratamento em larga escala de categorias especiais de dados, e em situações de controle sistemático de zonas acessíveis ao público em grande escala, além de outras situações em que direitos fundamentais de pessoas singulares estejam em risco.

De forma sintética e para responder a pergunta da pesquisa sobre quais os limites e condicionantes para a aplicação do legítimo interesse no uso secundário de dados, entende-se que o teste da base legal do legítimo interesse, com suas quatro fases, que são (i) legitimidade, (ii) necessidade, (iii) balanceamento e (iv) salvaguardas reflete, exatamente, a estrutura do art. 10 da LGPD, e tem a finalidade de garantir segurança no tratamento e no uso secundário de dados com fundamento no legítimo interesse. Contudo, essa base legal se apresenta como uma porta aberta para qualquer tratamento de dados, mesmo com o teste de avaliação do legítimo interesse. Sendo assim, um dos instrumentos capazes de mitigar o risco desse tratamento realizado pelo controlador é o relatório de impacto à proteção de dados, o qual pode ser desenvolvido, como na análise do RIPD do TCU, em forma de escala multifatorial que contenha: vetores de risco, probabilidade, impacto e nível de risco.

Depois de analisar algumas possibilidades ao longo desta dissertação, conclui-se pela necessidade de a lei brasileira de proteção de dados prever a obrigação do RIPD , em algumas situações já citadas, razão pela qual foi proposta a alteração legislativa no artigo 38 da LGPD, com o objetivo de garantir maiores salvaguardas e maior proteção no tratamento dos dados pessoais, sugestão essa que visa a estabelecer parâmetros legais mais concretos para a determinação da elaboração do RIPD e, conseqüentemente, maior proteção no momento da aplicação do uso secundário de dados com fundamento no legítimo interesse.

REFERÊNCIAS BIBLIOGRÁFICAS

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, **Processo C-311/18**. Disponível em:< Acesso em 08.11.2021.

ALBERS, Marion. **A complexidade da proteção dados**. Direitos Fundamentais e Justiça, ano 10, n. 35, jul.-dez.-dez., 2016, p. 410-433.

ANPD. **Resolução CD/ANPD nº4**. Disponível em:<<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucao4CDANPD24.02.2023.pdf/view> >. Acesso em: 07 mar. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, **NBR ISO 31.000**: Gestão de Riscos: Diretrizes. Rio de Janeiro: 2018. Disponível em: <<https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf>. Acesso em: 15 mai. 2023.

ÁVILA, Humberto. **Teoria dos Princípios**: da definição à aplicação dos princípios jurídicos. 9 ed., rev. e atual. São Paulo: Malheiros, 2018.

ÁVILA, Humberto. **Subsunção e concreção na aplicação do direito**. In: MEDEIROS, Antônio Paulo Cachapuz de (Org.). Faculdade de Direito da PUC-RS: o ensino jurídico no limiar do novo milênio. Porto Alegre:Edipuc-RS, 1997,P.413-465, P.413.

BALBONI, Paolo; COOPER, Daniel; IMPERIALI, Rosario; MACENAITE, Milda. **Legitimate interest of the data controller**: New Data protection paradigm: legitimacy grounded on appropriate protection. International Data Privacy Law, Oxford, v.3, N.4, P. 244-261, 2013.

BARBOSA, Elisandra Cristina. **A Boa-Fé na Relação Contratual e o Princípio da Confiança**. São Paulo: Pontifícia Universidade Católica de São Paulo, 2008. Disponível em: <<https://repositorio.pucsp.br/bitstream/handle/8274/1/Elisandra%20Cristina%20Barbosa.pdf> > Acesso em: 28 dez. 2022.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run Around Consent and Anonymity. In: LANE, J.; STODDEN, V.; BENDER, S.; NISSENBAUM, H. (Ed.) Privacy, Big Data and the Public Good. CAMBRIDGE: Cambridge University Press, 2014,. 44-75.

BERBERET, Lúcia. **"Interesse legítimo" supera "consentimento" no tratamento de dados pessoais pelas empresas.** Disponível em: <<https://telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>>. Acesso em: 16 mai. 2023.

BIONI, Bruno Ricardo. **O dever e informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores:** convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo 'Lulu'. Revista de Direito do Consumidor, v. 94, p.283-326, 2014.

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

BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. **Relatório de Impacto à Proteção de Dados e Avaliação de Legítimo Interesse.** In: BLUM, Renato; VAINZOF, Rony; MORAES, Henrique. **Data Protection Officer (Encarregado): Teoria e Prática de Acordo com a LGPD e o GDPR.** São Paulo (SP): Editora Revista dos Tribunais, 2022. Disponível em <<https://thomsonreuters.jusbrasil.com.br/doutrina/1481212764/data-protection-officer-encarregado-teoria-e-pratica-de-acordo-com-a-lgpd-e-gdpr>>. Acesso em: 14 abr. 2023.

BRASIL. Código Civil Brasileiro. Disponível em <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm> Acesso em: 2 abr. 2023.

BRASIL. **Constituição Federal**. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais>. Acesso em: 31 out. 2022.

BRASIL. Lei 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Disponível em:

<https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%Aancias.&text=Art.,48%20de%20suas%20Disposi%C3%A7%C3%B5es%20Transit%C3%B3rias> Acesso em: 28 dez. 2022.

BRASIL. **Lei 12.527, de 18 de novembro de 2011**. 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 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, e 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 11 nov. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em:<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 abr. 2023.

BRASIL, **Tribunal de Contas da União**. TCU verifica alto risco à privacidade de dados pessoais coletados pelo governo. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>. Acesso em: 06 jun. 2023.

BRASIL. **Tribunal Regional Eleitoral de Mato Grosso**. Revista Democrática. Costa, Benedito Antônio. Utilização da Escala de Fibonacci na avaliação de riscos: vantagens, aplicações e didática. Volume 5. Cuiabá: 2019.

BUCAR, Daniel; VIOLA, Mario. **Tratamento de dados pessoais por “legítimo interesse do controlador”**: primeiras questões e apontamentos. FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro. São Paulo: Thomson, 2019, p.475.

CABRAL, Filipe F. O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais –Lei nº 13.709/18. (2019) Tese (Mestrado em Direito) –Faculdade de Direito. Universidade Estadual do Rio de Janeiro. Rio de Janeiro. p. 82.

CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000.(A era da informação: economia, sociedade e cultura, p. 67-215.

CATALA, Pierre. **Ebauche d’une théorie juridique de l’information**. In: Informatica e Diritto, ano IX, jan-apr., 1983, p. 22. Disponível em:<<https://mafr.fr/media/assets/publications/catalap-ebauche-dune-theorie-juridique-de-linformation-1998.pdf>>. Acesso em: 08 jan. 2023.

CATE, Fred H. and MAYER-SCHÖNBERGER, Viktor. **Notice and Consent in a World of Big Data**. Indiana: Maurer School of Law, 2013, p. 67-73. Disponível em: <<https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3662&context=facpub> >. Acesso em: 18 jan. 2023.

CHIAPPETTA, Aline Holanda. **Transferências transatlânticas de dados pessoais na era pós-Snowden à luz do Regulamento Geral sobre a Proteção de Dados**. Coimbra. 2018.

CLARKE, Roger A. Information Technology and dataveillance. **Communications of the ACM**, v. 31,n 5, mai./1988, p.498-512.

COLOMBO, Cristiano; NETO, Eugênio Facchini. ROSENWALD, Nelson; MARTINS, Guilherme Magalhães(Org.) **Decisões automatizadas em matéria de perfis e riscos algorítmicos**: diálogos entre Barsil e Europa acerca dos direitos das vítimas de dano estético digital. Ed. Foco, 2020, p. 176.

COMISSÃO EUROPEIA. **Decisão 2016/1250/EC**. C(2016) (4176). 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG> Acesso em: 10 dez. 2022.

CONVENÇÃO EUROPEIA. **Convenção 108 do Conselho da Europa**. Disponível em: < <https://rm.coe.int/1680078b37>>. Acesso em: 11 jan. 2023.

CORDEIRO, A. Barreto Menezes. **Direito da Proteção de dados: à luz Do RGPD e da Lei n. 58/2019**. Coimbra: Al Medina, 2020, p. 110.

COUNCIL OF EUROPE. **Convention for the protection of individuals with regard to automatic processing of personal data**. Strasbourg, v. 108, 1981. Disponível em: <<https://rm.coe.int/1680078b37>> Acesso em: 11.11.22.

COUNCIL OF EUROPE. **Handbook on European Data Protection Law. Luxembourg**: Publications Office of the Europe Union, 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf >. Acesso em 01 jan. 2023.

DEUTSCHLAND. Bürgerliches Gesetzbuch-BGB. 1896, p. 58. Disponível em < <https://www.gesetze-im-internet.de/bgb/BGB.pdf> > Acesso em: 27 dez. 2022.

DEWEY, John. **Human Nature and Conduct**: An introduction to social psychology. Originally published in 1922. Cosimo Inc., mar. 2007, p. 115.

DILL, Amanda Lemos. **A delimitação dogmática do legítimo interesse para tratamento de dados pessoais**. In: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). Lei geral de proteção de dados: aspectos relevantes. Indaiatuba, SP: Editora Foco, 2021. p. 95- 118.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJL], 12(2), 91-108. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 23 out. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021. p. 307.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: BIONI, Bruno et al. (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 8.

DONEDA, Danilo; VIOLA, Mario. **Risco e Informação Pessoal**: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. Revista Brasileira de Risco e Seguro, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar.2010. p. 100.

DOUEK, Daniel; PASTORE, Ricardo; RENZETTI, Bruno. **Proteção de Dados e Direito de Concorrência**: a privacidade como diferencial competitivo. In: BRANCHER, Paulo Marcos Rodrigues e BEPPU, Ana Cláudia (coord.). Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei n. 13.709/2018. Belo Horizonte, Fórum, 2019, p. 126.

EDPB, **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**. Adopted on 10th November 2020. Disponível em: <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> Acesso em: 18.11.22.

ENGISCH, Karl. **Introdução ao pensamento jurídico**. Trad. de J. Baptista Machado. Lisboa: Fundação Calouste Gulbenkian, 1996, p.208-209.

ESSER, Josef. **Grundsatz und Norm in der Richterlichen Fortbildung des Privatsrechts**. 4 ed. Tübingen, Mohr, Siebeck, 1990. Disponível em <https://www.trans-lex.org/101900/_/esser-josef-grundsatz-und-norm-in-der-richterlichen-fortbildung-des-privatrechts-4th-ed-t%C3%Bcbingen-1990>. Acesso em: 26 dez. 2022.

EUROPEAN COMMISSION. **European Commission approves Trans-Atlantic Data Privacy Framework**. Disponível em: < <https://cdp.cooley.com/european-commission-approves-trans-atlantic-data-privacy-framework/#:~:text=European%20Commission%20Approves%20Trans%2DAtlantic%20Data%20Privacy%20Framework,-on%20December%2016&text=On%2013%20December%202022%2C%20the,from%20EU%20to%20US%20companies.> > Acesso em: 25 jan. 2023.

EUROPEAN UNION. **Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais**. Disponível em: <<https://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 11 jan. 2023.

EUROPEAN UNION. Regulation(EU) 2016/679. **General Data Protection Regulation**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 12 out. 2022.

EUROPEAN UNION. **Guidelines on Automated Individual decision-making and Profiling for the purpose of Regulation 2016/679**-Adopted on 3 October 2017-As last Revised and Adopted on February 2018. Disponível em:< https://www.ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826>. Acesso em: 25 abr. 2023.

EXECUTIVE ORDER 12333. **United States Intelligence Activities**. Disponível em:<<https://www.archives.gov/federal-register/codification/executive-order/12333.html>. Acesso em: 24 jan. 2023.

FERRARI, Isabela; BECKER, Daniel; Wolkart, Erik Navarro. **Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos**. São Paulo: Revista dos Tribunais, 2018, vol.995, p 4. Disponível em: < <https://dspace.almg.gov.br/handle/11037/30128>>. Acesso em: 19 dez. 2022.

FERRETI, Frederico. Data Protection and the Legitimate Interest of Data Controllers: Much Ado or About Nothing or the Winter of Rights? *Common Market Law Review*, n. 51(3):843-868. Acesso em: 25 abr. 2023.

FGV. **Guia de Proteção de Dados Pessoais**. Transferência Internacional. Versão 1.0-Outubro, 2020. Disponível <https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf>. Acesso em: 30 out. 2022.

FINCK, Michèle; PALLAS, Frank. **They who must not be identified**- distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, v. 10, n.1, p. 11-36, 2020, p.16.

FRADA, Manuel Antônio de Castro Portugal Carneiro da. **Teoria da Confiança e responsabilidade civil**. Coimbra: Almedina, 2004, p. 17-18.

GARCIA, Rafael Scaroni. **A mercadoria é você**: o uso secundário de dados pessoais. UFRGS. Porto Alegre, 2020. Disponível em <<https://www.lume.ufrgs.br/bitstream/handle/10183/248468/001125855.pdf?sequence=1&isAllowed=y>>. Acesso em: 10 abr. 2023.

GOMES, Maria Cecília Oliveira. **Para além de uma “obrigação legal”**: o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In: LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Org.). *Direito Digital: Debates Contemporâneos*. São Paulo: Revista dos Tribunais, 2019.

GOMES, Maria Cecília Oliveira. **Relatório de Impacto à proteção de dados**. Disponível em: <https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=relat%C3%B3rio+de+impacto+da+prote%C3%A7%C3%A3o+de+dados&btnG> Acesso em: 10 mar. 2023.

GÖTTING, Horst-Peter. **Inhalt, Zweck und Natur des Persönlichkeitsrechts**. In: GÖTTING, Horst-Peter; SCHERTZ, Christian; SEITZ, Walter. *Handbuch es Persönlichkeitsrechts*. C.H.Beck, München, 2008, p.2.

GRAFENSTEIN, Maximilian von. **The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation.** Nomos , Germany, 2018. Disponível em: https://pdfs.semanticscholar.org/6082/b3e2d80e810c0b2fe323e38d1304c14c77e4.pdf?gl=1*18npkyd*_ga*MTYwOTU3NzI1LjE2NzgwNDAwMzA.*_ga_H7P4ZT52H5*MTY3ODA0MDAyOS4xLjEuMTY3ODA0MDMxNS4wLjAuMA. Acesso em: 05 fev. 2018.

GRASSO, Ian Matiello. **Relatório de impacto à proteção de dados pessoais na Lei Geral de Proteção de Dados: uma banalização?**. Cadernos Jurídicos da Faculdade de Direito de Sorocaba, v. 3, n.1, pág.142-174, 2021.

GRUPO DE TRABALHO DO ARTIGO 29 PARA PROTEÇÃO DE DADOS. **Parecer 03/2023 sobre limitação da finalidade.** Abr. 2013. Disponível em: https://www.gdpd.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC03_2013%20%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_%E7%9B%AE%E7%9A%84%E9%99%90%E5%88%B6_PT.pdf > Acesso em 14 abr. 2023.

GRUPO DE TRABALHO DO ARTIGO 29 PARA PROTEÇÃO DE DADOS. **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE.** Abr. 2014. Disponível em: <[https://www.uc.pt-protecao-de-dados/suporte/20140409_wp_2017 - partecer_2_2014](https://www.uc.pt-protecao-de-dados/suporte/20140409_wp_2017-partecer_2_2014)>. Acesso em: 17 abr. 2023

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital: transformação digital-desafios para o direito.** 2 ed. Rio de Janeiro: Forense, 2022, p. 83-92.

HORNUNG, Gerrit, SCHNABEL, Christoph; **Data Protection in Germany I: The population Census Decision and the right to informational self-determination.** Computer Law & Security Report, v. 25, n. I, 2009, p.84.

IBC-Instituto Brasileiro de Coaching. Disponível em: <<https://www.ibccoaching.com.br/portal/coaching-e-financas/trade-off-o-que-e-e-qual-a-sua-importancia/>>. Acesso em: 24 abr. 2023.

ICO—Information Commissioner’s Office. Disponível em:<<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>>. Acesso em: 09 mar. 2023.

ICO-Information Commissioner’s Office. **The Information Commissioner’s response to a call for evidence on digital identity from the Secretary of State for the Department for Digital, Culture, Media and Sport.** 13 sep. 2019. Disponível em: <<https://ico.org.uk/media/about-the-ico/consultation-responses/2019/2616260/ico-response-dcms-call-for-evidence-20190913.pdf>> Acesso em: 13 jan. 2023.

KAMARA, Irene; DE HERT, Paul. **Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground:** a Pragmatic Approach. Brussels Privacy Hub Working Paper, vol.4,n.12, 2018. Acesso em: 20 abr. 2023.

KELLY, Kevin.**Out of Control:** the new biology of machines, social systems and the economic world. USA, 1995, 1. ed Basic Books, p. 101.

KRETZMANN, Renata Pozzi. O legítimo interesse no tratamento de dados do consumidor. Conjur, 2021. Disponível em:<<https://www.conjur.com.br/2021-out-06/garantias-consumo-legitimo-interesse-tratamento-dados-pessoais-consumidor>>. Acesso em: 10 abr. 2023.

LARENZ, Karl. **Metodologia da Ciência do Direito.** Trad. José Lamego.3 ed. Lisboa. Fundação Calouste Gulbenkian, 1997, p. 474.

LIMA, Cíntia Rosa Pereira de; BIONI, Bruno Ricardo. **A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo art. 7, incisos VIII e IX do Marco Civil da Internet a partir da human computer interaction e da privacy by default.** In: DE LUCCA, Newton; SIMÃO FILHO, A dalberto; LIMA, Cíntia Rosa Pereira de (COORD.). Direito e Internet III: marco civil da internet. São Paulo: Quartier Latin, 2015, t. I, p.263-290.

LISBOA, Roberto Senise. **Confiança contratual.** São Paulo: Atlas, 2012, p.151.

MACDONALD, Aleecia M.; CRANOR, Lorrie Faith. **The Cost of Reading Privacy Policies.** Journal of Law and Policy for Information Society, v.4, 2008, p. 565.

MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano Bruno Santos. **A proteção de dados da pessoa jurídica e a Lei 13.709/2018:** reflexões à luz dos direitos da personalidade. Scientia Juris, v. 23, n. 2, p.74-90, jul. 2019, p. 43.

MALGIERI, Gianclaudio. **The concept of Fairness in the GDPR:** a linguistic and contextual interpretation. Proceedings fo FAT, jan. 2020. Disponível em:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517264>. Acesso em 03 nov. 2022.

MANTOVANI, Alexandre Casanova. **O consentimento na disciplina da proteção dos dados pessoais:** uma análise dos seus fundamentos e elementos. Dissertação(Mestrado em Direito). Faculdade de Direito. Universidade Federal do Rio Grande do Sul. PORTO Alegre, 2019.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor:** o novo regime das relações contratuais. São Paulo. Revista dos Tribunais, 2011, p.74-75; 86-87.

MARQUES, Fernanda Mascarenhas. **Regulação do Fluxo de Dados Pessoais entre fronteiras: os contornos e limite da decisão de adequação de países terceiros.** São Paulo: FGV, 2020, p. 89.

MARTINS-COSTA, Judith. **A boa-fé no direito privado: critérios para a sua aplicação**. 2. ed. São Paulo: Saraiva, 2018.

MARTINS-COSTA, Judith. **Mercado e solidariedade social entre cosmos e taxis: a boa-fé nas relações de consumo**, p. 611/661. In MARTINS-COSTA, Judith (org.). *A Reconstrução do Direito Privado: reflexos dos princípios, diretrizes e direitos fundamentais constitucionais no direito privado*. São Paulo: Editora Revista dos Tribunais, 2002. p. 95-96.

MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideu: Fundação Konrad Adenauer, 2005, p. 233-245. Disponível em:
https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf. Acesso em: 16 jan. 2023.

MATTELART, Armand. **História da sociedade da informação**. São Paulo: Edições Loyola, 2022, p. 151.

MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Philip e.; ROTENBERG, Marc. *Technology and privacy: the new landscape*. CAMBRIDGE: The MIT Press, 2002, p. 219-242.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: a revolution that will transform how we live, work and think**. First Mariner Books: New York, 2014, p. 103.

MENDES, Laura Schertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais**. Portal Jota, 10 de maio de 2020. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020>>. Acesso em: 12 jan. 2023.

MENDES, Laura Schertel; DONEDA, Danilo. **Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016**. Revista de Direito Civil Contemporâneo, v.9, p.35-48, out-dez 2016.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. **Proteção de Dados Para Além do Consentimento**: tendências contemporâneas de materialização. REI – Revista Estudos Institucionais, Rio de Janeiro, v. 6, n. 2, p. 507-533, set. 2020. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/521>. Acesso em: 15 mai. 2021.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. São Paulo: Ed. RT, nov.-dez. Revista do Direito do Consumidor, vol. 120, ano 27, p. 469-483.

MENDES, Laura Schertel. **Transparência e Privacidade: violação e proteção da informação pessoal na sociedade de consumo**. Dissertação. Faculdade de Direito da Universidade de Brasília, 2008, p.81-85.

MENDES, Laura Schertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais**. Portal Jota, 10 de maio de 2020. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020>>. Acesso em: 12 jan. 2023.

MENEZES CORDEIRO, Antônio Manuel da Rocha. **Da boa-fé no direito civil**. Coimbra: Almedina, 2011, p.1242.

MENKE, Fabiano. **A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão**. In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P.(coord.). Direito, Inovação e Tecnologia. São Paulo: Saraiva, 2015, p. 205-230.

MENKE, Fabiano. **A interpretação das cláusulas gerais: a subsunção e a concreção dos conceitos.** Revista de Direito do Consumidor, v. 50, abr.-jun., 2004, p. 9-35.

MENKE, Fabiano. **A forma dos contratos eletrônicos.** Revista de Direito Civil Contemporâneo, v. 26, jan./mar. 2021, p. 85 – 113. Disponível em: <<https://menkeadvogados.com.br/wp-content/uploads/2022/05/A-FORMA-DOS-CONTRATOS-ELETRO%CC%82NICOS.pdf>>. Acesso em: 31 out. 2022.

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa.** In: MENKE, Fabiano; DRESCH, Rafael de Freitas VALLE(COORD.). Lei Geral de Proteção de Dados: aspectos relevantes. São Paulo: Editora Foco, 2021.

MESSINETTI, Davide. **Circolazioni dei dati personali e dispositivi di regolazioni dei poteri individuali.** Rivista Critica del Diritto Privato, 1998, p.339-407.

MIRANDA, Custódio da Piedade Ubaldino. **Contrato de Adesão.** São Paulo: Atlas, 2002, p.13-16.

MIRANDA, Lara Soares. **Relatório de Impacto à proteção de dados: um estudo comparado entre o direito brasileiro e o europeu.** Universidade Federal de Uberlândia.2021.<<https://repositorio.ufu.br/bitstream/123456789/33315/1/Relato%cc%81riolImpactoProtec%cc%a7a%cc%83o.pdf>>. Acesso em: 16 mai. 2023.

NISSENBAUM, Helen. **Privacy in context: technology, policy, and the integrity of social life.** Stanford: Stanford Law Books, 2010.

NOYB - **My Privacy is None of Your Business.** Disponível em: <<https://noyb.eu/en>> Acesso em: 07.11.22.

OECD. **Guidelines on the protection of privacy and transborder flows of personal data.** Disponível

em:<<https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1674741029&id=id&accname=guest&checksum=51F934C90C4174061CDC6B3E2B04B0F>>. Acesso em: 12 dez. 2022.

OECD. **Privacy Framework** 2013, p. 148. Disponível em:

<https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 25 jan. 2023.

OECD. **The evolving privacy landscape: 30 years after OECD privacy guidelines.** Disponível em:<<https://www.oecd-ilibrary.org/docserver/5kgf09z90c31-en.pdf?expires=1674760332&id=id&accname=guest&checksum=892CD98899BE6D73D686196FA92F5CDA>>.

Acesso em: 02 jan. 2023.

OLIVEIRA, Ricardo; COTS, Márcio (org.). **O legítimo interesse e a LGPD: Lei Geral de Proteção de DADOS Pessoais.** Revista dos Tribunais, 2ª ed., 2021, p. 63.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy.** New York: Crown, 2016(ebook), n.p.

OPICE BLUM. Princípios do Privacy by design. Disponível em:<<https://opiceblum.com.br/o-que-e-privacy-by-design-e-como-esta-inserido-na-lgpd/>>. Acesso em: 22 jan. 2023.

ORIENTAÇÕES relativas à transparência na aceção do Regulamento 2016/679.

Disponível:

<https://www.uc.pt/protecao-de-dados/suporte/20180411_orientacoes_relativas_a_transparencia_wp260_rev01> Acesso em: 12 abr. 20123.

PAIVA, Eduarda Beutinger. **A reversibilidade do processo de anonimização e as suas repercussões no regime de proteção de dados pessoais.** Universidade Federal do Rio Grande do Sul. Porto Alegre, 2021, p. 18.

PARLAMENTO EUROPEU. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>>. Acesso em: 24 jan. 2023.

RESTA, Giorgio. **Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali**. Rivista Critica del Diritto Privato. 2000, p. 307.

RODOTÀ, Stefano. **Elaboratori Elettronici e controllo sociale**. Bologna. Il Mulino, 1973, p. 341.

ROTH, Lucca Domingues. **Desenvolvimento Histórico da Transferência Internacional de Dados entre União Europeia e EUA**. Disponível em <<https://lume.ufrgs.br/handle/10183/227563>> Acesso em 08.11.2022.

RUARO, Regina L. **Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância?** Disponível em: <https://revistas.ufpr.br/direito/article/view/30768>. Acesso em: 22 de. 2022.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020.

SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: o direito fundamental à proteção de dados**. In: BIONI, Bruno et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 21-59.

SCHREIBER, Anderson. **Direitos da Personalidade**. São Paulo: Atlas, 2011, p. 21-22.

SECTION 702 OVERVIEW. Disponível em: <<https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf>>. Acesso em: 24 jan. 2023.

SCHWENKE, Mathias. **Individualisierung und Datenschutz**. Wiesbaden: Deutscher Universitäts-Verlag, 2006.

- SILVA, Daniel Pereira Militão. **Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação.** Dissertação(Mestrado)– Faculdade de Direito da PUCSP, 2009, p. 43.
- SIQUEIRA JR., Paulo Hamilton. **Teoria do Direito.** São Paulo: Saraiva, 2009, p. 218.
- SNOWDEN, Edward. **Referências bibliográficas.** Disponível em: <https://pt.wikipedia.org/wiki/Edward_Snowden>. Acesso em: 24 jan. 2023.
- SOLOVE, Daniel J. **A taxonomy of privacy.** University of Pennsylvania Law Review, v. 154, jan. 2006, p. 477-560, p. 519.
- SOLOVE, Daniel J. **Conceptualizing Privacy.** California Law Review, v. 90, 2002, p.1098-1156.
- SOLOVE, Daniel J. **Introduction: privacy self-management and the consent dilemma.** Harvard Law Review, v. 126, n. 7, nov, 2012, p. 1880-1903.
- SOLOVE, Daniel J. **”I’ve got nothing to hide” and other misunderstandings of privacy.** San Diego Law Review, n. 745, 2007.
- SOLOVE, Daniel J. **Privacy and Power: Computer Databases and Methafors for Information Privacy.** Standford Law Review, v.6, 2001. Disponível em:<https://heinonline.org/HOL/Page?collection=newyork&handle=hein.journals/stflr53&id=1411&men_tab=srchresults>. Acesso em: 15 jan. 2023.
- SOLOVE, Daniel J. **The myth of the privacy paradox.** The George Washington University Law School. **Public Law and Legal Theory Working Paper**, 2020-10. Disponível em: <https://papers.ssm.com/sol3/papers.cfm?abstract>.
- STRIPHAS, Ted. **Algorithmic Culture.** Bloomington: Sage Journals, 2015. Disponível em: <<http://journals.sagepub.com/doi/10.1177/1367549415577392>> Acesso em: 20 dez. 2022.

STURARI, Matheus. **O DPIA na LGPD: interpretação nacional ou banalização do instrumento?** Perfil do LinkedIn. Publicado em 29 de outubro de 2020. Disponível em: <https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-ou-banaliza%C3%A7%C3%A3o-do-matheus/> > Acesso em 13 mai. 2023.

TEIXEIRA, Lucas. **Teoricamente impossível: problemas com a anonimização de dados pessoais.** Disponível em: <<https://antivigilancia.org/pt/2015/05/animizacao-dados-pessoais/>>. Acesso em 04 fev. 2023.

TRIBUNAL CONSTITUCIONAL FEDERAL DA ALEMANHA. BverfG. **Decisão de 6 de novembro de 2019, nº 88.** Disponível em: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html >. Acesso em 16 jan. 2023.

TRIBUNAL DE CONTAS DA UNIÃO. **Relatório de impacto à proteção de dados.** Disponível: <https://portal.tcu.gov.br/data/files/FD/20/E4/CA/202128102DFE0FF7F18818A8/Relatorio%20de%20Impacto%20a%20Protecao%20de%20Dados%20Pessoais_web.pdf>. Acesso em: 15 mai. 2023.

UK Information Commissioner's Office. **Guide to the general data protection regulation (GDPR).** Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>>. Acesso em: 06 mar. 2023.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia.** Jornal Oficial da União Europeia, Bruxelas, 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em 16 out. 2023.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção dos dados singulares no que diz respeito**

ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://www.conjur.com.br/dl/diretiva-europeia.pdf>> Acesso em: 06 mar. 2023.

UNIÃO EUROPEIA. **Parecer n. 3, 2013**. Disponível

em:<https://www.gdp.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC03_2013%20%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_%E7%9B%AE%E7%9A%84%E9%99%90%E5%88%B6_PT.pdf>. Acesso em: 10 abr. 2023.

VAN DER SLOOT, Bart; BROEDERS, Dennis; SCHRIJVERS, Erik(org.). **Exploring the boundaries of Big Data**. Amsterdam: WWR, 2016, p.11.

VERMA, Shikha. **Weapons of mass destruction**: how big data increases inequality and threatens democracy. Book reviewer. New York: Crown, 2016(ebook), n.p.

Disponível

em<

https://appliedenergyscience.lbl.gov/sites/default/files/Weapons_of_Math_Destruction_How_Big_Data_Increases.pdf> Acesso em 18 dez. 2022.

VOSS, W. Gregory. **European Union Data Privacy Law Reform**: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. Disponível

em:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894571 > Acesso em 09.11.22.

WARREN, Samuel D; BRANDEIS, Louis D.The right to privacy. HARVARD Law Review, 1890, v. 4, Nº 5, Disponível

em:<https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html >. Acesso em:p. 193-220.

WILLIS, Lauren E. Why not privacy by default? Berkeley Technology Law School. Vol 29:61, 2014, p. 107. Disponível em:

https://btlj.org/data/articles2015/vol29/29_1/29-berkeley-tech-lj-0061-0134.pdf >.

Acesso em: 29 jan. 2023.

WORKING PARTY. Article 29 Data Protection Working Party. **Opinion 2/2010 on behavioural advertisement**. Brussels, 22 jun. 2010. Disponível

em:<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf>. Acesso em: 30 jan. 2023.

WORKING PARTY. Article 29. Data Protection Working Party. **Opinion 3/2013 on Purpose Limitation**. Brussels, 22 jun. 2010. Disponível

em:<https://www.gdpd.gov.mo/file/Documents%20of%20European%20Union/PT/%E7%AC%AC03_2013%20%E8%99%9F%E6%84%8F%E8%A6%8B%E6%9B%B8_%E7%9B%AE%E7%9A%84%E9%99%90%E5%88%B6_PT.pdf> Acesso em: 3 jan. 2013.

WORKING PARTY. Article 29. Data Protection Working Party. **Opinion 4/2007 on the concept of personal data**. Brussels, 20 jun. 2007. Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> Acesso em 04 jan. 2023.

WORKING PARTY. Article 29. Data Protection Working Party. **Opinion 6/2014 on the notion of legitimate interests of the data controller**. Brussels, 9 apr. 2014. Disponível:<<https://www.fia.org/sites/default/files/2019-11/Excerpts%20-%20Opinion%2006-2014%20on%20the%20notion%20of%20legitimate%20interests%20of%20the%20....pdf>>. Acesso em: 05 jan. 2023.

WORKING PARTY. Article 29 Data Protection Working Party. **The future of privacy**: joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Disponível em:< https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf >Acesso em 06 fev 2023.