



CENTRO UNIVERSITÁRIO DE BRASÍLIA – UNICEUB

**PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITO DO
CENTRO UNIVERSITÁRIO DE BRASÍLIA (PPGD) - MESTRADO**

VICTOR BENIGNO PORTO

**O SENTIDO E ALCANCE DO LEGÍTIMO INTERESSE NA LEI GERAL DE
PROTEÇÃO DE DADOS**

Brasília

2022

VICTOR BENIGNO PORTO

**O SENTIDO E ALCANCE DO LEGÍTIMO INTERESSE NA LEI GERAL DE
PROTEÇÃO DE DADOS**

Dissertação apresentada como requisito
para conclusão do curso de Mestrado do
Programa de Pós-Graduação *Stricto
Sensu* em Direito do Centro Universitário
de Brasília – UniCEUB. Orientador: Prof.
Dr. Leonardo Roscoe Bessa

BRASÍLIA

2022

VICTOR BENIGNO PORTO

**O SENTIDO E ALCANCE DO LEGÍTIMO INTERESSE NA LEI GERAL DE
PROTEÇÃO DE DADOS**

Dissertação apresentada como requisito
para conclusão do curso de Mestrado do
Programa de Pós-Graduação *Stricto
Sensu* em Direito do Centro Universitário
de Brasília – UniCEUB. Orientador: Prof.
Dr. Leonardo Roscoe Bessa

Brasília, 15 de fevereiro de 2022

BANCA EXAMINADORA

Prof. Dr. Leonardo Roscoe Bessa

Orientador

Prof. Dr. Gustavo Ferreira Ribeiro

Membro interno

Profa. Dra. Milena Donato Oliva

Membra Externa

À minha esposa e à minha
filha, que materializam o que
há de bom em mim;
Aos meus irmãos;
Aos meus pais.

AGRADECIMENTOS

A Deus.

Ao Professor Doutor Leonardo Roscoe Bessa por sua generosidade, especialmente em ter aceitado ser meu orientador, pelo compromisso com a excelência, por apontar os caminhos que deveriam ser seguidos, pelas constantes reflexões imprescindíveis à conclusão do trabalho, pelas correções e incentivos sempre que necessários, por me defender nos momentos em que precisei, pela oportunidade de aprender não só sobre o objeto de estudo, mas, sobretudo, a ser um ser humano melhor.

Ao Centro Universitário de Brasília pelo excelente corpo acadêmico e administrativo, especialmente a Marley, Alessandra e Fernando, pessoas fantásticas com quem tive o prazer de conviver durante os últimos dois anos.

Aos Professores Doutores Gustavo Ribeiro e Diógenes Carvalho pelas observações no momento da qualificação, as quais foram essenciais para a elaboração do texto final.

À Professora Milena Donato

Ao amigo Aldo que acompanhou e apoiou essa jornada de perto.

Aos meus irmãos Ciro e Lara por jamais deixarem de torcer e estar ao meu lado, pelas críticas construtivas e estímulo constantes. São as pontes que tenho com as boas lembranças do passado e estão entre os pilares que me dão força para encarar o presente e não temer o futuro.

À minha filha Ana Emília por todo dia me ensinar de onde retirar energia para seguir em frente e a compreender um pouco mais sobre o que é o amor.

À minha esposa Emiliana por seu amor, sua paciência e seu apoio incondicional em todos os momentos. Pela dedicação à nossa família, por proporcionar um ambiente no qual eu pudesse me dedicar aos estudos, pelas oportunidades de amadurecer em meio às profícuas discussões jurídicas, por me desafiar a ser alguém melhor sem deixar de me amar por ser quem sou. Enfim, por ser minha companheira de vida. Obrigado!

RESUMO

As constantes alterações nas relações entre seres humanos, novas tecnologias e novos modelos de negócios têm despertado muitas discussões sobre a amplitude do direito à privacidade e a possibilidade de utilização de informações referentes aos indivíduos por governos e entidades privadas. No Brasil, a Lei Geral de Proteção de Dados (LGPD) somente permite o processamento desses elementos de informação mediante a adoção pelo interessado de uma das bases legais de tratamento previstas em lei. O legítimo interesse é um dos fundamentos de licitude para o processamento de dados pessoais admitidos pelo legislador e guarda a peculiaridade de prescindir do consentimento do titular dos dados para ser utilizado. Contudo, se cuida de hipótese de tratamento permeada por conceitos abertos e, portanto, sujeita a elevado grau de subjetividade do intérprete da norma. Neste trabalho se examina o tratamento jurídico conferido ao legítimo interesse enquanto hipótese legal de tratamento de dados pessoais e se desenvolve a hipótese de que é possível, a partir da LGPD, operacionalizar, no plano fático, o processamento desses dados com fundamento nessa hipótese normativa, de modo que a imprecisão conceitual da lei não inviabiliza a compreensão dos sentido e alcance dessa base legal. O trabalho apresenta abordagem teórica e, por meio de pesquisa bibliográfica e documental, se busca demonstrar, a partir da concepção da proteção de dados como direito fundamental, que o legítimo interesse é hipótese de tratamento de dados pessoais baseada no risco da atividade e tão relevante quanto as demais, bem como que a sua funcionalização dentro das balizas normativas estabelecidas, em especial quanto ao teste de balanceamento, não se consubstancia em flexibilização do paradigma do consentimento ou de fragilização da privacidade, recaindo sobre o agente de tratamento os ônus decorrentes de eventual conduta em desacordo com o preconizado pela legislação. O tema é importante para os novos tempos e ajustes legais necessários em razão da disrupção ocasionada pela coleta e processamento permanente de dados pessoais e da opacidade desse processo nas atividades desenvolvidas pelos agentes de tratamento.

Palavras-Chaves: proteção de dados, privacidade, legítimo interesse.

ABSTRACT

The constant changes on the relationships between human beings, modern technologies and new business models have sparked many discussions about the extent of the right to privacy and the possibility of using information regarding individuals by governments and private corporations. In Brazil, the General Law of Data Protection (LGPD) only allows the processing of these pieces of information upon the adoption by the interested party of one of the legal grounds for processing provided by law. Legitimate interest is one of the legal grounds for processing personal data admitted by the legislator and has the peculiarity of not requiring the consent of the data subject to be used. However, this is a processing hypothesis permeated by open concepts and, therefore, subject to a high degree of subjectivity by the interpreter of the law. This work examines the legal treatment given to legitimate interest as a legal hypothesis for the processing of personal data and develops the hypothesis that it is possible, starting from the LGPD, to operationalize, on a factual level, the processing of these data based on this normative hypothesis, so that the conceptual imprecision of the law does not make it unfeasible to understand the meaning and scope of this legal basis. The work presents a theoretical approach and, by means of bibliographical and documental research, attempts to demonstrate, based on the conception of data protection as a fundamental right, that the legitimate interest is a hypothesis for the processing of personal data based on the risk of the activity and as relevant as the others, as well as that its adoption within the established normative limits, especially regarding to the balancing test, does not consist in flexibilization of the paradigm of consent or weakening of privacy, the burden resulting from eventual conduct in disagreement with that recommended by the legislation falling upon the agent of processing. The theme is important for the recent times and necessary legal adjustments due to the disruption caused by the permanent collection and processing of personal data and the opacity of this process in the activities developed by the processing agents.

Keywords: data protection, privacy, legitimate interest.

SUMÁRIO

INTRODUÇÃO.....	10
CAPÍTULO 1 - PANORAMA HISTÓRICO DA PROTEÇÃO DE DADOS: mudanças sociais, privacidade, dados pessoais e a tendência global de regulamentação	13
1.1. A proteção de dados como um direito fundamental	20
1.1.1. A algoritmização do direito	25
1.1.2. O valor patrimonial dos dados.....	30
1.1.3. O reconhecimento de um direito fundamental	41
1.2. As gerações de leis de proteção de dados.....	57
1.3. A Lei Geral de Proteção de Dados e o paradigma do consentimento	61
1.3.1. A possibilidade de reconhecimento do microsistema de proteção de dados	65
1.3.2. O tratamento com base no paradigma do consentimento e a condição de vulnerável do titular de dados	67
1.3.3. A tutela da privacidade desde a concepção (por padrão) como variante das tecnologias promotoras do direito fundamental à proteção de dados.....	74
CAPÍTULO 2 – O LEGÍTIMO INTERESSE ENQUANTO BASE LEGAL APLICÁVEL PELOS AGENTES DE TRATAMENTO DE ACORDO COM A LGPD	81
2.1. O legítimo interesse no GDPR	81
2.2. O legítimo interesse na LGPD.....	84
2.3. Legítimo interesse: sentido e alcance	86
2.3.1. O legítimo interesse enquanto fundamento de licitude para o processamento de dados pelos agentes de tratamento	92
2.3.2. O legítimo interesse enquanto elemento irradiador de deveres.....	98
2.3.2.1. Dever geral de fundamentação do tratamento	99
2.3.2.2. Dever de uso da base legal legítimo interesse atrelado a finalidades legítimas consideradas a partir de situações concretas.....	100
2.3.2.3. Dever de respeito às legítimas expectativas (boa-fé) e direitos fundamentais dos titulares.....	102
2.3.2.4. Dever de uso dos dados estritamente necessários à finalidade pretendida....	107
2.3.2.5. Dever de transparência	109
2.3.2.6. Dever de documentação da atividade de tratamento	111

2.3.3. A impossibilidade tratamento de dados pessoais sensíveis com base no legítimo interesse à luz do art. 11 da LGPD	114
2.3.4. Sobre a portabilidade dos dados coletados e tratados com base no legítimo interesse	119
2.4. O Parecer 6/2014 do Grupo de Trabalho para o Artigo 29, sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados conforme o artigo 7º da Diretiva 95/46/CE: um norte interpretativo para a implementação da LGPD	122
2.5. O teste de balanceamento	127
CAPÍTULO 3 – SITUAÇÕES HIPOTÉTICAS: compreendendo a dinâmica da base legal legítimo interesse	137
3.1. Estabelecimento comercial que envia publicidade dirigida aos seus clientes sobre produtos análogos aos já adquiridos com base no histórico de consumo.....	137
3.2. Coleta de documento nacional de identificação por drogarias e formação de perfis para ofertas de produtos e “descontos exclusivos” com base nos hábitos de consumo do titular de dados/ Utilização do histórico de consumo para aprimoramento logístico	138
3.3 Assistente pessoal por voz.....	140
3.4 Operações societárias	142
3.5. Empresa que pretende contratar colaboradores e terceiriza serviço de verificação da vida pregressa dos candidatos à vaga de trabalho.	143
3.6. Utilização de sistemas de vigilância para identificar fumantes em determinado estabelecimento	145
3.7. Atividade de monitoramento, detecção e prevenção de fraudes em redes de pagamento	146
3.8. Promoção da segurança dos usuários de redes sociais que encorajam encontros presenciais ou permitem o compartilhamento de eventos reais dos utilizadores	147
3.9. O lucro como legítimo interesse	148
CONCLUSÃO.....	152
REFERÊNCIAS	161

INTRODUÇÃO

As mudanças sociais têm como um de seus desdobramentos o incessante fluxo de informações a respeito dos indivíduos. Atualmente, qualquer elemento de informação é passível de digitalização e, nesse contexto, os agentes de tratamento devem atuar em consonância com a legislação, principalmente a partir do reconhecimento do direito fundamental à proteção de dados pessoais.

Nesse trilhar, se destaca a força conformadora dos fatos sobre o direito e a necessidade de se enfrentar a matéria sob o prisma jurídico. Desta sorte, o processamento de dados pessoais deve ocorrer dentro de balizas normativas que confirmam segurança jurídica tanto aos agentes de tratamento quanto aos titulares de dados, sem se perder de vista a posição de centralidade do indivíduo no ordenamento jurídico a partir do postulado da dignidade da pessoa humana.

A Lei Geral de Proteção de Dados (LGPD) somente permite o processamento dessas informações mediante a adoção pelo interessado de uma das bases legais de tratamento, sendo o legítimo interesse uma delas.

Contudo, se cuida de fundamento de licitude para o tratamento de dados permeado por conceitos imprecisos e, portanto, sujeito a elevado grau de subjetividade do intérprete da norma. Trata-se de base legal dissociada do consentimento e se discute se sua adoção se consubstancia em flexibilização desse paradigma ou sua densificação.

Neste trabalho, se desenvolve a hipótese de que esse diploma legislativo trouxe disposições normativas suficientes para definir o sentido e alcance do legítimo interesse como fundamento para o tratamento de dados pessoais, de sorte que a imprecisão conceitual advinda da regulação prevista nos arts. 7º, IX, e 10 da Lei 13.709/2018¹, embora presente, não impossibilita sua aplicação.

A partir do embasamento teórico construído em torno do conceito de dados pessoais e da necessidade de sua proteção, examinam-se algumas repercussões da LGPD sobre o direito à privacidade, em especial no que concerne à possibilidade de tratamento de dados sem o consentimento do titular com fundamento no legítimo interesse.

Analisa-se a natureza jurídica dos dados pessoais, abordando-se suas características específicas e a proximidade com a dignidade da pessoa humana com o objetivo de contribuir

¹ Brasil. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de dados. Brasília, DF. Diário Oficial da União - Edição extra de 15 ago. 2018.

para a ciência do direito ao se analisar se sua proteção se consubstancia em uma categoria autônoma de direitos fundamentais.

Outrossim, além de se perquirir sobre a ausência de hierarquia entre as bases legais para o tratamento de dados e a dificuldade de obtenção do consentimento para toda e qualquer hipótese de processamento desses elementos de informação, visa-se, também, a investigar e apontar formas de operacionalização do tratamento de dados pessoais com base no legítimo interesse e o respectivo teste de balanceamento como mecanismo preventivo da prática de ilícitos e indutor do adequado desenvolvimento dessa atividade pelos agentes de tratamento à luz da sua evolução como fundamento de licitude para o processamento de dados

Aborda-se, ademais, a consonância da regulação legislativa desse instituto do direito positivo nacional com o Regulamento Geral sobre Proteção de Dados (GDPR²), vigente na Europa, o qual referenciou a introdução do instituto no Brasil.

Sob prisma metodológico, optou-se por abordagem teórica. Por meio de pesquisa exploratória bibliográfica e documental, se aprofundam assuntos enfrentados pela doutrina nacional e estrangeira sobre a tutela dos dados pessoais, com foco na sua natureza jurídica, bem como sobre a atuação dos agentes econômicos que tratam esses dados com base no legítimo interesse.

É realizado, ainda, estudo das disposições normativas relativas ao tema constantes da LGPD e do GDPR, com enfoque na correta dimensão do legítimo interesse enquanto fundamento para o tratamento de dados pessoais nas realidades jurídicas brasileira e europeia.

Embora de complexa funcionalização, a previsão normativa do tratamento de dados com base no legítimo interesse não fragiliza o consentimento e é suficiente para se garantir sua utilização pelos agentes de tratamento interessados e a efetiva tutela dos direitos e liberdades dos titulares de dados.

O trabalho se subdivide em três capítulos. No primeiro, se contextualiza o tratamento de dados pessoais a partir de sua correlação com o direito à privacidade e se reconhece a tendência de regulação do tema em âmbito global, assim como se traça panorama histórico da proteção de dados, se aponta sua peculiaridade de bem revestido de relevância econômica e se aborda seu reconhecimento como direito autônomo, de cariz constitucional. Ainda, se enfrenta

² Sigla em inglês para General Data Protection Regulation, Regulamento 2016/679 do Parlamento Europeu e do Conselho (União Europeia), de 27 de abril de 2016, relativo à proteção das pessoas naturais no que concerne ao tratamento de dados pessoais e à sua livre circulação, bem como revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

o paradigma do consentimento para o tratamento de dados pessoais à luz da complexidade das relações interpessoais, vislumbrando-se outras bases legais para o desenvolvimento dessa atividade igualmente suficientes do ponto de vista jurídico, das quais se destaca o legítimo interesse. No segundo, se aborda o legítimo interesse e o tratamento jurídico que lhe é conferido nos âmbitos europeu e nacional. Busca-se delinear esse conceito jurídico partindo-se de análise histórica, de pesquisa sobre a base doutrinária em torno desse instituto e do regime jurídico aplicável. Examina-se o teste de balanceamento como o anteparo sobre o qual se desvela o liame lógico-jurídico que deve existir entre a materialização do interesse legítimo do agente de tratamento e o efetivo processamento dos dados pessoais. No terceiro capítulo, se busca analisar o aspecto dinâmico da opção pelo legítimo interesse pelo agente de tratamento e, por meio da referência a casos hipotéticos, se trata sobre a materialização do teste de balanceamento.

CAPÍTULO 1 - PANORAMA HISTÓRICO DA PROTEÇÃO DE DADOS: mudanças sociais, privacidade, dados pessoais e a tendência global de regulamentação

A velocidade das transformações proporcionadas pelos avanços tecnológicos impõe inúmeros desafios a serem enfrentados pelo direito. A sociedade está diante de novas formas de produção, de disseminação e de consumo de conteúdos com relevância jurídica e a existência de um fluxo maior de informações não necessariamente está atrelada à melhora na equivalência das relações sociais.

Atualmente, textos, fotos e diversas formas de manifestação em meio físico podem ser digitalizados. Praticamente qualquer coisa pode assumir a forma digital, de sorte que se pode falar, inclusive, em plasticidade das informações digitalizadas³.

O sentimento de privacidade, proporcionado pelo acesso à internet a partir de dispositivos individuais e de locais onde as pessoas tendem a ser menos inibidas, como a própria casa, não reflete a realidade dos dias atuais⁴.

Deve-se destacar, também, que a dinâmica das interações interpessoais tem por base a troca de informações entre os agentes que buscam estabelecer uma relação entre si. E, modernamente, o fluxo informacional tem se revelado de maneira intensa, principalmente a partir da expansão do comércio eletrônico, do uso de redes sociais, *blogs*, além de uma miríade de possibilidades, tais como a cognominada internet das coisas - *internet of things* (IoT)- e a inteligência artificial - *artificial intelligence* (AI)-, essa última cada vez mais presente nos processos de trabalho e de tomada de decisão de indivíduos, entidades privadas e governos⁵.

Um dos desdobramentos da vida moderna, na qual o manejo de dispositivos eletrônicos se tornou algo cotidiano, é a monetização⁶ dos dados pessoais. O direito, enquanto fenômeno

³ HILGENDORF, Eric; FELDLER, Jochen, **Digitalization and the Law**, Baden-Baden: Nomos, 2018.

⁴ A título de exemplo, sobre o assunto, vale mencionar a observação de Véliz: “[t]udo o que você faz enquanto está no Facebook é rastreado, desde os movimentos do seu mouse até as coisas que você escreve e decide apagar antes de publicar (sua autocensura)”. In: VÉLIZ, Carissa, **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**, São Paulo: Contracorrente, 2021, p. 33.

⁵ Schwab destaca que a “inteligência artificial (IA) está em nosso entorno, em carros que pilotam sozinhos, drones, assistentes virtuais e softwares de tradução. Isso está transformando nossas vidas. A IA fez progressos impressionantes, impulsionada pelo aumento exponencial da capacidade de processamento e pela disponibilidade de grandes quantidades de dados, desde softwares usados para descobrir novos medicamentos até algoritmos que preveem nossos interesses culturais. Muitos desses algoritmos aprendem a partir das “migalhas” de dados que deixamos no mundo digital. Isso resulta em novos tipos de “aprendizagem automática” e detecção automatizada que possibilitam robôs ‘inteligentes’ e computadores a se autoprogamarem e encontrar as melhores soluções a partir de princípios iniciais”. In: SCHWAB, Klaus, **A quarta Revolução Industrial [livro eletrônico]**, São Paulo: Edipro, 2016, p. 22.

⁶ TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca, **Lei Geral de Proteção de Dados Pessoais comentada artigo por artigo**, Salvador: Juspodivm, 2019.

social, deve, também, acompanhar essa evolução das relações interpessoais e se apresentar como instrumento hábil a permitir a identificação e tutela dos novos anseios dos indivíduos, bem como a conformar a sociedade ao estabelecer parâmetros objetivos para os comportamentos dos atores sociais.

Outro aspecto importante e correlacionado ao tema é a "reestruturação das relações sociais e políticas"⁷⁻⁸. Alguns estudiosos fazem referência ao chamado capitalismo de vigilância⁹, no qual a violação da privacidade surge como um negócio e se atribui relevância econômica à informação obtida a partir do dado tratado.

Nesse contexto, exsurtem novas tecnologias, as quais promovem o movimento incessante de elementos de informação a respeito dos indivíduos e trazem consigo ferramentas de classificação e perfilização dos sujeitos¹⁰, de sorte não se pode falar em dados irrelevantes. Pois, embora em um primeiro momento não se relacionem diretamente a alguém, uma vez correlacionados dentro de uma análise contextual, podem-se extrair diversas informações, não raro consideradas sensíveis¹¹, porquanto relacionadas à posição dos titulares desses dados na estrutura social na qual se encontram inseridos¹².

Ao lado dos mecanismos de processamento de informações está a coleta de dados. Quanto maior a importância conferida aos dados pessoais, maior será o estímulo à vigilância, principalmente se considerada sua realização de forma massiva e ubíqua, de modo que é possível antever uma relação de retroalimentação entre coleta e tratamento de dados. Para Ana Frazão¹³:

⁷ FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados, *in*: **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro [livro eletrônico]**, São Paulo: Revista dos Tribunais, 2019.

⁸ Para maior aprofundamento, ver: SCHWAB, **A quarta Revolução Industrial [livro eletrônico]**.

⁹ ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**, Nova Iorque: PublicAffairs, 2018.

¹⁰ RODOTÀ, Stefano, **A vida na sociedade da vigilância: a privacidade hoje**, Rio de Janeiro: Renovar, 2008, p. 14.

¹¹ De acordo com a LGPD, dado pessoal sensível é o “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (art. 5º, II). *In*: BRASIL. **Lei 13.709/18, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 15 jun. 2021.

¹² TEFFÉ, Chiara Spadaccini de; VIOLA, Mario, Tratamento de dados pessoais na LGPD: estudo sobre as bases legais, **civilistica.com**, v. 9, n. 1, p. 1–38, 2020, p. 131.

¹³ FRAZÃO, Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro [livro eletrônico]**, São Paulo: Revista dos Tribunais, 2019

(...) se os dados são os insumos e os *inputs* da economia digital, os algoritmos são os instrumentos por meio dos quais os dados são processados e podem ser revertidos em resultados (*outputs*) a serem utilizados para as mais diversas finalidades. Muito além de aperfeiçoar estratégias econômicas já existentes, como seriam os casos do marketing personalizado (*target marketing*) e das classificações ou perfilizações (*profiling*), tais aplicações podem levar à total modificação do cenário econômico, político e social.

Assim, é possível se compreender que um dos aspectos mais sensíveis relacionados à proteção de dados é a capacidade que os sistemas informatizados detêm de correlacionarem informações dispersas e organizá-las.

O processamento de dados é uma realidade que permeia várias atividades das pessoas e a utilização desses fragmentos de informação por agentes políticos e econômicos acontece de forma cada vez mais vigorosa¹⁴.

Esse fenômeno, ao lado do desenvolvimento de avançadas tecnologias, representa desafio ao livre desenvolvimento da personalidade dos indivíduos e, nesse contexto, a proteção de dados ganha peculiar relevância¹⁵ e é inequívoca a necessidade de adequada regulamentação do tema.

A tutela jurídica da proteção de dados tem origem no artigo de autoria de Samuel D. Warren e Louis D. Brandeis intitulado *The right to privacy*¹⁶, no qual os autores, com o objetivo de limitar notícias veiculadas pela imprensa americana, construíram, com base em regras e precedentes do sistema *civil law*, a ideia de que o direito à privacidade comportaria o direito de ser deixado em paz.

Assim, pelo menos desde 1890, o conteúdo da privacidade tem amadurecido e ganhado contornos que lhe permitem servir de fundamento para a contenção de comportamentos abusivos relacionados ao tratamento de informações concernentes aos indivíduos praticados nos âmbitos privado e público.

¹⁴ “Governos e centenas de empresas estão espionando você e eu, e todos que conhecemos. A cada minuto de cada dia. Eles rastreiam e registram tudo o que podem: nossa localização, nossas conversas, nossas buscas na internet, nossas informações biométricas, nossas relações sociais, nossas compras e muito mais. Eles querem saber quem nós somos, o que pensamos, o que nos machuca. Eles querem prever e influenciar nosso comportamento”. In: VÉLIZ, **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**, p. 19.

¹⁵ “Em razão de modificações sociais e da evolução tecnológica, a discussão sobre os danos causados pelo processamento e fluxo de dados na sociedade não se restringe mais à ameaça do enorme poder do Estado, expresso na figura do Big Brother de Orwell, mas abrange hoje, também, o setor privado, que utiliza massivamente dados pessoais para atingir os seus objetivos econômicos. Assim, a ameaça passa a ser representada pelos ‘pequenos irmãos’ (BUCHNER, 2006, p. 26), isto é, pelas milhares de empresas que coletam, armazenam e processam dados de seus clientes, consumidores finais ou não”. MENDES, Laura Schertel. O direito Fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 20, n. 79, 2011. p. 47.

¹⁶ WARREN, Samuel D.; BRANDEIS, Louis D., *The Right to Privacy*, **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

Para James Michael, o direito à privacidade seria, talvez, o direito humano fundamental mais difícil de se conceituar¹⁷. Alan Westin considera que a privacidade é a “pretensão de indivíduos, grupos ou instituições, de determinar quando, como e em qual extensão informações a seu respeito são comunicadas a outros”¹⁸. Segundo Véliz¹⁹:

A privacidade diz respeito à capacidade de manter certas coisas íntimas para si mesmo — seus pensamentos, suas experiências, suas conversas, seus planos. O ser humano precisa de privacidade para se desprender do fardo de estar com outras pessoas. Precisamos de privacidade para explorar livremente novas ideias, para tomarmos nossas próprias decisões. A privacidade nos protege de pressões indesejadas e abusos de poder. Precisamos dela para sermos indivíduos autônomos, e, para que as democracias funcionem bem, precisamos de cidadãos autônomos.

Não se pode negar a carga dinâmica da atual compreensão da privacidade. A concepção clássica – direito de ser deixado só –, cujo pressuposto seria o reconhecimento de aspecto negativo, garantindo-se aos indivíduos um espaço restrito inviolável por terceiros e, dentre eles o Estado, evoluiu para reconhecer, também, a dimensão positiva da privacidade, consubstanciada na possibilidade de controle pelos indivíduos sobre as próprias informações²⁰.

A proteção de dados pessoais é produto do desenvolvimento do conceito de privacidade e, de acordo com a realidade jurídico-política de cada Estado, serve à tutela de diferentes bens caros ao convívio em sociedade²¹.

Nesse diapasão, as atuais bases da defesa da privacidade partem do abandono da lógica patrimonialista, aproximando-a do aspecto existencial das pessoas, e integram em sua estrutura instrumentos de controle individuais e coletivos²².

Assim, é preciso se reconhecer, dentro da tábua de valores dos modernos ordenamentos jurídicos, o direito fundamental à proteção de dados como garantia do pleno desenvolvimento da personalidade e, *a fortiori*, como garantia da liberdade individual e da democracia²³.

No caso brasileiro, em maio de 2020, o Plenário do Supremo Tribunal Federal, ao referendar a Medida Cautelar nas Ações Diretas de Inconstitucionalidade n.ºs 6.387, 6.388, 6.389, 6.393, 6.390, suspendendo a aplicação da Medida Provisória 954 de 17 de abril de 2020,

¹⁷ MICHAEL, James, **Privacy and Human Rights**, Londres: Dartmouth Publishing Company, 1994, p. 1.

¹⁸ WESTIN, Alan F, **Privacy And Freedom**, Nova Iorque: Atheneum, 1967, p. 7, livre tradução.

¹⁹ VÉLIZ, **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**, p. 21.

²⁰ BESSA, Leonardo Roscoe, **O consumidor e os limites dos bancos de dados de proteção ao crédito**, São Paulo: Revista dos Tribunais, 2003, p. 92.

²¹ À guisa de exemplo, no caso do Brasil, a proteção de dados protege bens jurídicos relevantes para o direito penal (buscas e apreensões, interceptações telefônicas) e, também, para o direito civil (coleta e compartilhamento de dados relacionados a consumidores).

²² RODOTÁ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 50.

²³ *Ibid.*, p. 58.

a qual obrigava as operadoras de telefonia a repassarem ao Instituto Brasileiro de Geografia e Estatística (IBGE) dados identificados de seus consumidores de telefonia móvel, celular e endereço, reconheceu a proteção de dados pessoais como um direito fundamental autônomo²⁴.

Um efeito importante produzido por essa decisão é o reforço da discussão da proteção de dados em âmbito nacional, evidenciando a sensibilidade dos poderes constituídos ao tema em discussão e a necessidade de se fortalecer a moldura institucional da proteção de dados.

A matéria ocupa posição destacada nas discussões jurídicas hodiernas, principalmente por estar atrelada ao exercício das liberdades individuais, as quais, em um ambiente democrático, devem ser sempre resguardadas.

Calha destacar, também, que proteção de dados é objeto de atenção em escala global e sua incorporação aos diversos sistemas jurídicos parece ser inevitável, a exemplo do que vem ocorrendo em países como Noruega, Islândia, Lichtenstein, Japão, Austrália e Índia²⁵.

Dentro da literatura específica relativa ao assunto, podem ser identificados dois modelos de proteção de dados pessoais: o estadunidense e o europeu. Para Leonardo Bessa²⁶:

Em síntese, nos Estados Unidos, a proteção da privacidade em relação aos dados pessoais é fragmentada, representada por leis setoriais. Ademais, inexistente uma autoridade governamental específica para controle e fiscalização das empresas que realizam o tratamento de informações. Outra característica é a separação entre setor público e privado.

Na Europa, a disciplina do tema é mais sistemática, estruturando-se atualmente em torno do regulamento 679 que, em maio de 2018, revogou a Diretiva 95/46. O regulamento, na mesma linha da Diretiva revogada, disciplina praticamente toda forma – governamental e privada – de tratamento de dados, inclusive os relativos à proteção de crédito.

²⁴ “[F]oi a primeira vez que o STF reconheceu expressamente um direito fundamental à proteção de dados pessoais diretamente extraível da Constituição e que demandaria prestações positivas por parte do Estado”. In: ZANATTA, Rafael Augusto *et al.* Os Dados e o Vírus. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 14, n. 1, p. 231–256, 2020, p. 246.

²⁵ “Further, it is clear that the emphasis on data privacy is being embraced around the globe. Jurisdictions around the world are enacting legislation to conform to the EU’s GDPR, due both to the law’s extraterritorial application and the other countries’ recognition of the importance of data privacy. In addition to the EU Member States, the EFTA countries— Iceland, Lichtenstein, and Norway—have all agreed to adopt the GDPR. Also, many Asian countries have been adapting to the GDPR. For example, the EU announced a safe harbor agreement with Japan, indicating that the EU approved of Japan’s data protection laws. India has been working to bring itself closer to compliance with the GDPR’s level of data protection. A small number of Middle Eastern Companies have proposed GDPR-like data privacy laws, with Israel offering its citizens the most advanced protection in the region. Australia and New Zealand have advanced data privacy laws and Australia is updating its laws to comply with the GDPR. In South America, Argentina and Uruguay are the countries that are closest to compliance with the GDPR. Moreover, other countries have adopted their own independent data security laws, some of which predate the GDPR, like South Africa’s Protection of Personal Information Act of 2013, which includes a number of similarities to the GDPR. The GDPR is developing into ‘the transnational gold standard of data protection’ (...).” In: KESSLER, Joanna, Data protection in the wake of the GDPR: California’s solution for protecting “the world’s most valuable resource”, **Southern California Law Review**, v. 93, p. 31, 2019.

²⁶ BESSA, Leonardo Roscoe, **Nova Lei do Cadastro Positivo: comentários à Lei 12.414, com as alterações da Lei Complementar 166/2019 e de acordo com a LGPD**, São Paulo: Thomson Reuters Brasil, 2019, p. 54.

(...)

Apesar das diferenças estruturais, é possível identificar parâmetros de consenso na definição de alguns direitos e limites no tratamento de dados pessoais. Ambos os modelos estabelecem o direito de acesso às informações pessoais, a possibilidade de se exigir retificação dos dados inexatos, a ideia de que os dados devem ser colhidos e utilizados para finalidades legítimas e previamente identificadas, a exigência de que os dados devem ser verdadeiros, atualizados objetivos, relevantes e não excessivos.

Infere-se, portanto, que no sistema norte-americano, a regulamentação do tema é dispersa, por meio de leis setoriais, bem como inexistente autoridade governamental específica para fiscalização e controle dos atores sociais que realizam o tratamento de informações.

De outro lado, o modelo europeu apresenta concentração normativa, um único diploma para regular os aspectos centrais das relações privadas e públicas, e consagra a existência de autoridade autônoma de controle com poderes de fiscalização e de aplicação de sanções de forma independente.

Não se pode falar, contudo, que são sistemas antagônicos. Vale destacar, por oportuno, certos pontos de convergência, a exemplo do reconhecimento do direito de acesso aos dados pessoais, da possibilidade de retificação de dados inexatos, da ideia de que os dados devem ser colhidos e utilizados para finalidades legítimas e previamente identificadas, da exigência de que devem ser verdadeiros, atualizados, objetivos e não excessivos, e da fixação de limites temporais para o seu uso.

O sistema brasileiro se alinha mais ao modelo europeu. Nesse sentido, Bessa aponta que o Brasil “com a recente edição da Lei 13.709, em agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), inspira-se claramente no modelo europeu de proteção de dados pessoais”²⁷.

É oportuno registrar, ainda, que o tema da proteção de dados não é novidade no Brasil. A matéria já foi objeto de positivação em diversas normas, tanto em âmbito constitucional quanto infraconstitucional, como por exemplo a Constituição Federal (art. 5º, X, XI, XII, LV e IX), o Código Civil (arts. 20 e 21), o Código de Processo Penal (arts. 13-A, 13-B e 201, § 6º), o Marco Civil da Internet (Lei 12.965/14, arts. 3º, II, 7º, I, 8º, 21 e 23), o Código de Defesa do Consumidor (art. 43 e seguintes), a Lei do Cadastro Positivo (Lei 12.414/11, alterada pela Lei Complementar 166/2019) e, atualmente, a Lei Geral de Proteção de Dados (LGPD), Lei 13.709 de 14 de agosto de 2018.

²⁷ *Ibid.*, p. 60–61.

O consentimento é comumente apontado como a pedra angular do tratamento dos dados das pessoas. Contudo, o indivíduo, usualmente, não possui condições de analisar holisticamente as consequências do ato de disposição de informações a seu respeito a um determinado agente, ou, nos termos do artigo 5º, VI, da LGPD, ao controlador, o que lhe confere a condição de sujeito vulnerável, e, portanto, carente de tutela especial do Estado.

Todavia, não se cuida da única hipótese possível para o tratamento de dados. De acordo com a LGPD (art. 7º), são dez as hipóteses legais nas quais se pode realizar o tratamento de dados pessoais: i) consentimento; ii) cumprimento de obrigação legal ou regulatória pelo controlador; iii) execução de políticas públicas pela Administração pública; iv) estudos realizados por órgão de pesquisa; v) execução contratual ou procedimentos preliminares relacionados ao contrato; vi) exercício regular de direito em processo judicial, administrativo ou arbitral; vii) proteção da vida ou da incolumidade física do titular ou de terceiro; viii) tutela da saúde por profissionais da saúde, serviços de saúde ou autoridade sanitária; ix) legítimo interesse; x) proteção ao crédito.

Definir a base legal de tratamento de dados não é tarefa simples, pois a escolha do fundamento de licitude deve observar, também, a finalidade do tratamento e a situação concreta.

É importante se pontuar, também, que não há necessidade de se falar em hierarquia entre as hipóteses legais, mas, sim, em base legal a ser adotada, mediante justificção adequada, em cada caso de tratamento de dados pessoais²⁸, sendo certo que a atividade desenvolvida pelo agente de tratamento, bem como sua própria estrutura, exercerá papel importante na determinação do anteparo normativo que dará substrato ao desenvolvimento de sua atividade.

Nesse contexto, o legítimo interesse, em razão de se distanciar da necessidade de consentimento, pode parecer a escolha natural dos agentes de tratamento. Embora apresente imprecisão conceitual e, seja, portanto, dotada de certa plasticidade, essa base legal não se consubstancia em autorização genérica para o tratamento de dados. A sua utilização é indissociável da adoção de medidas específicas por parte do interessado antes, durante e após o término do tratamento.

Embora se trate de legislação nova, na perspectiva nacional, a experiência no direito comparado, em especial o direito europeu, pode servir de baliza para a introdução e abordagem do tema no direito brasileiro. Principalmente diante da expressa possibilidade de diálogo da

²⁸ PONCE, Paula Pedigone; MATTIUZZO, Marcela, O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa, **Internet & Sociedade**, v. 1, n. 2, 2020, p. 57.

LGPD com outras normas voltadas à proteção de direitos dos indivíduos em âmbito nacional ou internacional, consoante disposto no art. 64 dessa lei²⁹.

Certamente, a atuação dos agentes interessados no tratamento de dados em consonância com a legislação é tarefa desafiadora. Entretanto, a adequação à regulamentação não deve ser vista como entrave ao desenvolvimento da atividade empresarial ou como um elemento arrefecedor do desenvolvimento das relações intersubjetivas que sofrem a incidência da novel regulamentação, em especial se considerado que um dos fundamentos da disciplina da proteção de dados no Brasil é o desenvolvimento econômico, tecnológico e a inovação (art. 2º, V, LGPD).

A propósito, é oportuna a advertência no sentido da imperiosidade de não se realizar interpretações que impliquem o engessamento da atuação dos agentes privados, sendo certo que a previsibilidade do sistema é altamente desejada, principalmente quando a disciplina jurídica do tema é tendência mundial.

1.1. A proteção de dados como um direito fundamental

A fim de se compreender o legítimo interesse enquanto hipótese de tratamento de dados pessoais, é importante se evidenciar que se está lidando com um direito fundamental e projeção do direito da personalidade. O estudo em torno dos fatores sociais e jurídicos que levaram à essa categorização jurídica da proteção de dados é essencial ao entendimento da matéria dentro da perspectiva proposta.

Os dados e as informações extraídas a partir de registros relativos aos indivíduos são elementos inerentes ao atual estágio de desenvolvimento econômico e tecnológico. Ao lado do conforto proporcionado pelo desenvolvimento, se estrutura uma rede de coleta, análise e concentração de dados atinentes às pessoas, os quais permitem que governos e empresas desenvolvam ferramentas capazes de rotularem grupos e tomarem decisões precisas que podem se consubstanciar em medidas discriminatórias inquinadas de vícios e capazes de prejudicar diversos setores da sociedade.

²⁹ Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. BRASIL. **Lei 13.709/18, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 15 jun. 2021.

Há que se afastar, portanto, a prévia concepção de que os avanços tecnológicos são sempre benéficos. É preciso se perquirir, sempre, se aquilo que se revela tecnicamente possível é admissível sob as vertentes ética, política e social, ainda que juridicamente lícita³⁰.

Nesse cenário, calha delimitar o conceito de dado pessoal³¹. De acordo com a LGPD, dado pessoal é a informação relacionada à pessoa natural identificada ou identificável. A doutrina subdivide o conceito em restrito e amplo³² e a sua adoção por um determinado sistema jurídico é opção do legislador.

Em sentido restrito, o dado pessoal se adstringe a elementos de informação concernentes a alguém cuja identidade é identificável sem a necessidade de correlação com outros dados³³.

Em sentido amplo, se vai além do titular do dados identificado, sendo irrelevante se um elemento de informação se relaciona a um indivíduo em particular ou se pode ser a ele correlacionado no futuro³⁴. De tal modo, se considera dado pessoal, também, os dados que possivelmente conduzem à identificação de seu titular³⁵.

Imagine-se, à guisa de exemplo, informações, tais como número de Cadastro de Pessoa Física (CPF), nome e data de nascimento, relativas a milhões de indivíduos submetidos à jurisdição brasileira, obtidas a partir de vazamento de dados³⁶.

³⁰ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 142.

³¹Para Machado e Doneda "[a] delimitação do conceito de dado pessoal é hoje imprescindível na interpretação do alcance normativo de leis de proteção de dados. A título de exemplo, o Children's On-line Privacy Protection Act (COPPA) de 1998, estatuto norte-americano de proteção da infância no uso da internet, é aplicável a todos que coletam informação pessoal de menores de 13 anos, estabelecendo critérios para o legítimo tratamento desses dados. Pode-se citar também o Regulamento Geral de Proteção de Dados Pessoais da União Europeia, a Convenção 108 do Conselho da Europa e a Lei Federal 13.709/2018, do Brasil (Lei Geral de Proteção de Dados – LGPD). Nesses três recentes textos legislativos percebe-se que o conceito de informação pessoal é chave para entender o âmbito material de aplicação da lei, que, por sua vez, visa nas esferas regional, internacional e nacional, respectivamente, regular a atividade de tratamento de dados pessoais. *In*: MACHADO, Diego; DONEDA, Danilo, **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados**, *in*: DONEDA, Danilo (Org.), **Caderno especial: a regulação da criptografia no direito brasileiro [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2018.

³² SCHWARTZ, Paul M; SOLOVE, Daniel J, **The PII Problem: Privacy And A New Concept Of Personally Identifiable Information**, **New York University Law Review**, v. 86, p. 81; MACHADO; DONEDA, **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados**; BIONI, **Proteção de dados pessoais a função e os limites do consentimento**.

³³ SCHWARTZ; SOLOVE, **The PII problem: privacy and a new concept of personally identifiable information**, p. 1817.

³⁴ *Ibid.*

³⁵ MACHADO; DONEDA, **Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados**.

³⁶ G1, **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>>. Acesso em: 5 abr. 2021.

Nessa situação, certamente haverá homônimos e, a depender da forma como estruturadas as informações, não é possível individualizar a pessoa sem o recurso a outros elementos identificadores, a exemplo do CPF. Assim, numa visão reducionista, não se poderia falar em dado pessoal.

De outro lado, sob a óptica expansionista, a incerteza decorrente da homonímia poderia ser afastada a partir da correlação com os outros fragmentos de informação, de sorte que se poderia, sim, falar em dado pessoal.

Não há como se estabelecer, de antemão, o que é, ou não, dado pessoal, porquanto “verificar se um dado pode ser adjetivado como pessoal é uma análise contextual que depende de qual tipo de informação pode ser extraída de uma base de dados. Essa análise circunstanciada pode ser mais dura ou mais flexível”³⁷.

A moldura normativa estabelecida pela LGPD retira a repercussão prática da discussão, uma vez que é considerado dado a informação relacionada a pessoa natural identificada ou identificável (art. 5º, I). A conjunção alternativa “ou” denota a amplitude normativa desse diploma legislativo, na medida em que é possível se interpretar que o legislador optou por incluir no âmbito regulatório da LGPD o dado pessoal em sentido amplo e restrito.

Hoje, não é incomum que na aquisição de um bem ou serviço parte do pagamento seja a disponibilização de informações a respeito do interessado. Cuida-se de um fenômeno contínuo e cumulativo, viabilizando-se a criação de circunstância de “posse permanente” das informações relativas a alguém pelo receptor, materializando-se a figura do “homem de vidro”³⁸.

Não por outra razão, a intensidade da coleta, tratamento e transmissão de informações, ao lado do crescente conhecimento e controle de elementos sobre a vida pessoal, privada e social das pessoas, permitem entrever situações potencialmente vulneradoras de seus direitos fundamentais³⁹.

³⁷ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 94.

³⁸ Para Rodotà, “(...) a ideia de vigilância invade cada momento da vida e se apresenta como um traço próprio das relações de mercado, cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações. Materializa-se, assim, a imagem do ‘homem de vidro’, o verdadeiro cidadão desse novo mundo. Uma imagem que, não por acaso, provém diretamente do tempo diretamente do tempo do nazismo e que propõe uma forma de organização social profundamente alterada, uma espécie de transformação irrefreável da ‘sociedade da informação’ em ‘sociedade da vigilância’. In: RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 113.

³⁹ SARLET, Ingo Wolfgang, Fundamentos constitucionais: O direito fundamental à proteção de dados, *in*: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 41.

A onipresença da tecnologia afeta a vida em sociedade de uma maneira geral e não se sabe, ainda, de modo preciso, a forma e em que medida a ubiquidade tecnológica é capaz de moldar o comportamento dos atores sociais.

A relação de interdependência entre coleta de fragmentos de informações como pressuposto para o fornecimento e uso de diversos serviços parece fragilizar a própria noção de privacidade e revela o descompasso entre as forças dos titulares de dados e dos agentes de tratamento.

E não é só.

A atuação dos agentes de tratamento de dados influencia direta ou indiretamente o cotidiano dos indivíduos, a exemplo do caso de manipulação de informações envolvendo a empresa britânica Cambridge Analytica⁴⁰⁻⁴¹, contratada pela campanha eleitoral do então candidato Donald Trump. Em 2016 essa empresa de consultoria política obteve dados de mais de 80 (cinquenta) milhões de pessoas sem a respectiva autorização, a partir de suposto vazamento pelo Facebook, e, diante desses elementos de informação, estabeleceu estratégia de mensagens dirigidas a eleitores mais propensos a direcionarem o voto ao candidato para a qual prestava serviços, aumentando-se, assim, as chances de êxito na eleição e exercendo papel decisivo para que o candidato republicano se sagrasse vencedor na disputa presidencial. O mesmo método foi também utilizado para convencer a população britânica na campanha pela saída do Reino Unido da União Europeia⁴².

Há, ainda, discussão em torno da antecipação no combate a massacres com armas de fogo com base no tratamento de dados, consoante se infere de estudos realizados pelo

⁴⁰ BBC News. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1**. Caderno Economia. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 10 out. de 2019.

⁴¹ “Através da manipulação de informações você pode influenciar eleições, inspirar uma insurgência, desencadear um genocídio, virar as pessoas umas contra as outras e distorcer a realidade delas, até que elas não possam mais saber o que é verdade. Foi exatamente isso que a Cambridge Analytica fez para assistir às campanhas políticas”. *In: VÉLIZ, Privacidade é poder: por que e como você deveria retomar o controle de seus dados*, p. 105.

⁴² “O repertório da Cambridge Analytica de empreendimentos de guerra psicológica e informacional era vasto, e sem quaisquer limites morais. Incluía *fake news* direcionadas, propagação do medo (que chegava a mostrar imagens extremamente violentas de torturas e assassinatos reais), falsificação ideológica, e oferta de serviços altamente antiéticos, tais como “suborno ou armadilhas sexuais, campanhas de desinteresse dos eleitores, obtenção de informações para desacreditar os opositores políticos e divulgação anônima de informações em campanhas políticas”.²²⁹ Essa foi a empresa que ajudou Trump a ganhar a presidência dos Estados Unidos e a campanha pela saída do Reino Unido no referendo do Brexit (por intermédio de uma firma política associada, AIQ)”. *In: Ibid.*, p. 110.

Departamento Federal de Investigação (FBI)⁴³ dos Estados Unidos da América, além da criação de sistema que se alimente de dados provenientes de dispositivos móveis, tais como relógios inteligentes e assistentes domésticos, capazes de realizar, através de algoritmos, o monitoramento neurocomportamental dos indivíduos com o objetivo de se evitar chacinas.

Os exemplos de situações de coleta e tratamento de dados acima descritos, acaso incorretamente desenvolvidos e implementados, podem dar ensejo à captura de acervos digitais de indivíduos, de sorte que é evidente a condição de fragilidade dos titulares de dados e manifesta a necessidade de tutela de seus direitos e liberdades fundamentais. Ademais, não se pode olvidar das constantes notícias sobre vazamento de dados no contexto de crescente fornecimento de informações próprias a diversos agentes públicos e privados⁴⁴.

Cabe destacar, também, outro ponto que desvela a delicadeza do tema: os dados relacionados a alguém podem conter elementos de informação que ultrapassam sua esfera individual⁴⁵.

Portanto, deve ser claro que a necessidade de tutela dos dados pessoais não se dá em razão de sua natureza isoladamente considerada, mas no interesse da proteção do indivíduo, fonte desses elementos de informação, em face dos riscos à sua esfera jurídica que podem advir do seu tratamento inadequado.

Dessa forma, é imprescindível que se estabeleça um ponto de equilíbrio entre o livre desenvolvimento da personalidade, o princípio da livre iniciativa e a suficiência dos estatutos atualmente vigentes, sejam de índole cível ou criminal, para a proteção da pessoa.

⁴³ SILVER, James; SIMONS, Andre; CRAUN, Sarah. **A Study of Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013**. Federal Bureau of Investigation, U.S. Department of Justice. Washington, 2018. Disponível em: <https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view>. Acesso em: 4 de novembro de 2019.

⁴⁴ BRASIL, Autoridade Nacional de Proteção de Dados. **Meus dados vazaram, e agora?**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/meus-dados-vazaram-e-agora>. Acesso em: 15 fev. 2021.

⁴⁵Nesse sentido, Barocas e Nissenbaum: “ (...) [e]mbora questões de tipo e uso de informações possam, a princípio, parecer simples, elas são extremamente difíceis quando consideradas em detalhes: pode ser razoavelmente fácil para uma empresa de serviços públicos explicar aos clientes que, com medidores inteligentes, pode monitorar o uso, de modo minucioso, e, a partir disso, identificar padrões agregados inerentes ao indivíduo e entre clientes, além de poder usá-los como uma base para decisões importantes sobre a alocação de recursos e para aconselhamento específico sobre o uso de energia de clientes individuais. Ela pode explicar claramente quem receberá que informações e com que finalidade. Com este tipo de aviso, o consentimento é significativo. Entretanto, o processamento de dados por meio de *Big Data* normalmente não para aqui; uma empresa empreendedora pode tentar descobrir quantas pessoas estão associadas a uma determinada conta, quais aparelhos que eles possuem, suas rotinas (trabalho, hora de dormir e férias). Pode relacionar outras informações associadas à conta na análise e outras informações além da conta - pessoais ou ambientais, tais como o clima”. In: BAROCAS, Solon; NISSENBAUM, Helen, *Big data's end run around anonymity and consent, Privacy, Big Data, and the Public Good: Frameworks for Engagement*, p. 32, 2014, p. 59–60, livre tradução.

1.1.1. A algoritmização do direito

Antes do aprofundamento no estudo do tratamento de dados pessoais com base no legítimo interesse, se revela importante fazer breve incursão nos elementos que influenciam o comportamento dos agentes de tratamento, ainda que indiretamente, como é o caso dos algoritmos, compreendidos à luz da ciência jurídica.

Destarte, há aspecto relevante e ainda pouco debatido relacionado à ideia de programação computacional sob o influxo da lei, qual seja, a possibilidade de se elaborar códigos de programação com comandos a serem observados por um determinado sistema levando em consideração dispositivos legais⁴⁶.

Segundo Arndt⁴⁷, a expressão algoritmo decorre da latinização do nome árabe de Abu-Abdullah Muhammed ibn-Musa Al-Khwarizmi, matemático que teria vivido entre 780 e 850 depois de Cristo, para quem o algoritmo seria a expressão da concatenação de instruções a serem seguidas para que se chegasse à solução de equações.

Posteriormente, Alonzo Church e Alan Turing trouxeram à lume os conceitos de computabilidade e funções computacionais para formalizar a possibilidade de se elaborar sequências de instruções a serem seguidas não apenas por humanos, mas, também, por máquinas⁴⁸. Em 1961, Marvin Minsky foi além e vislumbrou a possibilidade de se introduzir "inteligência" nos sistemas computacionais, bem como a viabilidade da formulação de algoritmos com capacidade de aprender e ensinar sistemas computacionais⁴⁹.

⁴⁶A título de exemplo, imagine-se um carro autônomo. Certamente, é esperado que o veículo siga as normas de trânsito, tais como limite de velocidade, não ultrapassagem em faixa contínua, respeito à faixa de pedestres, entre outros aspectos corriqueiros que, acaso desobedecidos ensejam responsabilização civil e, possivelmente, também, criminal. Neste contexto, consoante defendido por Hilgendorf, a transposição do sistema jurídico para a linguagem binária (computacional), é chamada de algoritmização do direito. *In: HILGENDORF; FELDLER, **Digitalization and the Law**.*

⁴⁷ ARNDT, A. B., Al-Khwarizmi, *The Mathematics Teacher*, v. 76, n. 9, p. 668–670, 1983.

⁴⁸ *Ibid.*

⁴⁹ OSOBA, Osonde A.; WELSER, William IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*, Santa Monica: RAND Corporation, 2017, p. 4–5.

Para os propósitos do presente trabalho, conceitualmente, pode-se compreender algoritmo como complexo descritivo de etapas que, se executadas na sequência correta, permite a determinado programa de computador se desincumbir da tarefa que fora pré-estabelecida⁵⁰⁻⁵¹.

Atualmente se tem a noção de *Big Data* como expressão do potencial dos algoritmos enquanto mecanismos de correlação de diversas informações aparentemente desconexas e produção de conclusões importantes tanto do ponto de vista do interesse estatal quanto de agentes privados.

Com efeito, embora seja usualmente descrito como parte da ciência da computação associada à inteligência artificial, cuida-se de ideia de difícil expressão por meio de palavras, mas alguns autores identificam algumas propriedades desse fenômeno: a) larga quantidade de dados coletados; b) imprecisão dos elementos de informação recolhidos em razão da escalabilidade dos dados; e c) capacidade de correlacionar os dados entre si sem necessariamente se estabelecer relação de causalidade⁵².

O terceiro aspecto chama atenção na medida em que as conclusões a que se chega por meio da adoção dessa tecnologia não estão ancoradas, necessariamente, em cientificidade, mas em resultados estatísticos.

Por exemplo, cite-se o caso da empresa Target que, a partir do monitoramento de aquisições por suas consumidoras, conseguiu, por meio de correlação, estimar com elevado grau de precisão quais estariam grávidas, mesmo que os produtos adquiridos não se cuidassem de bens voltados diretamente para bebês ou gestantes⁵³.

Mediante o processamento de informações por meio de *Big Data*, portanto, importa menos saber o porquê de algum fenômeno que se tenha constatado e mais se ter a ciência de que ele está ocorrendo. Desta forma, se pode estabelecer ligações entre eventos que, em linha de princípio, sequer estariam relacionados.

⁵⁰ Para Cormen e outros, “um algoritmo é qualquer procedimento computacional bem definido que toma algum valor ou conjunto de valores como entrada e produz algum valor ou conjunto de valores como saída. Portanto, um algoritmo é uma sequência de passos computacionais que transformam a entrada na saída”. *In*: CORMEN, Thomas H. *et al*, **Algoritmos - teoria e prática**, 2. ed. São Paulo: Elsevier, 2002, p. 3.

⁵¹ No mesmo sentido da ideia aqui defendida, Mendes e outros entendem que “um algoritmo é comumente descrito como um conjunto de instruções, organizadas de forma sequencial, que determina como algo deve ser feito”. MENDES, Laura Schertel; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy, *Discriminação algorítmica à luz da Lei Geral de Proteção de Dados*, *in*: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 430.

⁵² MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth, **Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight**, Londres: John Murray, 2013.

⁵³ DUHIGG, Charles, **O poder do hábito: por que fazemos o que fazemos na vida e nos negócios [livro eletrônico]**, Rio de Janeiro: Objetiva, 2012.

Nesse contexto, os algoritmos, enquanto modelos probabilísticos postos em movimento, evidenciam os riscos aos indivíduos que vivem na era da "datificação" decorrentes da tomada de decisões baseadas em dados, já que é plenamente factível, por exemplo, por meio da análise elementos de informação fornecidos pelo titular dos dados, se prever quem teria maior probabilidade de desenvolver doenças, de se tornar inadimplente ao firmar contrato de mútuo feneratício ou, ainda, de cometer crimes, o que teria reflexos diretos, respectivamente, no preço do plano de saúde, na decisão do mutuante em relação ao pretense mutuário e no tratamento dado pelo Estado ao indivíduo potencialmente transgressor.

Erros nos algoritmos voltados para uso recreativo ou comercial podem até ser toleráveis. Contudo, quando equívocos ocorrem em áreas delicadas, a exemplo da aplicação do direito sancionatório ou situações de discriminação abusiva⁵⁴ de indivíduos, pode-se pensar em um risco sistêmico altamente indesejado, em especial se considerada a escalabilidade de modelos que ostentam o condão de definir e delimitar a vida dos indivíduos⁵⁵.

Nesse cenário, alguns autores mencionam o conceito de "sociedade pontuada", na qual modelos preditivos são elaborados e aplicados a partir da introdução, pelos engenheiros de *software*, de parâmetros sobre as análises dos dados minerados, fluxos de decisão, interconexões, sendo evidente que antes da operacionalização do programa de computador há a interlocução humana e, junto dela, a incorporação da carga de valores ético-sociais dos desenvolvedores de sistemas e programadores⁵⁶.

Paralelamente, a automação da tomada de decisões por governos e empresas incrementa a demanda por *softwares* que permitam aos atores sociais que se utilizam de mecanismos de

⁵⁴ É importante que se perceba que a mera diferenciação entre indivíduos, em si, não é algo prejudicial. A doutrina que discute o tema da proteção de dados e discriminação usualmente associa ao substantivo predicados que remetem à ideia de atuação em desconformidade com os preceitos legais vigentes e com a noção de igualdade material. A propósito, vale mencionar que a LGPD veda a discriminação com fins abusivos ou ilícitos, sendo certo que a diferenciação dissociada dessas finalidades não é, em linha de princípio, incompatível com o sistema de proteção de dados. Nesse sentido, Mendes e outros ponderam que “[n]a medida em que a lei afirma que são vedadas práticas discriminatórias cujas finalidades sejam abusivas ou ilícitas, compreende-se que práticas discriminatórias que não tenham tais finalidades são consideradas permitidas”. *In*: MENDES; MATTIUZZO; FUJIMOTO, Discriminação algorítmica à luz da Lei Geral de Proteção de Dados, p. 430. Na mesma linha: BIONI, Bruno Ricardo, Legítimo interesse: aspectos gerais a partir de uma visão obrigacional, *in*: **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Forense, 2021, p. 178.

⁵⁵ “If a bank’s model of a high-risk borrower, for example, is applied to you, the world will treat you as just that, a deadbeat—even if you’re horribly misunderstood. And when that model scales, as the credit model has, it affects your whole life—whether you can get an apartment or a job or a car to get from one to the Other”. O’NEIL, Cathy, **Weapons of math destruction: How big data increases inequality and threatens democracy**, Nova Iorque: Crown Publishers - Broadway Books, 2016, p. 28.

⁵⁶ CITRON, Danielle Keats; PASQUALE, Frank A., **The Scored Society: Due Process for Automated Predictions**, Rochester, NY: Social Science Research Network, 2014, p. 14.

decisões automatizadas a terem a segurança de atuarem de acordo com a lei. Sob esse prisma, a crescente confiança na inteligência artificial parece ensejar o mesmo crescimento no grau de risco envolvido no seu uso constante.

Os sistemas de tomada de decisão automatizados, os quais, com base em algoritmos, reagem de forma independente do estímulo humano às mais diversas situações e podem, ou não, lograr êxito ao lidar com problemas não previstos de forma autônoma. Isso ganha maior relevância quando se considera a possibilidade de esses sistemas aprenderem a partir das próprias experiências. É o que se chama de *machine learning*.

Cabe destacar, também, principalmente diante do fato de que "muitos dos algoritmos-chave que afetam a vida em sociedade são, também, considerados proprietários ou segredos comerciais"⁵⁷, a dificuldade de se difundir, sob o espectro cultural, a importância do domínio desse conceito, em especial sob a dimensão de sua legitimidade.

Outrossim, a ausência de regulamentação sobre o tema, a falta de transparência em torno dos elementos considerados para processamento e a sua forma de interação com outros fragmentos de informação dão margem à concretização de condutas arbitrárias que devem ser enfrentadas adequadamente.

Com efeito, a objetividade subjacente a decisões tomadas por computador pode se revelar eticamente deficiente. Todavia, essa imperfeição, por vezes, é muito mais difícil de identificar. Hoffmann-Riem observa que⁵⁸:

O desenvolvimento de algoritmos muitas vezes, embora nem sempre – por exemplo, em empresas comerciais –, é integrado a processos complexos de desenvolvimento de software. Estes visam a realização de problemas concretos, a elaboração de requisitos para a solução do problema, a concepção da arquitetura do software, a realização técnica de TI por codificação, o uso prático do software e, se necessário, a sua revisão após experiências em teste ou operação real. Diferentes jogadores ou equipes maiores são regularmente envolvidos neste processo, mesmo que a implementação técnica seja, em última instância, realizada por desenvolvedores de software ou programadores. Tal desenvolvimento de *software* não é um ato puramente técnico – ou mesmo neutro –, mas um ato de organização social no qual objetivos e avaliações são processados; ele pode ser orientado para experiências anteriores e possíveis consequências e pode exigir seleções. Neste sentido, existem paralelos estruturais à criação de normas legais. Uma diferença central, entretanto, é que os fatores que influenciam o desenvolvimento dos algoritmos não precisam ser, e em princípio não são, normas legais.

⁵⁷ OSOBA; WELSER, **An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence**, p. 6.

⁵⁸ HOFFMANN-RIEM, Wolfgang, **Teoria geral do direito digital: transformação digital: desafios para o direito**, Rio de Janeiro: Forense, 2021, p. 54.

É certo que a construção dos algoritmos conta com diversos atores e etapas de produção e, ainda assim, os modelos são pensados a partir da inserção controlada de informações durante o processo de sua formulação (dados probabilísticos), os quais não necessariamente corresponderão à realidade quando de sua aplicação prática. Dessa atividade podem advir resultados inesperados, desejados ou não⁵⁹.

Esses aspectos se tornam preocupantes na medida em que a opacidade e invisibilidade dos modelos adotados, não raramente protegida pelo segredo comercial⁶⁰, conforme já mencionado, dificulta sobremaneira a identificação da relação de causalidade entre os elementos processados e o comportamento da máquina, classificando indivíduos ou tomando decisões de forma autônoma.

Ademais, há, ainda, outra situação inquietante: a dificuldade de se elaborar legislação capaz de tutelar adequadamente os indivíduos contra análises probabilísticas realizadas por programa de computador, uma vez que vieses discriminatórios ainda podem fazer parte do algoritmo conquanto, caso aberto seu código-fonte, não se tenha nada que conecte diretamente o comportamento do modelo à tomada de decisões de cunho discriminatório, automatizadas ou não.

Espera-se que no futuro haja maior participação das máquinas na vida cotidiana dos indivíduos, que, para cumprirem suas tarefas, precisarão de autonomia cada vez maior. Essa afirmação conduz à necessidade de correlacionar mecanismos de tomada de decisão automatizados, a influência de vieses discriminatórios e a possibilidade de responsabilização dos agentes envolvidos, principalmente se considerado que um programa de computador tende a tomar decisões mais baseadas em racionalidade e eficiência do que em emoções e empatia.

Não se desconhece o risco da tomada de decisão moralmente questionável, mas indefectível sob o prisma lógico, e o sistema legal deverá enfrentar esse tipo de situação que venha a se materializar no plano fático⁶¹.

⁵⁹ “(...) a opacidade dos algoritmos torna mais difícil a atividade de aferir a correição, avaliar riscos e encontrar a justeza nas aplicações sociais. Pode, também, obscurecer a relação de causalidade entre os elementos de convicção e a tomada de decisão. Esse problema seria inofensivo se os algoritmos fossem (quase) infalíveis. Porém, a maioria dos algoritmos ostenta apenas garantias probabilísticas de acerto. Isso é, no melhor cenário, no qual modelos e algoritmos são aplicados apropriadamente, com a melhor intenção a dados "perfeitos". Os desenvolvedores de algoritmos e os usuários dificilmente têm a chance de atuar em cenários perfeitos. Eles têm que confiar em presunções que podem falhar e conduzir a resultados inesperados”. *In*: OSOBA; WELSER, **An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence**, p. 3, livre tradução.

⁶⁰ O'NEIL, **Weapons of math destruction: How big data increases inequality and threatens democracy**, p. 28.

⁶¹ HILGENDORF; FELDLER, **Digitalization and the Law**, p. 43.

Ademais, o funcionamento adequado de um equipamento dotado da capacidade de adotar decisões autonomamente demanda o processamento de um extenso volume de informações. Portanto, deve ser observado eventual regime de proteção de dados em vigor.

Assim, não pairam dúvidas de que novas tecnologias desafiam a sociedade e o arcabouço normativo vigente. Porém, o direito não pode se quedar inerte diante das mudanças sociais. Ao contrário. Deve ser capaz de, sob o influxo da força construtiva dos fatos sociais⁶², estabelecer as consequências jurídicas decorrentes dessas modificações de comportamento da sociedade.

Um dos caminhos para a solução do problema do viés dos modelos algorítmicos passa pela conciliação de abordagens técnicas e não-técnicas, sendo a transparência o anteparo sobre o qual se projetarão as soluções.

É imprescindível que aspectos multiculturais e interdisciplinares sejam levados em consideração e conhecê-los parece ser um passo fundamental, da mesma forma que se revela imperioso o reconhecimento de que algoritmos podem, sim, conduzir a resultados injustos.

1.1.2. O valor patrimonial dos dados

Tim Wu identifica o crescimento de uma indústria relativamente recente: a indústria dos mercadores de atenção⁶³. O autor aponta que os primeiros mercadores de atenção podem ser identificados no Século XIX.

Por volta de 1830, Benjamin Day, proprietário de uma gráfica em Nova York, decidiu vender jornais a um valor cerca de 80% (oitenta por cento) inferior ao dos concorrentes. Naquela época, o jornal era considerado artigo de luxo e o empresário decidiu comercializá-lo a preço similar ao de certos itens do cotidiano, ainda que por valor inferior ao do necessário para produzir o periódico.

O prospecto do negócio, embora negativo (venda de produto a preço inferior ao de produção), guardava uma mudança na estratégia tradicional dos empresários na busca de lucro (venda de produto a preço superior ao de produção): a revenda da atenção da audiência através de anúncios.

Segundo Wu, "o que Day entendeu - mais precisamente, mais claramente do que qualquer um antes dele - foi que enquanto os seus leitores pudessem pensar que eram seus

⁶² FACHIN, Luiz Edson, **Direito Civil sentidos, transformações e fim.**, Rio de Janeiro: Renovar, 2015.

⁶³ WU, Tim, **The Attention Merchants: The Epic Scramble to Get Inside Our Heads**, Nova Iorque: Alfred A. Knopf, 2016.

consumidores, eles eram, na verdade, seu produto"⁶⁴ e assim o The Sun foi lançado em 3 de setembro de 1833.

O mercado da atenção, na busca de se adaptar às mudanças de hábito dos consumidores e às modificações nas relações sociais, evolui de forma consistente e constante e é possível perceber sua interferência em diversos meios, a exemplo do rádio, da televisão e do cinema⁶⁵.

Nas diversas formas de disponibilização de produtos e serviços atrelados a esse mercado, se pode reconhecer um fato recorrente, qual seja a oferta de um bem ou serviço associada à disponibilização ao público de outro bem de seu interesse. Como exemplo, se menciona o anúncio de patrocinador em transmissão esportiva em canais de televisão "abertos" e, também, o chamado *product placement* (marketing indireto) em programas de entretenimento⁶⁶.

Mais modernamente é possível se identificar uma miríade de serviços digitais ofertados "gratuitamente" que exigem para sua disponibilização a concordância do consumidor com "termos e condições" de uso. Não raro, a cessão de dados pessoais, em maior ou menor escala, está presente como uma das cláusulas da avença e vem desacompanhada da necessária contrapartida ao usuário, principalmente sob o enfoque informacional, em especial no que concerne à abrangência da disposição de seus dados. Nesse contexto, o comportamento de várias grandes empresas (como o Facebook) serve de exemplo do que ora se afirma⁶⁷.

Hoje, grande parte das pessoas se utilizam de dispositivos "que constantemente encontram maneiras de comercializar as menores partículas de seu tempo e atenção"⁶⁸⁻⁶⁹.

⁶⁴ *Ibid.*, p. 10, livre tradução.

⁶⁵ "A partir do rádio, cada novo meio atingiria sua viabilidade comercial através da revenda de qual atenção poderia captar em troca de seu conteúdo 'livre'" (*Ibid.*, p. 6)

⁶⁶ PETROLL, Martin de La Martiniere; PRADO, Paulo Henrique Muller, A theoretical essay on TV show placement and its effects on consumers/Um ensaio teórico sobre placement televisivo e seus efeitos sobre o consumidor, **Revista de Administração Contemporânea**, v. 18, n. 2, p. 176–196, 2014.

⁶⁷ No ponto, Wu propõe a seguinte reflexão: "[p]or fim, o público tinha feito uma grande barganha com o Facebook - não exatamente inconscientemente, mas também não com pleno conhecimento. Tendo sido originalmente atraído para o Facebook com a tentação de encontrar amigos, ninguém parecia notar que este novo comerciante de atenção havia invertido os termos de acordo usuais do setor. Seus bilhões de usuários no mundo inteiro estavam simplesmente entregando um tesouro de dados demográficos detalhados e se expondo a publicidade altamente direcionada em troca de quê, exatamente? Os jornais tinham oferecido relatórios, a CBS tinha oferecido I Love Lucy, o Google o ajudou a encontrar seu caminho na super-estrada da informação. Mas Facebook?" (livre tradução). In: WU, **The Attention Merchants: The Epic Scramble to Get Inside Our Heads**, p. 280.

⁶⁸ *Ibid.*, p. 6.

⁶⁹ "Todos na indústria da tecnologia querem que você preste atenção nos aplicativos, nas plataformas, nos anúncios. Eles querem saber mais sobre você para que eles possam saber como melhor distraí-lo, mesmo que isso signifique atraí-lo para longe do tempo de qualidade com seus entes queridos ou necessidades humanas básicas, como o sono". In: VÉLIZ, **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**, p. 85.

Deveras, o contínuo fornecimento de dados para o desempenho das mais diversas atividades, seja através do uso de dispositivos eletrônicos ou mesmo de relações entabuladas com terceiros, torna bastante factível a ideia de uma espécie de “biografia digital”, nos termos propostos por Daniel J. Solove⁷⁰.

Com efeito, o uso de dados pessoais, hoje, faz parte do dia a dia de empresas e indivíduos, de sorte que esses fragmentos de informação sobre as pessoas se consubstanciam em poderoso ativo para pequenos e grandes empresários e, também, governos. Os dados são elementos basilares das relações sociais e a circulação e detenção de informações neles baseadas impactam diretamente nas relações de poder⁷¹.

Sob o ângulo comercial, o acúmulo de material a respeito dos indivíduos, especialmente no que diz respeito a preferências de consumo, permite às empresas o desenvolvimento de estratégias voltadas ao aumento de seus lucros, bem como à obtenção de diferencial competitivo na sua área de atuação⁷².

Ademais, a qualidade e quantidade dos elementos coletados permite uma série de usos secundários, possibilitando-se aos agentes tratadores de dados a criação de informações novas (perfis de consumo, análises de preferências de determinado público, informações estatísticas etc.) que interessam a outros atores sociais e não somente àqueles que coletaram esses fragmentos de informação⁷³.

Assim, ressoa inequívoco o reconhecimento da atenção enquanto elemento dotado de valor patrimonial, ainda mais diante da atual oferta de produtos dirigidos a consumidores específicos por agentes econômicos que se utilizam de avançadas tecnologias de processamento de dados.

O insumo e estímulo principal para a criação de bens e serviços capazes de captar a atenção dos indivíduos de forma diretamente remunerada, ou não, são os dados, traços de informação deixados pelas pessoas ao desempenharem suas atividades cotidianas.

⁷⁰ SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. Rochester, NY: Social Science Research Network, 2004. Disponível em: <<https://papers.ssrn.com/abstract=2899131>>. Acesso em: 21 jul. 2020.

⁷¹ “A crescente confiança na inteligência artificial parece ensejar o mesmo crescimento no grau de risco envolvido no seu uso constante”. RODOTÁ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 35.

⁷² OLIVEIRA, Ricardo; COTS, Márcio, **O legítimo interesse e a LGPD**, São Paulo: Thomson Reuters Brasil, 2020. pp.28-29

⁷³ RODOTÁ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 36.

A concepção amplamente difundida de que os dados seriam o novo petróleo faz cada vez mais sentido. Não se olvida que a afirmação é passível de ressalvas⁷⁴, mormente quando se considera que o petróleo é um recurso finito e não reutilizável, enquanto os dados são potencialmente infinitos e reutilizáveis⁷⁵.

Ao lado dessa diferença fundamental, há, também, ponto de convergência que merece destaque: assim como o petróleo, após o seu processamento e refino para os seus diversos empregos, o dado processado ostenta muito mais valor do que em seu estado bruto. A propósito, se menciona trecho, de relatório elaborado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD – sigla em inglês)⁷⁶:

Juntamente com a expansão dos dados, sua transformação em informações úteis para uma melhor tomada de decisões apresenta desafios adicionais. Uma cadeia de valor inteiramente nova evoluiu em torno de empresas que apoiam a produção de *insights* a partir de dados, incluindo aquisição de dados (para fornecer novas fontes de dados), armazenamento e armazenamento de dados, modelagem e análise de dados, e visualização de dados. Nos níveis inferiores da "cadeia de valor de dados", o conteúdo de informação é limitado e, portanto, o escopo para a geração de valor também é baixo. O valor aumenta à medida que o conteúdo de informação e conhecimento aumenta.

Hoje, a vida conectada a celulares e outros “dispositivos inteligentes”, tais como relógios, carros etc., enseja abundante produção de dados⁷⁷ e, em razão da gama de equipamentos dessa natureza existentes, as inferências decorrentes do exame dos rastros digitais deixados pelos usuários são cada vez mais precisas o que, de acordo com acima exposto, lhes confere ainda mais valor.

Nesse contexto, a coleta, armazenamento e uso de dados de usuários por grandes empresas de tecnologia lhes garante larga margem de lucros, já que essas entidades, além de utilizarem esses fragmentos de informação em sua própria estrutura, seja na formulação de

⁷⁴ HOFFMANN-RIEM, **Teoria geral do direito digital: transformação digital: desafios para o direito.**

⁷⁵ MARCIN, SZCZEPANSKI, *Is data the new oil?*, **European Parliamentary Research Service**, 2020, p. 4.

⁷⁶ UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, **Digital economy report 2019: value creation and capture: implications for developing countries**, Genebra: United Nations, 2019, p. 29.

⁷⁷ "Um dos traços distintivos dos últimos anos tem sido o crescimento exponencial na agregação de informações legíveis por máquina, ou dados digitais, através da Internet. Isto tem sido acompanhado por um expansão de grandes análises de dados, inteligência artificial (AI), computação em nuvem e novos modelos de negócios (plataformas digitais)" *Ibid.*, p. 3.

políticas internas, na elaboração de produtos ou disponibilização de serviços ou construção de perfis de usuários, os comercializam com terceiros⁷⁸.

Segundo o próprio site do Facebook, é possível "usar *cookies* internos e de terceiros com seu *pixel* do Facebook. A diferença entre os *cookies* internos e os de terceiros está em quem é o proprietário dos *cookies*"⁷⁹.

De acordo com a Associação Internacional de Profissionais da Privacidade (IAPP – sigla em inglês)⁸⁰:

Também conhecido como *web bug*, *pixel tag* ou *clear GIF*, um *web beacon* é uma imagem gráfica clara (normalmente um pixel em tamanho) que é entregue através de um navegador web ou e-mail HTML. O *web beacon* opera como uma *tag* que registra a visita de um usuário final a uma determinada página *web* ou a visualização de um determinado e-mail. Também é frequentemente usado em conjunto com um *cookie* da *web* e fornecido como parte de um serviço de rastreamento de terceiros. Os *Web beacons* fornecem uma capacidade de produzir perfis específicos de comportamento do usuário em combinação com os logs do servidor *web*. Cenários comuns de uso para *web beacons* incluem contagem de impressões de anúncios online, monitoramento de *download* de arquivos e gerenciamento de desempenho de campanhas publicitárias. Os *web beacons* também podem informar ao remetente sobre quais e-mails são lidos pelos destinatários. As considerações de privacidade para *web beacons* são similares às dos *cookies*. Algum tipo de aviso é importante porque o *pixel* claro de um *web beacon* é literalmente invisível para o usuário final.

Por oportuno, o considerando 30 do GDPR reconhece os identificadores por via eletrônica como instrumentos capazes de definir perfis e identificar pessoas singulares a partir dos vestígios deixados durante a navegação⁸¹.

⁷⁸“A corrida para obter dados já começou, liderada por gigantes como Google, Facebook e Tencent. Até agora, muitos deles parecem ter adotado o modelo de negócios dos “mercadores da atenção”. Eles capturam nossa atenção fornecendo-nos gratuitamente informação, serviços e entretenimento, e depois revendem nossa atenção aos anunciantes. Mas provavelmente visam a muito mais do que qualquer mercador de atenção anterior. Seu verdadeiro negócio não é vender anúncios. E sim, ao captar nossa atenção, eles conseguem acumular imensa quantidade de dados sobre nós, o que vale mais do que qualquer receita de publicidade. Nós não somos seus clientes — somos seu produto”. HARARI, Yuval Noah, **21 lições para o século 21**, São Paulo: Companhia das Letras, 2018, p. posição 1453 [ebook kindle].

⁷⁹ FACEBOOK, **Sobre configurações de *cookies* para o pixel do Facebook**, Central de Ajuda do Facebook para Empresas. Disponível em: <<https://pt-br.facebook.com/business/help/471978536642445>>. Acesso em: 3 maio 2021.

⁸⁰ IAPP, International Association of Privacy Professionals, **Web Beacon**. Disponível em: <<https://iapp.org/resources/article/web-beacon/>>. Acesso em: 3 maio 2021.

⁸¹ “As pessoas singulares podem ser associadas a identificadores por via eletrônica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares”. UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 3 maio 2021.

finalidade da coleta dos dados em relação aos titulares. Discutiu-se, ainda, à luz da Diretiva 46/95, se o tratamento ocorrido era com base no consentimento ou no legítimo interesse.

Embora se tenha decidido com base no consentimento em razão de peculiaridades das leis tomadas como parâmetro para a decisão, a Corte ponderou que caso o tratamento se desse com base no legítimo interesse, dispensado, portanto, o consentimento, se deveria esclarecer quais interesses legítimos autorizariam o tratamento: se os do próprio administrador da página, ou os do terceiro, também destinatário dos dados. Diante da conjugação de vontades, se assinalou que os interesses de ambas as empresas deveriam ser considerados⁸⁵.

Não restam dúvidas que os dados dos indivíduos são economicamente relevantes. Estabelecida essa premissa, se arrosta o seguinte desafio: quantificar o quanto valem os dados do consumidor para uma empresa⁸⁶.

É certo que peculiaridades culturais, geográficas e sociais refletem em diferente valoração dos fragmentos de informação que se obtém dos indivíduos e de outras pessoas relacionadas ao seu círculo social⁸⁷.

Desta sorte, dados financeiros podem ser mais caros a determinados indivíduos do que dados biométricos, ou mesmo a privacidade de maneira geral pode ser mais importante em determinada sociedade do que em outra, a exemplo do que constatado por Jeffrey Prince e Scott Wallsten, ao apontarem que, em geral, as pessoas na Alemanha valorizam mais a privacidade do que as pessoas nos EUA e na América Latina⁸⁸.

Questão central diz respeito à forma de se precificar a privacidade. Cuida-se de tarefa complexa, em especial quando se observa a dificuldade em se estabelecer conceito uniforme

⁸⁵ Quanto ao legítimo interesse, o tribunal europeu concluiu que "[n]uma situação como a que está em causa no processo principal, em que o administrador de um sítio Internet insere no referido sítio um módulo social que permite ao navegador do visitante desse sítio solicitar conteúdos do fornecedor do referido módulo e transmitir para esse efeito ao referido fornecedor dados pessoais do visitante, é necessário que esse administrador e esse fornecedor prossigam, cada um deles, com essas operações de tratamento, um interesse legítimo, na aceção do artigo 7.º, alínea f), da Diretiva 95/46, a fim de que estas sejam justificadas em relação a si."

⁸⁶ "Os dados pessoais passam a ser considerados um ativo dentro dessa nova estrutura econômica. Por meio da coleta e tratamento dos dados pessoais se tornou possível não só segmentar o mercado de consumo por meio da criação de perfis, como destacado anteriormente, mas também promover de forma eficiente a publicidade direcionada de produtos e serviços, baseada justamente no *profiling* realizado com base na reunião daqueles dados". In: TERRA, Aline de Miranda Valverde; MULLHOLLAND, Caitlin, A utilização econômica de rastreadores e identificadores on-line de dados pessoais, in: FRAZÃO, Ana; TEPEDINO, Gustavo; DONEDA, Danilo (Orgs.), **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2020, v. 1.

⁸⁷ BAROCAS; NISSENBAUM, Big data's end run around anonymity and consent.

⁸⁸ PRINCE, Jeffrey; WALLSTEN, Scott, How Much is Privacy Worth Around the World and Across Platforms?, **SSRN Electronic Journal**, 2020, p. 20.

em torno do que seja privacidade e das disparidades de tratamento conforme a realidade social do titular⁸⁹.

Ao lado dessa dificuldade, se pode mencionar, também, a diferença entre as informações que se obtém a depender do tipo de dado explorado, as distinções de perfil (etário, socioeconômico etc.) dos titulares de dados, bem como a complexidade das relações sociais diretamente impactadas por mudanças políticas, econômicas e tecnológicas⁹⁰.

Em junho de 2013, a empresa Financial Times desenvolveu ferramenta, atualizada em julho de 2017, para conscientizar os usuários sobre o valor de seus dados pessoais, tendo, ainda, alertado que "enquanto a indústria de corretagem de dados multibilionária lucra com o comércio de milhares de detalhes sobre indivíduos, esses pedaços de informação são frequentemente vendidos por uma fração de um centavo cada um"⁹¹.

Cuida-se de estimativa baseada em pesquisa de mercado realizada pelos próprios desenvolvedores, mas é relevante sob a óptica da ênfase dada ao aspecto econômico dos dados pessoais além de conduzir à conclusão, já anteriormente apontada, de que quanto mais precisa a informação em torno do indivíduo, mais valor têm os dados pessoais a ele relacionados.

Sob o prisma jurídico, a ausência de regulamentação ou mesmo de debate sobre o tema não impede a comercialização aberta de dados, a exemplo do estudante que vendeu seus dados, por meio de leilão, por €350 (trezentos e cinquenta euros) no ano de 2014⁹² ou do indivíduo que iniciou projeto de financiamento coletivo, intitulado de "um pedaço de mim", para venda de seus próprios dados⁹³.

⁸⁹ Para Rodotà, "a privacidade, portanto, não pode ser considerada como uma noção unificadora, como um conceito que exprime exigências uniformemente difundidas na coletividade". *In*: RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 28.

⁹⁰ A propósito, faz-se menção à ponderação de Prince e Wallsten: "[a] variação de valores [relativos a dados pessoais] dentro dos países examinados [Alemanha, Estados Unidos, Argentina, Brasil, Colômbia e México], em grande parte semelhante, traz interessantes implicações tanto para as empresas quanto para os governos. Para as empresas, a pesquisa sugere que, na medida em que proteção de privacidade por níveis pode ser economicamente sensível para um país, é provável que seja economicamente sensível para todos em nosso grupo objeto de estudo. Com relação às políticas governamentais, estes resultados sugerem que, quando vista em termos econômicos, a distribuição de apoio na tutela da privacidade é provavelmente semelhante em todos os países. A notável exceção em ambos os casos é a Alemanha, que parece ter mais preferências homogêneas em relação à privacidade de dados on-line." PRINCE; WALLSTEN, *How Much is Privacy Worth Around the World and Across Platforms?*, p. 27.

⁹¹ STEEL, Emily *et al*, **How much is your personal data worth?**, Financial Times. Disponível em: <<https://ig.ft.com/how-much-is-your-personal-data-worth/>>. Acesso em: 3 maio 2021.

⁹² SOLON, Olivia, **"Data soul" of Shawn Buckles sells for £288**, Wired UK. Disponível em: <<https://www.wired.co.uk/article/shawn-buckles-is-worth-350-euros>>. Acesso em: 3 maio 2021.

⁹³ ZANNIER, Frederico, **A bite of Me**, Kickstarter. Disponível em: <<https://www.kickstarter.com/projects/1461902402/a-bit-e-of-me>>. Acesso em: 3 maio 2021.

No direito comparado, conquanto não verse diretamente sobre a quantificação do valor patrimonial do dado pessoal, a Lei de Proteção de Dados da Califórnia, California Consumer's Privacy Act (CCPA), na seção 1798.110, inserida no título 1.81.5 do Código Civil da Califórnia, estabelece a obrigação de o agente de tratamento informar ao consumidor o propósito da coleta ou venda de suas informações pessoais, as categorias de dados coletados, as fontes de obtenção desses dados, os terceiros com quem os dados são compartilhados e o direito do consumidor de impedir a venda dos dados mediante requerimento, sem que isso possa implicar discriminação negativa do consumidor que requeira as informações ou opte pela cessação de seu fornecimento, nos termos da seção 1798.125⁹⁴.

Identifica-se, no referido diploma, um dever geral de transparência imposto àqueles que lidam com dados pessoais ao mesmo tempo em que se robustece a figura do titular, pois ao lado dos direitos de exigir que as informações relativas aos dados comercializados lhe sejam prestadas e de impedir sua venda, há o dever de o agente de tratamento de informar sem que isso represente uma discriminação que gere consequências negativas ao consumidor.

Outrossim, se infere que o legislador da Califórnia não desconhece o caráter patrimonial dos dados pessoais e, embora não tenha adentrado na regulamentação acerca da precificação desse ativo, cuida-se de norma que já está em vigor e representa etapa relevante no amadurecimento da discussão.

⁹⁴ 798.100. (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(...)

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out.

(...)

798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. UNITED STATES. California Consumer Privacy Act. Disponível em: <https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375&showamends=fals>. Acesso em: 3 mai. 2021.

A instrumentalização legal da possibilidade de conhecimento do consumidor sobre o fenômeno da comercialização de elementos de informação que lhe dizem respeito representa aspecto fundamental no exercício de seus direitos, pois: a) permite reflexão sobre o valor intrínseco de suas próprias informações; b) propicia uma redução da assimetria na relação entre o agente de tratamento e o titular de dados⁹⁵; c) proporciona eventual mudança de comportamento a partir da detenção de informações sobre a viabilidade de se comercializar suas informações.

Também nos Estados Unidos, dois membros do Senado, no ano de 2019, apresentaram projeto de lei que busca obrigar empresas coletoras de dados a informar aos consumidores e agentes reguladores exatamente quais dados estão sendo coletados e o quanto eles geram de lucro para cada plataforma⁹⁶.

Trata-se de iniciativa relevante e sensível às mudanças proporcionadas pelo avanço da tecnologia. Deveras, medidas que privilegiem a transparência e reforcem os direitos dos titulares de dados devem sempre ser bem recebidas.

Embora não haja, no referido documento, a descrição de como se chegaria ao valor dos dados pessoais de alguém, acaso se logre êxito no processo legislativo, as relações entre agentes de tratamento e titulares de dados tenderá a mudar.

No Brasil, não há, na LGPD, previsão específica e explícita sobre o dever de informação do agente de tratamento ao titular de dados acerca da venda de seus dados e sobre o lucro proporcionado pelo comércio dessas informações.

Em que pese a ausência de previsão na legislação pátria, na linha do que defendido por Hoffman-Riem⁹⁷ e a partir da premissa de que os dados são sim relevantes do ponto de vista

⁹⁵ “Vive-se em ambiente marcado por elevada assimetria informacional: uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que o cidadão comum, por vezes consumidor nas relações desenvolvidas. Esse cenário enseja diversos questionamentos acerca, por exemplo, da validade do consentimento do titular dos dados nos contratos celebrados, principalmente quando eles são de adesão. A assimetria informacional não se revela apenas no poder que o agente dispõe sobre os dados pessoais de terceiros, mas também nas novas modalidades de negócio, em que informações pessoais de seus usuários representam uma das bases centrais do sistema desenvolvido”. *In*: TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados na LGPD. *In*: **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro [livro eletrônico]**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

⁹⁶ Disponível em: <<https://www.warner.senate.gov/public/index.cfm/2019/6/warner-hawley-introduce-bill-to-force-social-media-companies-to-disclose-how-they-are-monetizing-user-data>>. Acesso em 21 abr. 2021.

⁹⁷ “Em termos de política legal, seria mesmo justificável, se não necessário, obrigar os provedores a pagar aos usuários uma taxa justa se eles concordarem com a coleta e utilização dos dados, mesmo na medida em que isso não sirva para fornecer ou melhorar o serviço solicitado, mas para uso posterior. É verdade que nem todos os dados

econômico, posiciona-se no sentido de ser salutar a existência da obrigação de pagamento àqueles que anuírem com a coleta e utilização de seus dados.

Uma previsão legal dessa natureza, certamente estimularia a transparência nas relações e, por via de consequência, também a participação dos indivíduos fontes de dados no controle do processamento e circulação de informações sobre si, além da redução da distorção do mercado pela assimetria de poder entre os seus participantes.

Há que se deixar claro que o conhecimento em torno da expressão pecuniária de dados pessoais é elemento de extrema importância, mas é apenas o começo da possibilidade de solução de o problema igual relevância: o uso de dados pessoais como instrumento de indução comportamental da sociedade e os seus efeitos sobre os indivíduos⁹⁸ como reflexo do seu impacto na conformação das relações de poder⁹⁹.

Não se pode olvidar, todavia, da existência de doutrina nacional que, a partir de interpretação ampliativa do Código de Defesa do Consumidor, sob o influxo do princípio da finalidade do tratamento dos dados pessoais (art. 6º, I da LGPD), se manifesta pela impossibilidade da comercialização de bancos de dados de consumidores¹⁰⁰.

têm um alto valor econômico. Entretanto, como mostram as substanciais margens de lucro de muitas empresas de TI que se (co)financiam por intermédio da exploração de dados, o acesso aos dados pode ser muito lucrativo em termos econômicos e muitas vezes é". HOFFMANN-RIEM, **Teoria geral do direito digital: transformação digital: desafios para o direito**, p. 104.

⁹⁸A propósito, para Zuboff (em livre tradução): “esta concorrência para vender com certeza produz os imperativos econômicos que impulsionam as práticas comerciais. Por fim, ficou claro que os dados mais preditivos provêm da intervenção em nossas vidas para sintonizar e conduzir nosso comportamento em direção aos resultados mais lucrativos. Os cientistas de dados descrevem isto como uma mudança do monitoramento para a atuação. A ideia não é apenas conhecer nosso comportamento, mas também moldá-lo de forma que possa transformar previsões em garantias. Já não basta automatizar os fluxos de informação sobre nós; o objetivo agora é nos automatizar.” ZUBOFF, Shoshana. *It’s not that we’ve failed to rein in Facebook and Google*”. In: ZUBOFF, Shoshana, **It’s not that we’ve failed to rein in Facebook and Google. We’ve not even tried**, the Guardian. Disponível em: <<http://www.theguardian.com/commentisfree/2019/jul/02/facebook-google-data-change-our-behaviour-democracy>>. Acesso em: 21 abr. 2021.

⁹⁹RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 35.

¹⁰⁰ Nesse sentido, Doneda: “(...) cabe verificar que na doutrina podemos encontrar propostas para uma interpretação de caráter expansivo da normativa do Código de Defesa do Consumidor, de forma a identificar a presença dos princípios de proteção de dados pessoais que se comunicam a outras situações. Assim, por exemplo, entende-se a existência do princípio da finalidade, por intermédio da aplicação da cláusula da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo qual os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que motivaram a sua coleta – o que pode servir como fundamentação para o reconhecimento de um princípio de vedação da coleta de dados sensíveis e da comercialização de bancos de dados de consumidores”. In: DONEDA, Danilo, **Da privacidade à proteção de dados pessoais [livro eletrônico]**, 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

No plano internacional, Rodotà considera que a proteção de dados seria manifestação de direito da personalidade e não propriedade e, sob essa compreensão, certas categorias de dados, como os de natureza médica e genética, não seriam negociáveis¹⁰¹.

Calha destacar que o tema guarda compatibilidade com o escopo da LGPD, sendo certo que a ausência de dispositivo regulamentando o assunto, não implica na inexistência do fenômeno e, tampouco, na impossibilidade de se lhe conferir tratamento jurídico.

Essas ponderações guardam correlação com o tratamento de dados com base no legítimo interesse uma vez que, conforme se examinará ao longo do trabalho, há influência direta na finalidade que se atribui ao tratamento e, também, quanto ao processamento de dados realizados por terceiros.

1.1.3. O reconhecimento de um direito fundamental

Para a doutrina especializada, mesmo diante da atualidade e da relevância da matéria, os sistemas jurídico-positivos de diversos Estados não preveem de modo expresso o direito fundamental à proteção de dados¹⁰².

O reconhecimento e a incorporação do direito fundamental à proteção de dados têm se dado de forma paulatina nos diferentes ordenamentos jurídicos.

Na seara internacional, a Declaração Universal dos Direitos Humanos de 1948 (artigo 12º)¹⁰³ e a Convenção para a proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950 (artigo 8º, 1)¹⁰⁴ trazem em seu corpo dispositivos cuja exegese permite extrair o direito à proteção de dados.

¹⁰¹ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 19.

¹⁰² A propósito, consoante menciona Ingo Sarlet: “(...) já no limiar da terceira década do século XXI, ainda existem Estados constitucionais onde um direito fundamental à proteção de dados não é reconhecido, pelo menos na condição de direito expressamente positivado na Constituição – como se dá, em caráter ilustrativo, com a Alemanha (a despeito da longeva tradição regulatória na área) e o Brasil –, muito embora tal direito seja, em vários casos, tido como implicitamente positivado e vinculado ao assim *designado* direito à autodeterminação informativa, sem prejuízo de uma mais ou menos ampla regulação legislativa e administrativa”. *In*: SARLET, **Fundamentos constitucionais: O direito fundamental à proteção de dados**, p. 41.

¹⁰³ ORGANIZAÇÃO DAS NAÇÕES UNIDAS, ONU, **Declaração Universal dos Direitos Humanos**. Disponível em: <<https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>>. Acesso em: 15 fev. 2021.

¹⁰⁴ CONSELHO DA EUROPA. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais**. Disponível em: <https://www.echr.coe.int/documents/convention_por.pdf>. Acesso em: 15 fev. 2021.

A partir da Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (Capítulo II, artigo 4 e seguintes)¹⁰⁵ de 1981, se positivaram princípios básicos concernentes à proteção de dados.

Posteriormente, na Carta de Direitos Fundamentais da União Europeia de 2000, se reconheceu expressamente a condição de direito fundamental da proteção de dados (artigo 8º)¹⁰⁶.

Portanto, a partir de perspectiva histórica, se pode perceber que a proteção de dados vem ganhando destaque em nível global, principalmente no que diz respeito a países ocidentais. Nessa toada, o direito não é imune a interferências recíprocas, de sorte que essa tendência tem sido bem recebida pela doutrina e legisladores pátrios.

Com efeito, o cenário tecnológico muda ao lado do jurídico-institucional e o reconhecimento de novos direitos, derivados da dignidade da pessoa humana, a partir do progresso científico é uma reação do direito à eventual obsolescência das soluções jurídicas até então existentes que podem não ser suficientes para a adequada proteção do cidadão do novo milênio¹⁰⁷.

No que diz respeito ao conteúdo, sob o enfoque material, a densidade das posições relevantes para o direito impostas pela ordem jurídica ao titular expressa a fundamentalidade de um determinado direito. Já sob o prisma formal, deve-se observar as prescrições do texto constitucional¹⁰⁸.

¹⁰⁵ CONSELHO DA EUROPA. **Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais de 28 de janeiro de 1981**. Disponível em: <<https://www.coe.int/en/web/conventions/full-list>>. Acesso em: 15 fev. 2021.

¹⁰⁶ PARLAMENTO EUROPEU. **Carta de Direitos Fundamentais da União Europeia**. Disponível em: <[https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218(01)&from=EN)>. Acesso em: 15 fev. 2021.

¹⁰⁷ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 44.

¹⁰⁸ Ingo Sarlet ensina que “O marco distintivo principal, contudo, da condição de direito fundamental prende-se a dois elementos, ou, caso se prefira, está ancorado em dois esteios, quais sejam, a fundamentalidade em sentido material e a fundamentalidade em sentido formal. A fundamentalidade em sentido material (aqui a ponte para com os direitos humanos) guarda direta relação com a relevância do conteúdo das posições subjetivas atribuídas pela ordem jurídica a determinado sujeito de direitos, isto é, a determinado titular, visto que, no sentido formal, um direito é tido como fundamental de acordo com o nível de robustez das garantias estabelecidas pelo constituinte. Dito de outro modo, é o regime jurídico-constitucional reforçado que qualifica um direito fundamental como tal, regime que pode variar de acordo com as peculiaridades de cada ordem constitucional. Esse regime jurídico (garantias), por sua vez, implica que os direitos fundamentais correspondam a posições jurídicas oponíveis pelo indivíduo contra o Estado, no sentido daquilo que se convencionou chamar de trunfos contra a maioria (Dworkin), ou seja, posições jurídicas que, pela sua relevância na perspectiva do poder constituinte, encontram-se, por força da própria constituição originária, subtraídas à plena disposição pelos poderes públicos (Alexy)”. *In*: SARLET, **Fundamentos constitucionais: O direito fundamental à proteção de dados**, p. 46.

Cumpra esclarecer que a privacidade se relaciona à proteção de dados, mas com ela não se confunde.

A proteção de dados surgiu a partir do amadurecimento da tutela da privacidade e é certo que ambos os conceitos, embora não se ignore a dificuldade de uniformidade doutrinária sobre seu conteúdo, dialogam entre si, embora possuam âmbitos de proteção distintos.

A primeira possui caráter mais amplo (abrange quaisquer elementos de informação que digam respeito aos indivíduos) e dinâmico (demanda comportamentos ativos e negativos do Estado e dos cidadãos) do que a segunda, não podendo ser encarada como seu mero desdobramento.

Assim, a proteção de dados seria direito fundamental autônomo e estreitamente ligado à proteção da personalidade¹⁰⁹⁻¹¹⁰.

Nessa senda, o livre desenvolvimento da personalidade é indissociável da proteção de dados e ambos estão correlacionados à autodeterminação informativa como corolário do princípio da dignidade da pessoa humana.

A previsão normativa expressa do direito à proteção de dados no texto constitucional se revela interessante sob o prisma de sua instrumentalização jurídica, porquanto diminui o ônus argumentativo daqueles que pretendem utilizar esse direito autônomo como fundamento para implementação de políticas públicas, formulação de pleitos judiciais ou elaboração de decisões jurisdicionais.

Outrossim, o arranjo institucional decorrente de seu fundamento de validade ser extraído diretamente da Constituição Federal, tem o condão de irradiar efeitos negativos (limite à atuação normativa do legislador ordinário) e positivos (possibilidade de se exigir do Estado comportamentos ativos com fundamento no direito fundamental à proteção de dados). Nesse sentido, Ingo Sarlet¹¹¹:

Mesmo que se possa, como já tem sido o caso, reconhecer a proteção de dados como um direito fundamental implícito, daí extraindo todas as consequências atinentes a tal condição, o fato é que sua positivização 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.

Dentre as razões que aqui poderiam ser colacionadas, destacam-se:

¹⁰⁹ Para Sarlet, "o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade". *Ibid.*, p. 51.

¹¹⁰ No mesmo sentido, Leonardo Bessa e Ana Nunes, para quem: "a proteção de dados pessoais é direito fundamental uma vez que integra os direitos da personalidade". *In*: BESSA, Leonardo Roscoe; NUNES, Ana Luisa Tarter, Instrumentos processuais de tutela individual e coletiva: análise do art. 22 da LGPD, *in*: **Tratado de Proteção de Dados Pessoais**, Rio de Janeiro: Forense, 2021, p. 669.

¹¹¹ SARLET, Fundamentos constitucionais: O direito fundamental à proteção de dados, p. 55–56.

- a) a despeito das interseções e articulações com outros direitos, fica assegurada à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio;
- b) ao direito à proteção de dados passa a ser atribuído de modo inquestionável o pleno regime jurídico-constitucional relativo ao seu perfil de direito fundamental em sentido material e formal já consagrado no texto da CF, bem como na doutrina e na jurisprudência constitucional brasileira, ou seja:
 - 1) como parte integrante da constituição formal, os direitos fundamentais possuem status normativo superior em relação a todo o restante do ordenamento jurídico nacional;
 - 2) na condição de direito fundamental, assume a condição de limite material à reforma constitucional, devendo, ademais disso, ser observados os assim chamados limites formais, circunstanciais e temporais, nos termos do art. 60, §§ 1.º a 4.º, da CF;
 - 3) também as normas relativas ao direito à proteção de dados são – nos termos do art. 5.º, § 1.º, da CF – dotadas de aplicabilidade imediata (direta) e vinculam todos os atores públicos, bem como – sopesadas as devidas ressalvas, consoante será tratado em tópico específico – os atores privados.

Quanto ao seu objeto, cabe fazer breve distinção entre os conceitos de informação e dados. Um não se confunde com o outro.

Os dados não possuem qualidade intrínseca. É dizer: isoladamente considerados, não são nada além de um potencial registro sobre algo ou alguém. De outro lado, a informação é o resultado da correlação de dados, a partir de determinado contexto.

Em suma, os dados são elementos destituídos de sentido os quais, quando processados e contextualizados¹¹², se convolam em informação¹¹³.

Por não se tratar do objeto do presente estudo, é importante esclarecer que inexiste a pretensão de exaurimento da discussão. Embora não se ignore a controvérsia existente em torno

¹¹² Para Stefano Rodotà, "(...) nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou pelas outras informações às quais tem sido associada". *In: RODOTÀ, A vida na sociedade da vigilância: a privacidade hoje*, p. 78.

¹¹³ De acordo com Marion Albers: “[o]s conceitos de ‘dados’ e ‘informação’ são definidos de maneiras multifárias e dependentes da respectiva disciplina. No contexto (social) da proteção de dados, é ao menos importante dar-se conta de que dados e informação não são sinônimos. Esses termos devem, pelo contrário, ser diferenciados rigorosamente. Dados podem ser descritos como caracteres gravados em um suporte de dados, incluindo documentos escritos ou vídeos, bem como dados armazenados digitalmente em discos rígidos ou dispositivos móveis de armazenamento. Os dados, as formas de armazenamento e as operações de processamento são caracterizados pelas várias mídias, tecnologias e redes. Devido à sua objetificação, os dados podem ser concebidos de modo distinto e oferecem um ponto de partida para a regulamentação jurídica. Não obstante, os dados não são significativos em si mesmos, e sim como “informação em potencial”. Seu conteúdo informacional não é um atributo intrínseco dos próprios dados. Ele só é criado por meio de interpretação no contexto particular da interpretação. A informação implica sentido, e informações avulsas são elementos de sentido. Unidades de informações podem se basear em dados (ou em observações ou comunicações), mas os dados só adquirem sentido ao serem explicados e interpretados por quem recebe ou usa os dados para obter informação. A elaboração de sentido depende das condições situacionais individuais para a interpretação e do contexto do conhecimento e da interpretação. A informação depende do contexto de uma maneira elementar. Embora essa percepção talvez esteja bem estabelecida atualmente, as pessoas dificilmente percebem as dificuldades que isso acarreta para a regulamentação legal e para uma descrição do objeto a ser regulamentado”. *In: ALBERS, Marion, A complexidade da proteção de dados, Revista Brasileira de Direitos Fundamentais & Justiça*, v. 10, n. 35, p. 19–45, 2016, p. 30.

da amplitude do conteúdo dos direitos fundamentais (posições jurídicas¹¹⁴), se parte da premissa de que a proteção de dados, direito fundamental, pode ser compreendida a partir de dimensão subjetiva e objetiva.

É possível se extrair a dimensão subjetiva desse direito por meio da leitura da própria LGPD (art. 17 e seguintes) que, ao elencar os direitos dos titulares, estabelece uma série de deveres dirigidos aos agentes de tratamento¹¹⁵.

No que concerne à dimensão objetiva, um direito fundamental, enquanto manifestação jurídica de valor prevalecente em determinada sociedade, deve ter seu conteúdo essencial preservado com base no seu significado para aquele corpo social¹¹⁶.

Ainda sobre o assunto, destaque-se que a LGPD não contempla, de modo expreso, o cognominado "direito ao esquecimento", de sorte que o direito fundamental à proteção de dados não poderia servir de fundamento para a implementação de uma pretensão cuja base seja o direito ao esquecimento, principalmente diante de recente manifestação do Supremo Tribunal Federal que fixou a seguinte tese, em sede de Repercussão Geral (Tema: 786): “[é] incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expresas e específicas previsões legais nos âmbitos penal e cível”¹¹⁷.

Em relação à titularidade, os arts. 1º e 5º da LGPD deixam claro que a pessoa natural seria o titular do direito à proteção de dados pessoais. No ponto, se mostra relevante expor a

¹¹⁴ ALEXY, Robert, **Teoria dos direitos fundamentais**, 5. ed. São Paulo: Malheiros, 2008.

¹¹⁵ A propósito, para Sarlet: “[t]itular do direito, notadamente na perspectiva da dimensão subjetiva dos direitos e garantias fundamentais, é quem figura como sujeito ativo da relação jurídico-subjetiva, ao passo que destinatário é a pessoa (física, jurídica ou mesmo ente despersolaizado) em face da qual o titular pode exigir o respeito, proteção ou promoção de seu direito”. In: SARLET, Ingo Wolfgang, **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**, 10. ed. Porto Alegre: Livraria do Advogado, 2009, p. 208.

¹¹⁶ Para Virgílio Afonso da Silva, "isso significaria dizer que proteger o conteúdo essencial de um direito fundamental implica proibir restrições à eficácia desse direito que o tornem sem significado para todos os indivíduos ou para boa parte deles" SILVA, Virgílio Afonso da, **Direitos Fundamentais: conteúdo essencial, restrições e eficácia**, 2. ed. São Paulo: Malheiros, 2009, p. 185.

¹¹⁷ BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário nº 1.010.606**, Relator: Min. Dias Toffoli. Publicação 20 mai. 2021. Disponível em: <<http://stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>>. Acesso em 17 jun. 2021.

existência de entendimento doutrinário mais abrangente no sentido de se considerar a pessoa jurídica como titular de certos direitos da personalidade¹¹⁸⁻¹¹⁹, dentre eles a privacidade, o que poderia permitir uma evolução para a titularidade do direito à proteção de dados. Todavia, para os fins do presente trabalho, o aspecto primordial a ser considerado é o reconhecimento da proteção de dados como direito fundamental e sua matriz constitucional.

Quanto aos destinatários do direito, pode-se dizer que todos devem tratar os dados de terceiros com os quais se tenha contato de forma diligente.

O art. 1º da LGPD estabelece que o referido diploma "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado" e, no art. 3º se deixa clara aplicabilidade da norma a "qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados". Todavia a própria lei estabelece no mesmo dispositivo os requisitos para sua incidência, bem como prevê hipóteses de não incidência (art. 4º). Para Sarlet, os destinatários do direito tanto seriam o Estado quanto os particulares¹²⁰.

Consoante já exposto, não há como se negar a sua correlação com princípio da dignidade da pessoa humana. Neste passo, é inequívoca a necessidade de se procurar lhe conferir máxima eficácia e mínima constrição.

Portanto, intervenções no direito à proteção de dados devem ser sujeitas a amplo controle, ainda que em momento distinto da efetiva intromissão, no intento de se minimizar a possibilidade de objetificação do indivíduo¹²¹.

¹¹⁸ PEREIRA, Daniel Queiroz, Direitos da personalidade e pessoa jurídica: uma abordagem contemporânea, **Revista da Faculdade de Direito da UERJ**, v. 2, n. 22, p. 1–20, 2012.

¹¹⁹ DE ANDRADE, Fábio Siebeneichler, A tutela dos direitos da personalidade no direito brasileiro em perspectiva atual, p. 32, 2013.

¹²⁰ Pondera o autor que “[d]estinatários do direito (vinculados pelo direito) são tanto o Estado quanto os particulares, pois a devassa da vida privada, incluindo o acesso e a utilização de dados pessoais, é algo que atualmente decorre tanto de ações (ou, a depender do caso, de omissões) de órgãos e agentes estatais quanto das de entidades privadas ou pessoas físicas”. *In*: SARLET, Fundamentos constitucionais: O direito fundamental à proteção de dados, p. 68.

¹²¹ A propósito, para Ricardo Maurício Freire Soares: “(...) a dignidade da pessoa humana identifica um núcleo de integridade física e moral a ser assegurado a todas as pessoas por sua existência no mundo, relacionando-se tanto com a satisfação espiritual quanto com as condições materiais de subsistência do ser humano, vedando-se qualquer tentativa de degradação ou coisificação do ser humano em sociedade”. *In*: SOARES, Ricardo Maurício Freire, **O princípio constitucional da dignidade da pessoa humana em busca pelo direito justo**, São Paulo: Saraiva, 2010, p. 142.

Cumpra destacar, ainda, que o sujeito não pode ser considerado mera fonte de dados. Deve haver o fortalecimento de sua posição jurídica através da estruturação de mecanismos de sindicabilidade do tratamento de dados a seu respeito.

Neste passo, é preciso se reconhecer em âmbito nacional, dentro da tábua de valores do modernos ordenamentos jurídicos, o direito fundamental à proteção de dados como garantia do pleno desenvolvimento da personalidade e, *a fortiori*, como garantia da liberdade e democracia¹²²⁻¹²³, primando-se pela harmonia do sistema, sob pena de se inviabilizar seu amadurecimento enquanto instituto jurídico e se dificultar o desenvolvimento das relações sociais que, a partir da LGPD, passaram a receber, de modo mais intenso, a atenção do Estado.

Sob o prisma da evolução jurisprudencial, no plano internacional, pode-se mencionar como paradigma a decisão do Tribunal Constitucional Federal da Alemanha (*Bundesverfassungsgericht*), em 1983, que declarou inconstitucional lei de recenseamento de população, profissão, moradia e trabalho em razão de sua vagueza e amplitude.

A Corte alemã reconheceu a autodeterminação informativa como direito autônomo e de fundo constitucional. Essa decisão é dotada de peculiar importância na medida em que atribuiu caráter constitucional ao direito à proteção de dados e conferiu aos indivíduos o direito subjetivo de ter controle sobre o tratamento de dados a seu respeito.

Observe-se que se partiu dos direitos da personalidade para se garantir ao cidadão o direito de controlar a extensão da utilização ou enunciação de qualquer aspecto relacionado à sua privacidade por meio do manejo de seus dados pessoais¹²⁴⁻¹²⁵. O tratamento de dados, então, passou a ser compreendido sob perspectiva funcionalizada¹²⁶.

¹²² RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 58.

¹²³ “Os cientistas de dados estão brincando com nossas vidas como se fossem deuses infantis, agarrando-se a tudo o que veem como se fosse deles. Eles têm se movimentado rapidamente e quebrado as coisas, como vidas, nossa capacidade de nos concentrarmos em uma coisa de cada vez, e democracias”. *In*: VÉLIZ, **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**, p. 112.

¹²⁴ DONEDA, Danilo, Panorama histórico da proteção de dados pessoais, *in*: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 28.

¹²⁵ No mesmo sentido, Laura Mendes, para quem: “(...) opera-se na dogmática e na prática jurídica uma clara evolução no direito à privacidade (Rodotà, 2008, p. 17). Primeiramente, ele passa a ser compreendido como um fenômeno coletivo, na medida em que os danos causados pelo processamento impróprio de dados pessoais são, por natureza, difusos, exigindo igualmente uma tutela jurídica coletiva. Em segundo lugar, a privacidade, antes compreendida como o direito negativo de ser deixado em paz (*right to be let alone*), passa a significar também o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular (BVerfG 65, 1, Censo Demográfico). Por fim, a privacidade, antes ligada exclusivamente a um ideal de liberdade, passa a se vincular também a outros direitos fundamentais, como a igualdade, em razão do crescente risco de discriminação pelo Estado e pelo mercado”. MENDES, Laura Schertel, O direito Fundamental à proteção de dados pessoais, **Revista de Direito do Consumidor**, v. 20, n. 79, 2011, p. 52.

¹²⁶ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**.

No âmbito jurídico-positivo interno brasileiro, antes da aprovação da PEC 17/2019¹²⁷, a proteção constitucional dos dados pessoais era extraída a partir de interpretação sistemática de dispositivos que versam sobre dados (art. 5º, X, XII e LXXII) e, também, de documentos transnacionais que reconhecem à proteção de dados pessoais a qualidade de direito fundamental¹²⁸.

Após modificações elaboradas pela Câmara dos Deputados¹²⁹, em outubro de 2021 foi aprovada em dois turnos pelo Senado Federal Proposta de Emenda Constitucional, promulgada pelo Congresso Nacional em 10 de fevereiro de 2022 como Emenda Constitucional nº 115¹³⁰, que, dentre outras modificações no texto constitucional, “estabeleceu, em comando específico (o novo inciso LXXIX do art. 5º), a proteção dos dados pessoais como direito individual”¹³¹.

Essa alteração é positiva, pois além de reduzir o ônus argumentativo daqueles que desde antes lhe atribuíam estatura constitucional, a previsão expressa, no texto da Constituição, do direito à proteção dos dados pessoais, na forma estabelecida, lhe confere a característica de direito fundamental autônomo dotado de aplicabilidade direta e imediata, aplicável, portanto, a todos, inclusive, ao próprio Estado.

Além disso, de sua autonomia, similarmente ao que ocorre com o direito do consumidor, decorre espectro de proteção próprio e o seu diferenciado status normativo viabiliza sua

¹²⁷ No primeiro texto, antes do final aprovado em ambas as casas, se acrescentaria “o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria”. BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 17 jul. 2020.

¹²⁸ Artigo 8º da Carta dos Direitos Fundamentais da União Europeia, artigo 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) e Considerando 1 do Regulamento Geral sobre a Proteção de Dados (RGPD).

¹²⁹ A matéria foi devolvida ao Senado Federal em razão de mudanças ocorridas no âmbito da Câmara dos Deputados. In: BRASIL, Câmara dos Deputados, **Câmara aprova em 2º turno PEC que inclui a proteção de dados pessoais na Constituição - Notícias**, Portal da Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/noticias/801696-camara-aprova-em-2o-turno-pec-que-inclui-a-protecao-de-dados-pessoais-na-constituicao/>. Acesso em: 31 ago. 2021.

¹³⁰ Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

¹³¹ De acordo com o Parecer de relatoria da Senadora Simone Tebet, “[a] redação da PEC nº 17, de 2019, aprovada pela Câmara dos Deputados, fez apenas duas alterações no texto deliberado por esta Casa. A primeira, mero ajuste de forma, estabeleceu, em comando específico (o novo inciso LXXIX do art. 5º), a proteção dos dados pessoais como direito individual, ao invés de tratar essa proteção no mesmo mandamento que garante ao indivíduo a inviolabilidade de suas comunicações (inciso XII do art. 5º). A segunda modificação, de mérito, atribuiu à União as competências de organizar e fiscalizar a proteção e o tratamento de dados pessoais, de acordo com a lei. Mantiveram-se inalteradas, portanto, a previsão da competência privativa da União para legislar sobre a matéria e a cláusula de vigência da proposta”. BRASIL. Senado Federal. **Parecer nº 242 de 2021-PLEN/SF**, Rel. Senadora Simone Tebet, p. 2. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9029060&ts=1634767663452&disposition=inline>. Acesso em 21 out. 2021.

instrumentalização, em ordem a se fortalecer o arquétipo da proteção de dados previsto pelo legislador na Lei 13.709/2018.

No que tange às manifestações do Poder Judiciário pátrio, o Supremo Tribunal Federal, ao se pronunciar diretamente sobre o tema, em algumas oportunidades, entendeu que os dados em si considerados não receberiam proteção constitucional, mas tão-somente a sua comunicação¹³², sendo, então, imperiosa uma correta compreensão da abrangência do disposto no art. 5º, XII, da CRFB¹³³.

O referido entendimento se amparou em texto doutrinário de autoria de Tércio Sampaio Ferraz Júnior¹³⁴. As ideias principais desse artigo que levaram à construção da orientação jurisprudencial que se firmou, em um primeiro momento, no Supremo Tribunal Federal foram: a) o sigilo seria um instrumento e não um fim em si mesmo, de sorte que seria marcado pela “assessoriedade”¹³⁵; b) o objeto do direito à inviolabilidade do sigilo (previsto no art. 5º, XII, da CRFB) seria a comunicação¹³⁶; c) haveria distinção entre dados em trânsito (art. 5º, XII, da Constituição Federal) e dados armazenados (art. 5º. X); e d) a “integridade moral do sujeito” seria o objeto do direito à privacidade, de sorte que a exploração dos elementos de identificação do indivíduo é que deveria ser alvo de condicionantes normativas.

¹³² BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário nº 418.416**. [...] IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). Relator: Min. Sepúlveda Pertence. Publicação: 19/12/2006. Disponível em <https://jurisprudencia.stf.jus.br/pages/search/sjur92577/false>. Acesso em: 20 jul. 2020.

¹³³ BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus nº 91.867**. [...] 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados [...]. Relator: Min. Gilmar Mendes. Segunda Turma. Publicação: 20/09/2012. Disponível em https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22HC%2091867%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 20 jul. 2020.

¹³⁴ JÚNIOR, Tércio Sampaio Ferraz, Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 88, p. 439–459, 1993.

¹³⁵ *Ibid.*, p. 444.

¹³⁶ *Ibid.*, p. 447.

Essa orientação dogmático-jurisprudencial prevaleceu por mais de dez anos na Suprema Corte, até que, no ano de 2020, sobreveio a Medida Provisória nº 954/2020, adotada pelo Presidente da República, a qual dispunha sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19), de que trata a Lei nº 13.979¹³⁷.

De acordo como Chefe do Poder Executivo do Brasil, para a elaboração e implementação de políticas públicas destinadas ao enfrentamento da pandemia decorrente do covid-19, seria necessário se franquear ao Instituto Brasileiro de Geografia e Estatística (IBGE) “acesso a informações sobre o número de telefone e respectivo endereço residencial dos consumidores de serviços de telecomunicações, de pessoas naturais ou jurídicas”¹³⁸ abrangidos pela Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua).

Ações diretas de inconstitucionalidade foram propostas por diversas entidades, autuadas sob os n.ºs 6.387, 6.388, 6.389, 6.390 e 6.393¹³⁹, as quais foram julgadas conjuntamente.

De acordo com o relatório elaborado pela Ministra Rosa Weber, os promoventes argumentaram, quanto ao aspecto nomoestático, em síntese, que a norma impugnada: a) violaria dados sigilosos de todos os brasileiros; b) teria finalidade genérica e imprecisa; c) estabeleceria a guarda dos dados pelo IBGE, sem referência à possibilidade de controle e fiscalização pelo Poder Judiciário, pelo Ministério Público ou outros órgãos da sociedade civil; d) não haveria precisão na descrição da modalidade, frequência e objetivos das pesquisas que seriam realizadas; e) careceria das razões de urgência e relevância da medida; f) impescindiria da apresentação de razões justificantes da necessidade do compartilhamento de dados para a pesquisa estatística; g) seria silente sobre a adoção de mecanismo de segurança que salvaguardasse os dados coletados de riscos de acesso e uso indevidos; e h) a previsão de

¹³⁷ BRASIL. Poder Executivo. **Medida Provisória nº 954 de 17 de abril de 2020**. Brasília, DF, Diário Oficial da União de 17 abr. 2020 – edição extra.

¹³⁸ BRASIL. Ministério da Economia. **Exposição de motivos nº 00151/2020**. Brasília, DF, 15 abr. 2020.

¹³⁹A ADI nº 6.387 foi proposta pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB; ADI nº 6.388 pelo Partido da Social Democracia Brasileira (PSDB); ADI nº 6.389 pelo Partido Socialista Brasileiro (PSB); ADI nº 6.390 pelo Partido Socialismo e Liberdade (P-SOL) e ADI nº 6.393 pelo Partido Comunista do Brasil (PC do B).

elaboração de relatório após o uso dos dados, e não previamente ao compartilhamento, fragilizaria a efetiva avaliação dos riscos¹⁴⁰.

Na oportunidade do julgamento colegiado, o Supremo Tribunal Federal, em sua composição plenária, reconheceu, por maioria e de modo expreso, a proteção de dados pessoais como direito fundamental distinto da intimidade e privacidade, o qual retira seu fundamento de validade diretamente da Constituição Federal.

¹⁴⁰ BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade nº 6.387**. Rel. Min. Rosa Weber. Ementa: MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *FUMUS BONI JURIS. PERICULUM IN MORA*. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais não de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam “adequados, relevantes e não excessivos em relação a esse propósito” e “conservados apenas pelo tempo necessário.” (artigo 45, § 2º, alíneas “b” e “d”). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpra as exigências que exsurtem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. *Fumus boni juris* e *periculum in mora* demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true>. Acesso em: 9 dez. 2020.

Vale menção ao raciocínio desenvolvido pelo Ministro Gilmar Mendes que constatou o direito fundamental da proteção de dados pessoais a partir de uma compreensão sistemática do texto constitucional. Para o magistrado, o direito fundamental à dignidade da pessoa humana (fundamento da república, art. 1º, III), a proteção da intimidade (insculpida no art. 5º, X) e a centralidade do *habeas data* (previsto no art. 5º, LXXII, todos da CRFB), enquanto instrumento de defesa do direito à autodeterminação informativa, permitiriam desvelar dentro do sistema constitucional positivo direito fundamental autônomo e mais abrangente do que o direito ao sigilo¹⁴¹.

A mudança de entendimento da Corte em relação ao tema veio em momento oportuno, porquanto próxima à entrada em vigor da LGPD.

Nesse trilhar, considera-se que a decisão da Corte Constitucional brasileira certamente estimulará a realização no plano fático das disposições previstas nesse diploma normativo.

Essa manifestação do Estado-juiz contribui para o delineamento de arranjo institucional capaz de resguardar os titulares de dados de utilizações que ultrapassam as finalidades da coleta.

Em adição ao aspecto formal, é oportuno se destacar o seu caráter simbólico na medida em que se pode concluir que a Suprema Corte, instada a se manifestar, mais uma vez reconheceu a posição de centralidade da pessoa dentro da estrutura constitucional, sendo certo que a proteção de dados, enquanto manifestação da personalidade, carece de tutela jurídica adequada¹⁴².

A Corte, sensível à força construtiva dos fatos sobre o direito e amparada na posição destacada dos indivíduos no sistema jurídico constitucional¹⁴³, viabilizou, no que diz respeito à proteção de dados, a construção de caminhos hermenêuticos que permitem aos interessados

¹⁴¹ Em seu voto, o Ministro Gilmar Mendes destacou que “a autonomia do direito fundamental em jogo na presente ADI exorbita, em essência, de sua mera equiparação com o conteúdo normativo da cláusula de proteção ao sigilo. A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa”. BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade nº 6.387**, p. 109. Acesso em: 9 dez. 2020.

¹⁴² Para Rafael Zanatta e outros, “(...) o reconhecimento do status constitucional da proteção de dados configura uma conquista institucional fundamental, tanto pela força formal do precedente, quanto pelo seu simbolismo. E até pela mensagem que deixa registrada para os atores brasileiros sobre o tratamento de dados durante uma pandemia: a de que o Tribunal reconhece e privilegia a centralidade da proteção de dados nas sociedades contemporâneas, bem como a sua relação com o cumprimento de garantias constitucionais individuais e coletivas”. In: ZANATTA *et al*, **Os Dados e o Vírus**, p. 250.

¹⁴³ FACHIN, **Direito Civil sentidos, transformações e fim**.

exercer controle permanente e direto sobre os sujeitos a quem as informações fornecidas tendem a fortalecer a assimetria de poder já existente¹⁴⁴.

Assim, de forma similar ao Tribunal Constitucional alemão, que em 1983 reconheceu o direito fundamental à autodeterminação informativa a partir dos direitos fundamentais à dignidade humana e ao livre desenvolvimento da personalidade, o STF assegurou à proteção dos dados pessoais envergadura constitucional, conferindo tutela abrangente a esse elemento da personalidade dos indivíduos e, ao mesmo tempo, consignou a necessidade de ampliação da proteção para além do seu conteúdo de direito material, alcançando, também, as possibilidades e finalidades de seu processamento¹⁴⁵.

Ainda no ano de 2020, em outra oportunidade, a Corte Constitucional brasileira, no exame da medida cautelar na ADI 6.529, ao conferir interpretação conforme ao artigo 4º da Lei 9.883/99, estabeleceu que os órgãos integrantes do Sistema Brasileiro de Inteligência (Sisbin) somente estariam autorizados a fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) diante de comprovado interesse público.

O Plenário do Supremo Tribunal federal estabeleceu que: a) aos órgãos componentes do Sistema Brasileiro de Inteligência seria permitido apenas o fornecimento de dados específicos à Abin mediante comprovação do interesse público, afastada qualquer possibilidade de satisfação de interesses individuais dissociados da impessoalidade que deve reger a Administração Pública; b) qualquer manifestação no sentido de pedido de dados deverá ser precedida de motivação, cuja legalidade é plenamente sindicável pelo Poder Judiciário; c) a caracterização do interesse público não possui o condão de permitir o compartilhamento de dados albergados pela cláusula da reserva de jurisdição; d) deve haver procedimento formal no qual se documente os registros de acesso, inclusive para fins de responsabilização na hipóteses de abuso¹⁴⁶.

¹⁴⁴ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 37.

¹⁴⁵ Conforme destacado por Laura Mendes e outros: “[a]o fazer referência ao julgado, o STF expressamente mencionou o conceito de autodeterminação informativa, já positivado na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), a fim de ressaltar o necessário protagonismo exercido pelo cidadão no controle do que é feito com seus dados. Assim, pôs-se em destaque a existência de finalidades legítimas para seu processamento, bem como da necessidade de implementação de medidas de segurança para tanto”. In: MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da; JÚNIOR, Otavio Luiz Rodrigues, **O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo**, in: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 85.

¹⁴⁶ Em outubro de 2021 o julgamento foi concluído e “por unanimidade, confirmando cautelar deferida pelo Plenário do Supremo Tribunal, conheceu parcialmente da ação direta e deu interpretação conforme ao parágrafo

Assim, para o STF, o dever de motivação, bem como a adoção de procedimento formal com registro de acesso a dados de inteligência, deve ser rigorosamente observado pela Abin no exercício de sua competência no que concerne aos pedidos de informações "para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais".

Ademais, deve ser viabilizado o controle de legalidade pelo Poder Judiciário. Também é relevante observar a vedação ao compartilhamento de dados obtidos em processos judiciais, em razão de sua aquisição se dar mediante a limitação de direitos fundamentais para finalidades pré-determinadas em lei.

Há que se deixar claro que não há vedação entre o compartilhamento de informações entre órgãos públicos, principalmente quanto se fazem presentes interesses nacionais e o postulado da presunção de legalidade e legitimidade dos atos públicos. A própria LGPD prevê a possibilidade desse compartilhamento, mesmo quando se cuide de dados pessoais.

O obstáculo ao compartilhamento acontece com a finalidade de se inviabilizar comportamentos não republicanos, daí a importância da adoção de procedimento formal e a necessidade de motivação clara e expressa quanto ao pedido de informações.

Com efeito, embora esse *decisum* não faça referência à LGPD, a possibilidade de controle da atuação dos agentes de tratamento com garantia da exatidão e do uso correto dos dados, se revela como instrumento de promoção do equilíbrio nas relações entre o Estado e o particular, bem como nas relações interprivadas.

O tema tangencia o tratamento de dados e o reconhecimento de sua essência de direito fundamental se revela de particular importância, pois se cuida de um pressuposto lógico para a irradiação de efeitos em relação ao ordenamento jurídico brasileiro como um todo, com reflexos

único do art. 4º da Lei n. 9.883/1999 para estabelecer que: a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso. Tudo nos termos do voto da Relatora. Plenário, Sessão Virtual de 1.10.2021 a 8.10.2021". BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade nº 6.529**. Relatora: Min. Cármen Lúcia. Publicação: 22 out. 2021. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837>>, acórdão pendente de publicação. Acesso em 21 out. 2021.

diretos no dia a dia das pessoas, empresas e governos, máxime se considerado que se cuida do direito mais expressivo da condição humana contemporânea¹⁴⁷.

Hoje o fluxo informacional se dá na perspectiva "pessoa-informação-circulação-controle", e não mais apenas "pessoa-informação-sigilo"¹⁴⁸. Ao titular dos dados deve ser garantida a possibilidade de efetivo controle sobre as informações a seu respeito e não apenas fazer cessar eventual circulação disfuncional de informações.

Dessarte, o pleno desenvolvimento da personalidade, sob o influxo da dignidade da pessoa humana, é valor constitucional que serve de alicerce ao reconhecimento do direito fundamental autônomo da proteção de dados¹⁴⁹ e, nessa medida, regras sobre os mecanismos de processamento de dados possuem o condão de estabelecerem balizas objetivas para a aferição legitimidade para a tomada de medidas que potencialmente se caracterizem como intrusão indevida na esfera individual dos titulares dessa posição jurídica.

A proteção de dados, enquanto direito fundamental, conquanto não possa ser subordinada a nenhum outro direito¹⁵⁰, também está sujeita a limites e restrições e, portanto, não se cuida de direito absoluto, valendo a advertência de Sarlet no sentido da plena aplicabilidade da teoria dos limites dos limites ao direito à proteção de dados¹⁵¹.

Quanto à possibilidade de relativização do princípio da proteção de dados, é evidente a imprescindibilidade da preservação de sua essência sem se prejudicar o próprio fluxo informacional.

Com efeito, a óptica supraindividual deve ser considerada e, também, necessitam ser sopesados outros bens jurídicos igualmente protegidos. Inclusive, é possível que o próprio

¹⁴⁷ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 19.

¹⁴⁸ *Ibid.*, p. 93.

¹⁴⁹ Para Bruno Bioni, “[a] tutela jurídica dos dados pessoais é um imperativo que impõe uma nova fronteira aos direitos da personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana e, por tabela, ao livre desenvolvimento de sua personalidade. Por isso, o direito à proteção dos dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera “evolução” do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação”. *In: BIONI, Proteção de dados pessoais a função e os limites do consentimento*, p. 92.

¹⁵⁰ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 18.

¹⁵¹ Para o autor, “(...) embora seja o direito à proteção de dados submetido a limites e passível de restrições, acionam-se, também nesse caso, os assim chamados limites aos limites dos direitos fundamentais, dentre os quais desponta a necessária observância dos critérios da proporcionalidade e da salvaguarda do núcleo essencial, o que se aplica seja qual for a origem e natureza da intervenção estatal (judiciária, administrativa e legislativa) na esfera de proteção do direito à proteção de dados”. *In: SARLET, Fundamentos constitucionais: O direito fundamental à proteção de dados*, p. 73.

detentor da posição jurídica tenha interesse em pontualmente flexibilizar a proteção de seus dados na intenção de alcançar situação jurídica que julgue mais favorável a si¹⁵².

Releva notar, também, que apesar da necessidade de abertura da ordem constitucional à inovação técnica, não basta a mera atribuição de estatura constitucional a esse direito. Mostra-se imprescindível o correto delineamento da amplitude desse bem jurídico, afastadas orientações reducionistas que dificultem o seu amadurecimento.

Os princípios insculpidos na LGPD¹⁵³ conferem maior densidade jurídica a esse novo direito fundamental ao estabelecerem parâmetros legais que possibilitam o escrutínio do tratamento dos dados realizado pelos agentes e viabilizam a possibilidade de concretização de sua proteção, especialmente através da positivação dos princípios da boa-fé, da finalidade, da transparência e da prevenção de danos em virtude do tratamento de dados pessoais.

A abordagem que se fez até aqui é relevante para a compreensão do legítimo interesse, uma das bases legais para o tratamento de dados, na medida em que, no transcurso da evolução do direito de ser deixado só para o direito a controlar o uso que terceiros fazem das informações a respeito dos indivíduos (autodeterminação informativa), densifica-se o papel do titular dos

¹⁵²Nesse sentido, Albers, para quem “[o] raciocínio sobre a razão pela qual e até que ponto a pessoa em questão deve ser protegida precisa, pelo contrário, provir de uma perspectiva supraindividual, a saber, assumindo-se uma visão categorizadora do contexto e das consequências adversas a serem esperadas em relação à pessoa à qual se referem os dados, as informações e o conhecimento. O mero fato de que uma informação avulsa se refere a uma pessoa ainda não implica a necessidade de proteção de uma pessoa. A necessidade de proteção surge, em particular, em relação aos efeitos negativos do tratamento dos dados pessoais e das informações obtidas a partir dele. Os bens juridicamente protegidos e os mecanismos de violação ou ingerência exigem seus próprios padrões separados de descrição. Além disso, a proteção direcionada unicamente à defesa contra o processamento de dados pessoais e ao impedimento desse processamento é insuficiente. A pessoa protegida também pode ter interesse em que dados pessoais sejam disponibilizados de modo que um órgão ou agência tenha à sua disposição as informações de que necessita para tomar uma decisão correta”. *In: ALBERS, A complexidade da proteção de dados*, p. 34.

¹⁵³ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: 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; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; 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; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

dados como sujeito ativo na relação jurídico-subjetiva de tratamento, possibilitando-se-lhe exigir, a todo tempo, a observância da Constituição e do sistema de proteção de dados e assim resguardar seus direitos e liberdades.

O legítimo interesse, conforme se demonstrará, é hipótese de processamento de dados marcada por elevado grau de subjetividade, assim, uma compreensão constitucionalmente adequada da proteção de dados deve partir do reconhecimento do caráter autônomo desse direito. Eventuais situações de tensão devem ser solucionadas a partir de visão sistemática e do reconhecimento da posição de centralidade do indivíduo se determinar seu sentido e alcance.

1.2. As gerações de leis de proteção de dados

Oportuno, também, se mostra o estudo das gerações de leis de proteção de dados a fim de se compreender como a evolução do direito à privacidade influenciou a conformação da atual dimensão do direito fundamental à proteção de dados e, também, se situar a LGPD dentro dessa evolução.

Em clássico artigo a respeito da tutela da privacidade, Samuel D. Warren e Louis D. Brandeis propõem, a partir de precedentes extraídos do sistema da *common law*, a necessidade de o direito se adequar às modificações sociais proporcionadas pela tecnologia e, sob a óptica da privacidade, estabelecem a necessidade de o indivíduo ter o poder de decidir sobre quais aspectos de sua vida pode ser dada publicidade, fazendo emergir a existência de um direito, autônomo e carecedor de tutela específica, desvinculado do direito à propriedade¹⁵⁴.

Os autores concluíram que a tutela da privacidade não pode se consubstanciar em óbice à publicização daquilo que se considerasse interesse geral. De igual sorte, pontuais flexibilizações desse direito, funcionalizadas dentro de determinado sistema jurídico, não poderiam ser consideradas ilegais.

Quanto às formas de vulneração da esfera jurídica dos interessados, se faria necessário o exame casuístico, podendo-se estabelecer previamente que não se poderia falar em responsabilidade diante da ausência de dano no caso concreto e, uma vez caracterizada a violação ao direito, ainda que verdadeira a informação, não se poderia afastar a

¹⁵⁴ WARREN; BRANDEIS, **The Right to Privacy**.

responsabilização da conduta, nem mesmo a ausência de dolo. Em contrapartida, a demonstração da existência de consentimento excluiria a possível lesão à privacidade¹⁵⁵.

Assim, em um primeiro momento, conferiu-se a esse direito densidade marcadamente individual, concebido como um direito de índole negativa e limite à atuação do Estado. Todavia, as mudanças das relações sociais permitiram-lhe atribuir matiz supraindividual e a proteção de dados advém do amadurecimento do tratamento jurídico dado à privacidade.

Conquanto a expressão “proteção de dados” pareça enfatizar a tutela de fragmentos de informação a respeito das pessoas, o que se protege é o sujeito a quem os dados se relacionam¹⁵⁶.

Com efeito, o movimento incessante dos dados pessoais potencializa o aspecto dinâmico de sua proteção, na medida em que interesses econômicos usualmente tendem a diminuir espaços de privacidade e a compreensão das formas de materialização desse fenômeno propicia a elaboração de moldura jurídica protetiva dos titulares, em especial no que diz respeito ao combate de práticas discriminatórias¹⁵⁷.

Examinando-se a evolução normativa do tema em diversos países europeus, é possível se falar em gerações de leis de proteção de dados, de acordo com estudo realizado por Viktor Mayer-Schönberger¹⁵⁸.

Na primeira geração, desenvolvida durante a década de 1970, houve profusão de leis que predominantemente versavam sobre a concessão de autorização para a criação de bancos de dados e o seu controle posterior pelos órgãos públicos. O foco dessas leis é o processamento de dados em si, deixando o conteúdo das informações e a discussão em torno da privacidade para o segundo plano.

Para Mayer-Schönberger, o enfoque dado pelas normas de primeira geração se concentraria no funcionamento do processamento de dados na sociedade, mais distantes do indivíduo e mais dirigidas ao controle das tecnologias até então disponíveis e utilizadas¹⁵⁹.

¹⁵⁵ Nesse sentido, por oportuno, vale transcrever a compreensão de Laura Schertel Mendes sobre o referido texto: “Warren e Brandeis, ao identificarem o direito à privacidade, buscam igualmente definir os seus limites, nos seguintes termos: (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 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 também não exclui a violação desse direito (1890, p. 12-14)”. *In*: MENDES, O direito Fundamental à proteção de dados pessoais. p. 49

¹⁵⁶ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 99.

¹⁵⁷ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**.

¹⁵⁸ MAYER-SCHÖNBERGER, Viktor, *Generational development of data protection in Europe*, *in*: **Technology and Privacy: The New Landscape**, Cambridge: MIT Press, 1998.

¹⁵⁹ *Ibid.*, p. 222.

Demais disso, o Estado, destinatário de grande volume de informações coletadas, deveria ter seu poder de processamento de informações limitado.

Ainda, para o autor, os estatutos de primeira geração evitaram o uso de vocábulos como “privacidade” e “informação”, tendo optado por terminologia técnica, a exemplo de expressões tais como “dados” e “bancos de dados”¹⁶⁰.

De acordo com Doneda, essa "primeira geração de leis vai, aproximadamente, até a *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais de 1977"¹⁶¹.

No que diz respeito à segunda geração, ainda durante a década de 1970, o eixo normativo são os direitos individuais relacionados à privacidade. A evolução da tecnologia e a proliferação dos sujeitos aptos a lidarem com os dados coletados evidenciou a inviabilidade do controle dessa atividade unicamente pelo Estado através do sistema de autorizações em razão da impossibilidade de ser realizado o acompanhamento adequado e na profundidade necessária.

Os riscos antevistos não se circunscreviam à detenção de informações a respeito dos indivíduos pelo Estado. A multiplicação de processamento de dados por milhares de computadores também se consubstanciaria em aspecto mitigador da privacidade dos sujeitos¹⁶².

A saída encontrada, então, foi incluir o indivíduo, fonte desses dados, entre os agentes incumbidos da tarefa de controle.

Destarte, a proteção de dados pessoais passou a ser tratada como liberdade negativa, a ser exercida pelo próprio interessado que deveria fiscalizar o uso das suas informações pessoais e, também, buscar os meios de proteção adequados.

Diminuiu-se o uso de jargões técnicos e os conceitos utilizados foram mais abstratos e menos ligados ao estado da arte tecnológica daquele momento histórico. A tutela dos dados pessoais foi robustecida por meio da legitimação jurídica de mais um agente fiscalizador e promotor de sua proteção, o titular¹⁶³.

Pode-se dizer, então, que nas legislações de segunda geração houve a aproximação entre privacidade e proteção de dados.

A terceira geração, desenvolvida durante a década de 1980, traz normas relativas à dinâmica das relações sociais e reconhece o fornecimento de dados pessoais pelos indivíduos

¹⁶⁰ *Ibid.*, p. 224.

¹⁶¹ DONEDA, Danilo, A proteção dos dados pessoais como um direito fundamental, *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91–108, 2011. p.96.

¹⁶² MAYER-SCHÖNBERGER, *Generational development of data protection in Europe*, p. 226.

¹⁶³ DONEDA, *A proteção dos dados pessoais como um direito fundamental*.p.97

como pressuposto para a vida plena em sociedade e para o seu desenvolvimento enquanto ser humano, de sorte que a não entrega dessas informações traz como consequência a exclusão, em qualquer grau, da vida em coletividade.

As normas de terceira geração atribuem ao indivíduo a posição de centralidade e, além disso, ampliam sua esfera protetiva, uma vez que a tutela das informações pessoais se dá contextualmente e se busca estabelecer meios de proteção fundados em caráter principiológico.

Abandonou-se o tortuoso caminho de constante adaptação da legislação às mudanças sociais tecnológicas por meio da adoção de larga base principiológica e conceitos razoavelmente abertos. Permitiu-se, assim, a adaptação das leis às novas realidades, de modo que o transcurso do tempo não se caracterizasse como elemento distanciador dos fatos e as respectivas normas de regência¹⁶⁴. Fala-se, ainda, no princípio da autodeterminação informativa.

Nas leis de quarta geração, reconhece-se a desproporcionalidade de se deixar sob exclusiva responsabilidade dos sujeitos, a quem, em linha de princípio, cabe o consentimento ou a recusa à coleta de dados por terceiros.

Ao mesmo tempo em que se reconhece a autodeterminação informativa, há preocupação quanto à tutela da informação em si considerada. Isso é implementado através do fortalecimento da posição da pessoa diante dos agentes que tratam seus dados, bem como por meio da criação de autoridades, dotadas de algum grau de independência, com competência para fiscalizar a aplicação e o cumprimento da lei pelos atores sociais. De acordo com Doneda¹⁶⁵:

Muito sinteticamente, esses marcos regulatórios reconhecem os dados pessoais e o seu tratamento como fenômenos juridicamente relevantes, estabelecendo direitos e garantias para os cidadãos, limites para a sua utilização por empresas e organizações e mecanismos que procuram reduzir o risco proporcionado pelo tratamento de dados. Esses elementos são organizados de forma a proporcionar maior controle e proteção ao cidadão sobre seus dados, indo além de uma abordagem vinculada meramente à proteção da privacidade e, ainda, têm como uma de suas consequências mais importantes a consolidação de espaços dentro dos quais os dados pessoais possam ser tratados lícitamente, proporcionando garantias para utilizações legítimas de dados pessoais e fomentando espaços de tratamento e livre fluxo de dados. (...)

As mais recentes legislações na área já incorporam instrumentos que procuram responder a essas novas demandas. Nelas, percebe-se que a manutenção dos instrumentos individuais de garantia convive cada vez mais com uma abordagem regulatória baseada no risco; que elementos organizacionais que privilegiam a demonstração de cumprimento com os parâmetros legais, em uma lógica de *accountability*, são sempre mais presentes; que alguns instrumentos que originalmente sequer pareceriam estar relacionados com a tutela da privacidade cada vez mais encontram um espaço natural para desenvolvimento nas legislações de proteção de

¹⁶⁴ MAYER-SCHÖNBERGER, **Generational development of data protection in Europe**, p. 230.

¹⁶⁵ DONEDA, **Panorama histórico da proteção de dados pessoais**. P. 22.

dados, como é o caso das normas sobre transparência, os limites às decisões automatizadas ou aquelas referentes à portabilidade de dados pessoais.

Assim, parece não haver dúvidas que está delineado novo conceito jurídico, de importância global, o qual se vincula ao livre desenvolvimento da personalidade e, portanto, carecedor de tutela específica, consistente e adequada por parte do Estado.

A subdivisão das legislações em gerações não pode implicar a sua compreensão compartimentalizada, como se não houvesse comunicação entre cada uma. Em verdade, se pode perceber a constante evolução das normas a partir do desenvolvimento das relações sociais e da incessante busca de se operacionalizar o livre fluxo informativo sem esvaziar a posição jurídica dos titulares de dados.

A LGPD contempla conceitos técnicos e atribui, também, e não somente, ao indivíduo a tarefa de exercer o controle sobre a coleta e utilização de seus dados. Ademais, expressamente prevê a autodeterminação informativa como fundamento (art. 1º, II) e a não discriminação como princípio (art. 6º, IX). Assim, parece se situar na quarta geração de leis e isso se reveste de importância na medida em que a compreensão da matéria deve se pautar pela edificação de arcabouço normativo-dogmático que, à luz das disposições normativas, seja capaz de, a um só tempo, potencializar o “livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais”¹⁶⁶ e ostente a capacidade de se adaptar força disruptiva das constantes mudanças sociais.

1.3. A Lei Geral de Proteção de Dados e o paradigma do consentimento

É certo que o legislador foi prolixo ao dispor sobre as hipóteses de tratamento de dados e isso reflete preocupação genuína com a matéria, antes de se apontar redundância ou atecnia.

Previamente ao aprofundamento do estudo sobre a disciplina do legítimo interesse na LGPD, cabe a enunciação de alguns conceitos trazidos pela própria lei¹⁶⁷ que são relevantes para a adequada compreensão do raciocínio que será desenvolvido.

Destarte, o titular dos dados é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”; controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”; operador: “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”; agentes de tratamento: “o controlador e o operador”;

¹⁶⁶ Art. 1º, VII, da LGPD

¹⁶⁷ A LGPD, em seu art. 5º, traz diversos conceitos que são utilizados ao longo de todo o diploma normativo.

tratamento: “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização. Acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”; relatório de impacto à proteção de dados pessoais: “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”¹⁶⁸.

Quanto ao regime jurídico, o art. 7º, *caput*, da LGPD prevê regra geral de que não pode haver tratamento de dados sem uma base legal que o fundamente e as hipóteses legais de tratamento são extraídas a partir do exame dos artigos 4º, 7º e 11¹⁶⁹ desse diploma normativo.

¹⁶⁸ Art. 5º, I, V, VI, IX, X e XVII, da LGPD.

¹⁶⁹ Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Fala-se no princípio da proibição do tratamento dissociado de substrato normativo, o qual preconiza que todo tratamento de dados, para ocorrer, precisa de base jurídico-positiva, não sendo suficiente para sua realização a simples manifestação de vontade de quem coleta e processa esses elementos de informação¹⁷⁰.

Logo, para que o tratamento de dados seja considerado lícito, primeiramente se deve perquirir se a situação é tutelada pela LGPD. Posteriormente, escolher uma das hipóteses legais estabelecidas, de forma cumulada ou não¹⁷¹, seguir-se a principiologia da LGPD e as regras estabelecidas na lei, devendo-se observar, inclusive, as disposições que por venturam sejam elaboradas em âmbito infralegal¹⁷².

Da leitura dos dispositivos mencionados, é possível antever que as hipóteses de tratamento de dados pessoais podem ser agrupadas em três blocos: a) tratamento de dados com base no consentimento; b) tratamento de dados com base no interesse público ou cumprimento de obrigação legal ou regulatória; e c) tratamento de dados com base no legítimo interesse.

No mesmo sentido, Bessa fundamenta a referida divisão ao propor que a proteção de dados, enquanto direito da personalidade disponível, torna razoável a adoção da vontade do titular como forma legitimadora do tratamento desses dados (Art. 7º, I, da LGPD). De outro lado, não se cuida de direito absoluto. Portanto, o legislador pode restringir esse direito e permitir, em algumas situações, o processamento de dados (v.g. lei que pontualmente autorize ou determine o tratamento de dados pessoais em certas hipóteses) e isso pode se dar no seio na

¹⁷⁰ Segundo Indra Döhmman, “[e]sse princípio da proibição também deve ser sempre entendido no sentido de que o tratamento lícito para determinadas finalidades e de determinada maneira não significa necessariamente que qualquer outro tratamento segundo a vontade do agente de tratamento dos dados fosse admissível. O titular dos dados continua sendo o ponto de referência para todo e qualquer tratamento adicional. Por conseguinte, devem-se recusar concepções como a da “soberania sobre os dados”, que considera suficiente uma justificação inicial para a primeira transmissão de dados por parte do titular deles, ou de uma transparência substitutiva referente a todos os outros tratamentos de dados sem outras restrições”. In: DÖHMANN, Indra Spiecker Gen., A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia, in: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 120.

¹⁷¹ Viola e Teffé se posicionam pela possibilidade de cumulação de fundamentos de licitude. Nesse sentido: “(...) não sendo uma hipótese de exclusão, deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito, sendo possível inclusive cumular as mesmas, assim como no GDPR. Essas bases foram estipuladas de forma geral e variada, devendo detalhes e adequações ser realizados especialmente pela Autoridade Nacional de Proteção de Dados (ANPD), pelo Legislativo e pelo Judiciário”. In: VIOLA, Mário; TEFFÉ, Chiara Spadaccini de, Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o E 11, in: **Tratado de Proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 131.

¹⁷² Para Viola e Teffé: “(...) não sendo uma hipótese de exclusão, deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito, sendo possível inclusive cumular as mesmas, assim como no GDPR. Essas bases foram estipuladas de forma geral e variada, devendo detalhes e adequações ser realizados especialmente pela Autoridade Nacional de Proteção de Dados (ANPD), pelo Legislativo e pelo Judiciário”. In: TEFFÉ; VIOLA, **Tratamento de dados pessoais na LGPD**, p. 131.

própria LGPD ou em outras normas (CDC, por exemplo). Essas seriam o segundo grupo de hipóteses de tratamento (art. 7º, II, III, IV, V, VI, VIII e X, da LGPD). Ainda, o legislador, com base no princípio da proporcionalidade, pode atribuir ao intérprete a possibilidade de restrição contextual e pontual do direito à proteção de dados. Essa seria a hipótese pertencente à terceira categoria de processamento dos dados (art. 7º, IX, da LGPD)¹⁷³.

Assim, o tratamento de dados pessoais somente pode se dar dentro das referidas bases legais e, caso realizado fora desses parâmetros, sujeita o agente de tratamento às sanções previstas na norma.

A lei prevê hipóteses nas quais o tratamento tem por base o consentimento, ainda que indiretamente, e, também, situações que não dependem da vontade do titular dos dados.

Nesse contexto, ao optar pelo dispositivo que fundamentará a atividade de tratamento, o controlador deve observar as proposições permissivas presentes na LGPD, bem como a finalidade do tratamento e a situação concreta, sendo descabido estabelecer uma relação de primazia entre um ou outro permissivo legal.

O consentimento, via de regra, é o fundamento de licitude mais utilizado em razão da segurança que confere ao agente de tratamento. Todavia, por vezes, os requisitos previstos em lei para a sua obtenção não são realizáveis no caso concreto, consoante sucedeu durante a pandemia decorrente do COVID-19, na qual diversas entidades não sabiam exatamente qual base legal adotar para tratar dados relativos à doença e outras pesquisas¹⁷⁴.

Em situações como a acima mencionada, a melhor alternativa parece ser a que se defende no presente trabalho no sentido de se reconhecer a ausência de hierarquia entre as bases legais e se permitir ao agente de tratamento a escolha daquela que lhe pareça mais adequada, dentre elas o legítimo interesse.

Quando do escrutínio do tratamento pela autoridade nacional de proteção de dados ou pelos respectivos titulares, de forma organizada ou não, é que se verificará o efetivo cumprimento dos requisitos legais e, eventualmente, se aplicará o regime de responsabilidade previsto na LGPD.

¹⁷³ BESSA, Leonardo. **Lei de Proteção de Dados #1: Prof. Leonardo Bessa**. Youtube, 28 set. 2020. Disponível em: < <https://youtu.be/5clK12I2zdk>>. Acesso em: 20 out. 2021.

¹⁷⁴ CIPL, Centre for Information Policy Leadership, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation**, Washington-London-Brussels: Hunton Andrews Kurth, 2021, p. 6.

1.3.1. A possibilidade de reconhecimento do microsistema de proteção de dados

A LGPD estabelece como objetivo a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (titular dos dados)¹⁷⁵.

O legislador, ciente da necessidade de se robustecer o sistema protetivo dos titulares de dados, positivou a possibilidade de diálogo entre as disposições da LGPD e outros direitos e princípios previstos no ordenamento jurídico pátrio, ou mesmo em tratados internacionais, relacionados à matéria¹⁷⁶.

Cuida-se de previsão profícua na medida em que amplia o espectro de proteção da pessoa construído dentro do que se pode chamar de microsistema de proteção de dados. A referida regra torna viável, inclusive, a aplicação de institutos reconhecidos pelo ordenamento jurídico, ainda que tacitamente, embora não tenham sido desenvolvidos com vistas à proteção de dados.

É certo que a positivação da possibilidade de diálogo entre os direitos e princípios estatuídos na LGPD e em outros diplomas diminui sobremaneira o ônus argumentativo do intérprete que pretende potencializar o efeito útil do sistema mediante essa operação interpretativa, além de o reconhecimento formal dessa possibilidade atuar como mecanismo de indução espontânea dos agentes coletores à adequação de seu comportamento às prescrições legislativas¹⁷⁷.

Ainda que fosse ausente a previsão legal, a interpretação do sistema de proteção de dados, permeado por princípios e cláusulas gerais, à luz dos valores consagrados constitucionalmente, conduziria o aplicador do direito à possibilidade de se referenciar outros diplomas normativos como fontes de normas aplicáveis à proteção de dados sob o influxo da teoria do diálogo das fontes¹⁷⁸.

¹⁷⁵ Art. 1º, LGPD.

¹⁷⁶ Art. 64, LGPD.

¹⁷⁷ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 67.

¹⁷⁸ Nesse sentido, para Cláudia Marques: “[d]iálogo das fontes’ é a expressão visionária do grande mestre Erik Jayme. Pela força da Constituição (e dos Direitos Fundamentais), fontes plurais não mais se excluem – ao contrário, mantêm as suas diferenças e narram simultaneamente suas várias lógicas (dia-logos), cabendo ao aplicador da lei coordená-las (“escutando-as”), impondo soluções harmonizadas e funcionais no sistema, assegurando efeitos úteis a essas fontes, ordenadas segundo a compreensão imposta pelo valor constitucional”. MARQUES, Cláudia Lima, *Diálogo das fontes, aplicação das normas e teoria do direito: a teoria do diálogo das fontes hone no Brasil e seus novos desafios: uma homenagem à magistratura brasileira*, in: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Orgs.), **Diálogo das fontes: novos estudos sobre a coordenação e aplicação das normas no direito brasileiro [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2020.

Neste cenário, o direito fundamental à proteção dos dados pessoais deve ser resguardado sob diferentes ângulos e a abertura normativa já estabelecida pelo legislador parece ser o caminho para, dentro da moldura principiológica da LGPD, se "priorizar a harmonia e a coordenação entre as normas do ordenamento jurídico (concebido como sistema unitário) e a 'coerência derivada ou restaurada' (*cohérence dérivée* ou *restaurée*), que se fará pelo 'diálogos' (uso das várias lógicas)"¹⁷⁹.

Assim, deve-se buscar, na maior medida possível, se conferir efetividade às imposições constitucionais. A partir dessa diretriz hermenêutica, a coordenação das leis protetivas dos indivíduos através de sua conexão sistêmica se mostra como o *ethos* a ser preservado com a finalidade de se observar os fundamentos insculpidos na Constituição Federal, em especial o da dignidade da pessoa humana¹⁸⁰.

Essas ponderações permitem pressupor que o diálogo de coordenação e adaptação sistemática de aplicação autorizam a "redefinição do campo de aplicação"¹⁸¹ do Código de Defesa do Consumidor à LGPD em reforço desse novo microsistema protetivo e assim se garantir o "efeito útil"¹⁸² de ambas as leis.

Consoante já mencionado, usualmente, o tratamento de dados não é o produto a ser entregue ao destinatário final, mas pressuposto para a fruição de determinado bem ou serviço¹⁸³. A título ilustrativo, menciona-se a obrigatoriedade de disponibilização do número de cadastro de pessoa física para aquisição de remédio em drogarias ou mesmo a adesão a termos de contrato para utilização de serviços prestados por meio da internet.

Deveras, a dependência crescente entre o fornecimento de informações e uso de serviços ou aquisição de bens obscurece os limites da privacidade, ao mesmo tempo que se evidencia a assimetria de poder entre os fornecedores desses bens da vida e as pessoas que pretendem adquiri-los.

¹⁷⁹ *Ibid.*

¹⁸⁰ Art. 1º, III, da Constituição Federal.

¹⁸¹ MARQUES, **Diálogo das fontes, aplicação das normas e teoria do direito: a teoria do diálogo das fontes hoje no Brasil e seus novos desafios: uma homenagem à magistratura brasileira.**

¹⁸² *Ibid.*

¹⁸³ Para Guilherme Mucelin: "(...) podemos seguramente afirmar que, na pós-modernidade, onde tudo é hiperconectado e os "dados pessoais chegam a fazer as vezes da própria pessoa", diálogo das fontes também é conexão, necessária e essencial, para além das "lógicas tradicionais", a qual valoriza as inovações e suas duas lógicas, o analógico e o tecnológico, e que se traduz na visualização holística do mundo contemporâneo e das relações nas quais os sujeitos se inserem, colocando a pessoa – na sua inteireza – no centro da transformação digital, sem descuidar de suas vulnerabilidades e de seus direitos". *In*: MUCELIN, Guilherme, Transformação digital e diálogo das fontes: a interface jurídica de proteção das pessoas entre o virtual e o analógico, *in*: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Orgs.), **Diálogo das fontes: novos estudos sobre a coordenação e aplicação das normas no direito brasileiro [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2020.

Essa disparidade precisa ser diminuída acaso se pretenda materializar o objetivo de livre desenvolvimento da personalidade. Assim, a LGPD e o CDC são diplomas legislativos que convergem para a mesma finalidade: proteção da pessoa humana, consumidor ou titular de dados.

Sob essa perspectiva, cabe referência à “dupla face que a tutela da dignidade da pessoa humana assume em relação ao tratamento de informações”¹⁸⁴, na medida em que os bens da vida almejados pelo titular têm por pressuposto, não raras vezes, o processamento de seus dados mediante a flexibilização do direito à privacidade.

A aproximação entre essas leis se mostra relevante pois se pode atribuir ao titular de dados, desde o início da vigência da LGPD, a condição de vulnerável¹⁸⁵ e assim lhe garantir tratamento adequado aproveitando-se o amadurecimento doutrinário e jurisprudencial que acompanha os 30 (trinta) anos de vigência do Código de defesa do Consumidor¹⁸⁶.

Esse entendimento é possível. Inclusive, a teoria do diálogo das fontes é aceita no âmbito das cortes superiores. A propósito, "a evolução da teoria foi muito interessante e é grande o potencial (re-) ou (i)novador da aplicação, interpretação das leis e integração das lacunas sob esse método. Considerando que a ADIN 2.591 terminou em 2006 no STF e a primeira citação no STJ é de 2005"¹⁸⁷.

Portanto, essa valorização ético-legislativa do titular de dados pessoais, independentemente da sua condição de consumidor no caso concreto, se revela como chave hermenêutica capaz de conduzir a construção racional do microsistema de proteção de dados.

1.3.2. O tratamento com base no paradigma do consentimento e a condição de vulnerável do titular de dados

Consoante já mencionado no presente trabalho, hoje, não é incomum que na aquisição de um bem ou serviço parte do pagamento seja a disponibilização de informações a respeito do adquirente.

¹⁸⁴ Leonardo Bessa identifica uma "dupla face que a tutela da dignidade da pessoa humana assume em relação ao tratamento de informações pelos bancos de dados de proteção ao crédito". Entende-se que o raciocínio pode ser aplicado à proteção de dados, uma vez que o art. 2º, V, da LGPD estabelece o "desenvolvimento econômico e tecnológico e a inovação" como um de seus fundamentos, evidenciando-se a tensão existente entre o "bem estar material", o livre fluxo de informações e a privacidade". *In*: BESSA, **Nova Lei do Cadastro Positivo: comentários à Lei 12.414, com as alterações da Lei Complementar 166/2019 e de acordo com a LGPD**, p. 58.

¹⁸⁵ RODOTÁ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 138.

¹⁸⁶ O Código de Defesa do Consumidor entrou em vigor no dia 11/03/1991.

¹⁸⁷ MARQUES, **Diálogo das fontes, aplicação das normas e teoria do direito: a teoria do diálogo das fontes hoje no Brasil e seus novos desafios: uma homenagem à magistratura brasileira**.

Parcela relevante dos serviços atualmente consumidos pela sociedade está atrelada, de modo geral, à concordância, por parte do usuário, a documentos, usualmente rotulados como "termos de uso", os quais se destinam a regular a relação jurídica entabulada entre o fornecedor e o interessado.

Essa espécie de avença é comum em produtos ofertados em nível global e a adoção de documentos padronizados viabiliza a sua distribuição e funcionamento a uma gama indefinida de usuários sujeitos a jurisdições distintas¹⁸⁸.

Na “sociedade dos serviços”, o elevado grau de padronização e a profusão de vínculos internacionais, segundo Rodotà, geram duas consequências: a) a contínua sofisticação das relações ocasiona maior entrega, pelos indivíduos, de dados nas mãos dos fornecedores; e b) quanto mais a rede de serviços se amplia, maiores são as possibilidades de interconexões entre bancos de dados e, portanto, de difusão, em nível global, das informações coletadas¹⁸⁹.

Desta sorte, a complexidade das relações que atualmente são construídas impõe uma melhor compreensão em torno da ideia do consentimento enquanto pressuposto para a coleta e tratamento legítimos de dados pessoais.

Mendes e Fonseca identificam aspectos que fragilizam o uso do consentimento como regra para o tratamento de dados, quais sejam: limitações cognitivas dos titulares de dados pessoais para sopesar a relação de custo-benefício relativa ao ato de fornecer elementos de informação e as repercussões em sua esfera individual; a existência de situações nas quais, faticamente, não se está diante de real liberdade de escolha do titular; e as modernas técnicas de tratamento e processamento de dados, em especial *Big Data*, que retiram a capacidade das pessoas de aferirem, no momento do consentimento, a amplitude da disponibilização dos dados¹⁹⁰.

Em relação ao primeiro obstáculo, o artigo 5º, XII, da LGPD dispõe que o consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

¹⁸⁸ Para Ramon Carneiro: “[t]rata-se, portanto, de mecanismo jurídico que visa viabilizar a oferta dos serviços a nível global, criando previsibilidade e segurança jurídica, resguardando o provedor de serviços online de uma série de limitações jurídicas existentes, como a responsabilidade pelo fato ou vício do produto ou do serviço, a diversidade de jurisdições competentes e de leis aplicáveis para o julgamento de eventuais litígios”. In: CARNEIRO, Ramon Mariano, “Li e aceito”: violações a direitos fundamentais nos termos de uso das plataformas digitais, *Internet & Sociedade*, v. 1, n. 1, 2020.

¹⁸⁹ RODOTÀ, *A vida na sociedade da vigilância: a privacidade hoje*, p. 100.

¹⁹⁰ MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da, *Proteção de dados para além do consentimento: tendências de materialização*, in: *Tratado de proteção de dados pessoais*, Rio de Janeiro: Forense, 2021, p. 95.

Com efeito, a minoria dos consumidores se predispõe a ler os termos de uso de serviços. Dentro desse espaço amostral, o número daqueles que compreendem o que foi lido é bem menor¹⁹¹, de modo que, sob essa perspectiva, é manifesta a limitação cognitiva.

Ao lado da limitação da capacidade de compreensão do destinatário da informação, há, também, a dificuldade intrínseca ao próprio conteúdo do documento mediante o qual se obtém consentimento, o qual, frequentemente, limita direitos fundamentais do consumidor sem se olvidar, ainda, da sua forma de apresentação.

Advirta-se que não se trata de retirar do titular dos dados a sua capacidade de pensar criticamente. Cuida-se de um olhar atento à realidade, porquanto o ato de disposição de informações usualmente não de adstringe ao titular e vai além da simples relação de aquisição de serviço ou bem.

Em verdade, a partir do acúmulo de informações sobre alguém é possível se construir perfis, inclusive a respeito de sujeitos que pertencem ao círculo social da fonte dos dados, mas que não forneceram, diretamente, elementos de informação sobre si.

A avaliação segura e consciente sobre os riscos e prejuízos decorrentes do consentimento, em especial na vida conectada a diversos serviços por meio da internet, é extremamente complexa e demanda tempo de análise que frequentemente desborda do que se espera do consumidor comum¹⁹².

Demais disso, deve-se buscar o ponto de equilíbrio entre excesso de informação e livre manifestação de vontade inequívoca de sorte que há estreita correlação entre consentimento e transparência¹⁹³.

No que diz respeito ao segundo obstáculo à adoção do consentimento como regra para a autorização do tratamento de dados, destaca-se o uso massivo de certos serviços que retiram

¹⁹¹ CALO, M. R., Against Notice Skepticism in Privacy (and Elsewhere), *Notre Dame Law Review*, v. 87, n. 3, p. 1027–1072, 2012, p. 1050.

¹⁹² Para Mendes e Fonseca: “(...) não se trata de simplesmente ‘infantilizar’ o titular dos dados, tratando-o como incapaz de decidir por si mesmo ou simplesmente ignorar sua capacidade racional. No entanto, o foco excessivo na obtenção de seu consentimento (aparentemente) informado deixa de lado algo mais complexo: a real capacidade do titular dos dados pessoais de substancialmente compreender e avaliar os riscos e prejuízos que poderão advir de seu consentimento, sobretudo on-line”. *In*: MENDES; FONSECA, **Proteção de dados para além do consentimento: tendências de materialização**, p. 96.

¹⁹³ Caio Lima pondera que: “(...) a transparência pode ser levada a efeito de diversas formas, tais como por escrito, áudio, vídeo, entre outros, sendo certo que em todas as situações deve ser utilizada: i) linguagem clara (evitando termos técnicos, ajustando o texto de acordo com o público-alvo); ii) linguagem direta e objetiva (evitando textos longos); e iii) a língua portuguesa (os documentos em outra língua devem ser traduzidos para o português, a fim de que tenham validade jurídica, conforme disposto no art. 224 do Código Civil)”. LIMA, Caio César Carvalho, *Estudo prático sobre as bases legais da LGPD*, *in*: **Proteção de dados - desafios e soluções na adequação à Lei**, Rio de Janeiro: Forense, 2020, p. 25.

do usuário sua real liberdade de escolha, pois acaso não concorde com as condições impostas pelo provedor do serviço, não terá como utilizá-lo. Cuida-se de situação caracterizadora de vulnerabilidade dos destinatários do serviço¹⁹⁴.

Assim, não pairam dúvidas de que condicionar o uso de produto ou serviço, não raro considerado indispensável e sem concorrente de igual nível, de interesse do titular de dados à disposição desproporcional de seus dados (a exemplo de elementos de informação dissociados da finalidade do uso do produto ou serviço)¹⁹⁵ enfraquece sobremaneira a manifestação livre do consentimento¹⁹⁶.

Já no que concerne ao terceiro óbice, qual seja o tratamento contextual de dados realizado por meio de avançados mecanismos de tratamento e correlação de fragmentos de informação dispersos obtidos por meio de diversas fontes, a exemplo de sistemas que se utilizam de *Big Data*, se revela imperiosa a imposição de limites e de possibilidade de controle desse tratamento.

¹⁹⁴ "Trata-se do cenário retratado por Spiros Simitis no qual o consentimento é meramente uma ficção, uma vez que o indivíduo carece de efetiva autonomia decisória para se proteger dos possíveis perigos e danos à sua personalidade. Nessas situações, a decisão individual de consentir não é livre e autônoma ou oriunda da avaliação dos ônus e dos bônus envolvidos. Ao revés, ela se origina de uma verdadeira imposição estabelecida por terceiro: consentir ou simplesmente não desfrutar de serviço/produto, que, muitas vezes, sob a perspectiva do indivíduo, é essencial para a sua sociabilidade ou acesso à informação na era digital". In: MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. **Proteção de dados para além do consentimento: tendências de materialização**. In: Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p..98.

¹⁹⁵ Menciona-se exemplo retirado do já citado texto de autoria de Caio César Carvalho Lima: "imagine a situação em que determinado titular, ao instalar aplicativo para acessar localização dos metrô em uma cidade, descobre que há obrigação, entre outras, de liberar o acesso à geolocalização do dispositivo, microfone, câmera de vídeo e fotos armazenadas, sob pena de não ter acesso à aplicação. À exceção da geolocalização, como os demais dados, em um primeiro momento, podem não ter direta correlação com o uso do aplicativo, a fim de garantir o consentimento livre, é importante que o titular dos dados tenha a possibilidade de optar se, de fato, deseja (ou não) ter esses dados tratados, não havendo nenhuma pressão no momento da sua coleta, especialmente porque o correto funcionamento do aplicativo não depende disso" (p.23).

¹⁹⁶ Hoffman-Riem aponta que "[o] Tribunal Constitucional Alemão também identificou este dilema e o formulou do seguinte modo: "Em todas as áreas da vida, serviços básicos para o público em geral estão sendo cada vez mais prestados por empresas privadas, muitas vezes poderosas, com base em extensas coletas de dados pessoais e medidas de processamento de dados. Os indivíduos dificilmente 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". HOFFMANN-RIEM, **Teoria geral do direito digital: transformação digital: desafios para o direito**, p. 97.

Essa capacidade de larga interligação entre dados aparentemente dispersos reforça a ideia de privacidade contextual¹⁹⁷, porquanto essa, considerada isoladamente, é incapaz de permitir a compreensão de todas as possibilidades de circulação de informações sobre os indivíduos. Na prática, o valor da informação advém do contexto no qual é coletada e tratada¹⁹⁸.

Portanto, a sujeição dos indivíduos a serviços prestados sob o modelo *take it or leave it* evidencia circunstância que retira do usuário, no momento da coleta, a capacidade de avaliar e decidir livremente sobre a repercussão presente e futura de determinada cessão pontual de informações a seu respeito e, *a fortiori*, ocasiona a perda da capacidade de controle sobre a dimensão do próprio perfil digitalmente existente¹⁹⁹, sua "biografia digital"²⁰⁰.

Doneda considera que o consentimento, no âmbito de proteção da LGPD, não pode ser considerado um negócio jurídico, mas, sim, manifestação de exercício de direito da personalidade²⁰¹. Afirma, ainda, que esse instituto deve ser compreendido à luz do princípio da autodeterminação dos dados pessoais, subdividindo-o em dois planos: a) autodeterminação; e b) legitimação do tratamento²⁰².

É certo que o consentimento é aspecto primordial, mas não se pode engessar a atuação do controlador e operador que devem ter a liberdade de utilizar os dados de maneira transparente e ética.

Pode-se falar, por oportuno, em “funcionalização do consentimento”²⁰³, na medida em que a sua interpretação deve partir do eixo principiológico insculpido pela própria LGPD.

¹⁹⁷ “(...) a privacidade como integridade contextual é uma teia complexa e delicada de restrições ao fluxo de informação pessoal que, por si só, traz equilíbrio a múltiplas esferas da vida social e política. Os sistemas e práticas que perturbam radicalmente esta teia de restrições não estão apenas a ameaçar um novato no palco dos valores e direitos, mas potencialmente pode romper o próprio tecido da vida social e política”. NISSENBAUM, Helen Fay, **Privacy in context: technology, policy, and the integrity of social life**, Stanford, Calif: Stanford Law Books, 2010, p. 128.

¹⁹⁸ Para Rodotà: “(...) nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou pelas outras informações às quais tem sido associada”. RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 77.

¹⁹⁹ Para Mendes e Fonseca: (...) seja pela escala em que a informação é processada, seja pela enorme capacidade de agregação da informação pelas novas tecnologias, é improvável que o indivíduo, no momento da coleta, gereencie plenamente algo que ocorrerá no futuro e que envolve inúmeras incertezas acerca de como todas as informações e dados acerca de um indivíduo serão agregados, cruzados ou utilizados. *In*: MENDES; FONSECA, **Proteção de dados para além do consentimento: tendências de materialização**, p.100.

²⁰⁰ SOLOVE, Daniel J., **The Digital Person: Technology and Privacy in the Information Age**, Rochester, NY: Social Science Research Network, 2004.

²⁰¹ Para o autor: O consentimento para o tratamento de dados pessoais toca diretamente em uma série de elementos da própria personalidade, ainda que não no sentido exato da disposição desses elementos. Ele assume com mais propriedade as vestes de um ato do titular cujo efeito será de autorizar um determinado tratamento para os dados pessoais. DONEDA, **Da privacidade à proteção de dados pessoais [livro eletrônico]**.

²⁰² *Ibid.*

²⁰³ *Ibid.*

Nesse cenário, o princípio da finalidade deve inviabilizar a possibilidade de consentimento indeterminado, o princípio da informação, por sua vez, deve resguardar tanto quem dá o consentimento quanto quem o obtém, de sorte que deve ser evidente o destinatário do dado, a finalidade e o período do tratamento, quem acessará os dados, a possibilidade de transmissão a terceiros “e mais tantos outros detalhes quanto sejam necessários em uma determinada situação para que o interessado possa formar sua convicção, livre e consciente, para realizar o ato de autodeterminação”²⁰⁴.

Há, ainda, outros posicionamentos doutrinários que merecem igual destaque e apontam a necessidade de interpretação restritiva do consentimento, tolhendo-se do agente de tratamento a possibilidade de extensão da autorização a ele concedida para outras formas de processamento não pactuadas²⁰⁵.

A propósito, é de se perceber que incumbe ao agente receptor dos dados o ônus da prova de demonstrar que obteve o consentimento de forma legítima e segundo as prescrições da LGPD (art. 8º, § 2º, da LGPD²⁰⁶).

Calha apontar, também, que o processamento de dados pessoais é atividade pautada pelo risco e o consentimento, conquanto manifestação revestida de absoluta importância²⁰⁷, pode não ser suficiente para legitimar a atuação do agente de tratamento, uma vez que as relações que são construídas são complexas não se podendo exigir do homem médio a plena consciência da amplitude, inclusive em relação a terceiros²⁰⁸, do ato de permitir a coleta e tratamento de seus dados.

²⁰⁴ *Ibid.*

²⁰⁵ Mário Viola e Chiara de Teffé destacam que “a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida a ele para o tratamento de dados para outros meios além daqueles pactuados, para momento posterior ou para finalidade diversa”. *In*: VIOLA, Mário; TEFFÉ, Chiara Spadaccini de, Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o E 11, *in*: **Tratado de Proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 134.

²⁰⁶ Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (...) § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

²⁰⁷ De acordo com Patrícia Peck Pinheiro: “(...) a necessidade do consentimento na coleta dos dados, principalmente no ambiente virtual, foi ganhando importância em razão da sensibilidade e vulnerabilidade que as informações pessoais foram adquirindo com o desenvolvimento da tecnologia. Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e a privacidade”. *In*: PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD)**, São Paulo: Saraiva Educação, 2018, p. 48

²⁰⁸ “(...) o consentimento abre a possibilidade prática para que as empresas que coletam e avaliam os dados possam invadir os direitos pessoais de terceiros, sem que estes últimos necessariamente estejam cientes disso e possam se proteger legalmente”. HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Trad. Ítalo Fuhrmann. Rio de Janeiro: Forense, 2021, p. 101.

Quanto à sua forma, nos termos do artigo 8º, *caput*, da LGPD, o consentimento deve ser fornecido por escrito, ou por outro meio que demonstre a manifestação de vontade do titular, para finalidade determinada, sendo consideradas nulas autorizações genéricas para o tratamento de dados pessoais²⁰⁹.

No que diz respeito à eficácia, adotada a premissa de que a proteção de dados é direito fundamental correlacionado aos direitos da personalidade, o consentimento é manifestação desvinculada de qualquer obrigação contratual. Doneda chama atenção para a sua plena revogabilidade e considera que a característica da indisponibilidade dos direitos da personalidade viabiliza a revogação do consentimento a qualquer momento pois se cuidaria de ato jurídico unilateralmente praticado pelo titular e de materialização da autodeterminação informacional²¹⁰.

No ponto, cumpre destacar que a LGPD contempla a possibilidade de revogação do consentimento a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado no art. 8º, § 5º²¹¹.

Desta sorte, à luz do exposto, não há como se estabelecer um conceito rígido sobre o sentido e alcance do consentimento na LGPD.

De outro lado, consoante preconizado pela própria norma sob estudo²¹², a proteção de dados não pode esvaziar o livre fluxo de informação e, tampouco, desestimular da atividade econômica.

É preciso que se empreste alguma ductibilidade a esse instituto a fim de se viabilizar a construção de diálogo hermenêutico permanentemente aberto entre leitor e texto a fim de se permitir o contínuo cotejo entre a adequação das normas regentes da matéria aos preceitos constitucionais e a realidade²¹³, bem como sua funcionalização a partir da confluência entre a disciplina jurídica do consentimento e os efeitos que dela são esperados²¹⁴.

²⁰⁹ Art. 8º, § 4º, da LGPD: o consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

²¹⁰ DONEDA, **Da privacidade à proteção de dados pessoais [livro eletrônico]**.

²¹¹ Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (...) § 5º 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.

²¹² Art. 2º, V, da LGPD.

²¹³ FACHIN, **Direito Civil sentidos, transformações e fim.**, p. 144.

²¹⁴ DONEDA, **Da privacidade à proteção de dados pessoais [livro eletrônico]**.

Portanto, embora se tenha exposto as limitações do consentimento enquanto paradigma da proteção de dados pessoais, não há que se falar em seu abandono como base legal para o tratamento de dados.

O dado não pode ser concebido como um fim em si mesmo e, ao mesmo tempo, não se pode diminuir a liberdade do titular de dados e dos agentes de tratamento²¹⁵. O direito deve tutelar os avanços tecnológicos sem inviabilizar o desenvolvimento da sociedade²¹⁶.

Nessa linha, em referência ao direito comparado, destaca-se que o GDPR prevê, de modo expresso, que o consentimento não é a única base legal idônea para o tratamento de dados pessoais, consoante se infere do Considerando 40²¹⁷.

A proteção de dados é instrumento fundamental para fazer convergir o desenvolvimento tecnológico com o progresso e ética necessários ao livre desenvolvimento da pessoa humana.

Neste contexto, a abertura normativa a outras hipóteses de tratamento que ostentam a mesma qualidade jurídica do consentimento merecem reconhecimento. Destaque-se, dentre elas, o legítimo interesse, o qual será examinado em capítulo próprio.

1.3.3. A tutela da privacidade desde a concepção (por padrão) como variante das tecnologias promotoras do direito fundamental à proteção de dados

Seus dados são você²¹⁸. Com efeito, cada sujeito é os próprios dados em uma sociedade digital. Sob essa perspectiva, um dado vulnerável é o mesmo que um indivíduo vulnerável²¹⁹.

À luz do que se expõe neste trabalho, ressoa inequívoco que, dentro das modernas e complexas relações interprivadas, os dados dos indivíduos são capazes de permitir a construção

²¹⁵ Art. 2º da Lei Geral de Proteção de dados: A disciplina da proteção de dados pessoais tem como fundamentos: (...) V - o desenvolvimento econômico e tecnológico e a inovação;

²¹⁶ COHEN, Julie E, *Examined Lives: Informational Privacy and the Subject as Object*, **Stanford Law Review**, v. 52, p. 1373–1438, 2000.

²¹⁷ Considerando 40: Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar. UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

²¹⁸ A expressão se refere à campanha realizada no ano de 2017 pela Coalizão Direitos na Rede, a qual abrange diversas entidades e acadêmicos em defesa da internet livre e aberta no Brasil destinada a pressionar o Congresso Nacional no sentido da edição de legislação dirigida à tutela dos dados pessoais. Disponível em: <<https://idec.org.br/noticia/seus-dados-sao-voce-campanha-alerta-sobre-uso-de-informacoes-pessoais>>. Acesso em 12 mai. 2021.

²¹⁹ SORO, Antonello, *Vulnerable Person: Data Protection and Digital Society*, **Digest: National Italian American Bar Association Law Journal**, v. 24, p. 117–132, 2016, p. 118.

de perfis que determinam e, ou, condicionam o acesso a diversos bens da vida, bem como influenciam a formulação de políticas públicas pelo Estado²²⁰.

Antonello Soro pondera que "o que está sendo analisado, desmontado e reprocessado é a nossa identidade - graças aos algoritmos que podem determinar decisões chave não apenas em economia, política ou finanças, mas, também, de modo crescente no nosso dia a dia"²²¹.

Assim, é lúdica a conclusão no sentido de que a moderna organização social se baseia no acúmulo e circulação de informações²²² e é certo, também, que elementos de informação referentes aos titulares de dados são cobiçados ativos. Não por outra razão, os agentes econômicos desenvolvem produtos e serviços, gratuitos ou não, destinados, também, à sua coleta e tratamento²²³.

Consoante já abordado, a abrangência global de determinados bens materiais ou serviços e a necessidade de se disponibilizar o "mesmo produto" a um público diversificado conduzem as empresas a elaborarem contratos de adesão, por vezes chamados de termo de uso, padronizados com pouca ou nenhuma flexibilidade. Esses documentos, elaborados em contexto de massificação de relações contratuais corriqueiras, evidenciam essa outra característica importante do mercado baseado no fluxo informacional²²⁴.

Essa é a dinâmica atual²²⁵. Como regra, ao consumidor se propõe um contrato genérico com a única opção de aceitação ou recusa. Na escolha da segunda hipótese, veda-se o acesso ao bem da vida pretendido.

²²⁰ Para Lemos e Branco, os dados pessoais seriam a representação do que cada um é e, mediante sua utilização, as vidas das pessoas são decididas em diversos aspectos. *In*: LEMOS, Ronaldo; BRANCO, Sérgio, *Privacy by design: conceito, fundamentos e aplicabilidade na LGPD*, *in*: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 457.

²²¹ SORO, **Vulnerable Person: Data Protection and Digital Society**, p. 118, livre tradução.

²²² RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 35.

²²³ Nesse sentido, Harari: No presente, as pessoas ficam contentes de ceder seu ativo mais valioso—seus dados pessoais—em troca de serviços de e-mail e vídeos de gatinhos fofos gratuitos. É um pouco como as tribos africanas e nativas americanas que inadvertidamente venderam países inteiros a imperialistas europeus em troca de contas coloridas e bugigangas baratas. Se, mais tarde, pessoas comuns decidirem tentar bloquear o fluxo de dados, podem descobrir que isso é cada vez mais difícil, especialmente se tiverem chegado a ponto de depender da rede para todas as suas decisões, até mesmo para sua saúde e sua sobrevivência física. HARARI, **21 lições para o século 21**, p. posição 1497 [ebook kindle].

²²⁴ Bioni considera que “as políticas de privacidade são, por excelência, um contrato de adesão. A massificação das relações contratuais ordinárias de consumo é também característica marcante no mercado informacional” BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 170–171.

²²⁵ Stefano Rodotà pondera que "hoje, a verdadeira utopia é aquela de quem acredita que seja possível extirpar a infraestrutura informativa das nossas organizações sociais: mesmo que isso não queira dizer que a tecnologia deva ser vista como um valor sempre progressivo, substituindo a ideologia do *laissez-faire* por aquela do *laissez-innover*, nem que se possa ocultar o caráter "totalitário" do computador por sua cortina da eficiência. Se a finalidade a ser atingida é a de fazer melhor uso possível de um dos mais importantes recursos básicos da sociedade do futuro, o caminho é aquele que coerentemente comas indicações da análise precedente, conduz à expansão do poder coletivo". *In*: RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 39.

Nesse cenário, e, na linha do que já mencionado, usualmente o titular dos dados pessoais não detém condições sequer de compreender no que consiste, no plano fático, o seu direito à autodeterminação informativa, uma vez que não lhe é dado conhecer, de forma plena, os elementos de informação que serão coletados e tratados, por quem seus dados passarão e, tampouco, se lhe faculta a possibilidade de transigir sobre um ou outro aspecto de sua privacidade. Bioni acrescenta, ainda, outro ponto importante, qual seja "a atualização contínua dos termos de uso cuja instabilidade retira qualquer perspectiva de controle, já que, na maioria das vezes, eles se tornam mais invasivos em relação às suas versões anteriores"²²⁶.

Embora se reconheça a dificuldade de leitura holística sobre a repercussão do ato de disposição dos dados, diante de ampla possibilidade de uso secundário dos elementos de informação fornecidos e à míngua de um sistema estruturado de proteção de dados, alguns autores percebem tendência de comportamento de autodefesa praticado pelos indivíduos, qual seja o fornecimento de informações inexatas quando não há a imposição de consequências negativas imediatas ou parcialmente exatas nos demais casos²²⁷.

Imagine-se, como exemplo, o fornecimento de endereço de e-mail falso, ou criado especificamente para determinada situação no momento do cadastro necessário à utilização de um determinado serviço ao qual o interessado não pretende se vincular de modo direto, ou não deseje que aquele uso venha a compor o seu perfil digital, ou, simplesmente, não pretende qualquer interlocução com o prestador do serviço.

Além disso, a assimetria informacional associada à ausência de controle efetivo por parte do titular dos dados sobre a amplitude da intrusão do agente de tratamento sobre sua privacidade evidencia a necessidade de se repensar as atuais formas de disposição dos dados pelos titulares e sua tutela jurídica²²⁸.

Certamente, os abusos devem ser contidos e resguardar o cidadão da utilização de dados que extrapole as finalidades da coleta deve ser objetivo perseguido a todo instante tanto pelo Estado quanto pela sociedade de maneira geral.

²²⁶ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 172.

²²⁷ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 82.

²²⁸ Para Bioni, “[t]rata-se, pois, de 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 dos dados pessoais, e que percorram universalmente todo o ambiente on-line 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 do ambiente eletrônico. É por tal razão, que esse ferramental não se ajusta à mencionada complexidade do fluxo informacional das renovadas relações de consumo, sobrecarregando o cidadão do século XXI”. BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 175.

No campo normativo, identifica-se algumas diretrizes no direito comparado. Por sua pertinência, faz-se menção ao artigo 25º do GDPR, o qual versa especificamente sobre a proteção de dados desde a concepção e por padrão²²⁹.

No ordenamento jurídico brasileiro, a LGPD dispõe que, desde a fase de concepção do produto ou do serviço até a sua execução, deverão ser observadas medidas de segurança, técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito deverão ser adotadas pelos agentes de tratamento (art. 46, *caput*, e § 2º)²³⁰.

Similarmente ao regulamento europeu, o dispositivo versa sobre a incorporação, pela LGPD, das balizas das cognominadas proteção da privacidade por padrão e proteção da privacidade por *design*.

Sufraga-se a compreensão de que o objetivo de adequada tutela dos dados pessoais deve permear todo o processo de disponibilização de produto ou serviço. Logo, desde a concepção do bem que se pretende disponibilizar, deve-se adotar técnicas que promovam a plena liberdade do titular de dados e isso pode ser alcançado a partir da observância do eixo principiológico da própria LGPD, a exemplo da implementação de medidas como a coleta apenas dos dados efetivamente necessários à finalidade do tratamento, do cumprimento do dever de transparência

²²⁹ Artigo 25º 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 3 maio 2021.

²³⁰ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (...) § 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

e da simplificação do processo de opção pelo titular quanto à gama de elementos de informação que pretende disponibilizar²³¹.

Neste cenário, o princípio da precaução, insculpido no art. 6º, VIII, da LGPD, deve ser ressaltado, pois, ao preconizar a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, se consubstancia em incentivo normativo aos agentes de tratamento para que elaborem formas de interação com os titulares que resguardem a sua autonomia informacional.

Calha destacar, ainda, que as tecnologias que promovem a privacidade, também chamadas de *privacy enhancing technologies* (PETs), despontam como alternativa relevante e amplamente aceita pela literatura nacional e internacional²³².

Os conceitos de *privacy by design* e *privacy by default* são espécies desse gênero e pode-se afirmar que são paradigmas que funcionalizam a tutela da privacidade ao se tomar como ponto de partida o reconhecimento da posição de centralidade dos indivíduos no sistema de proteção de dados.

Assim, o escopo principal da privacidade por padrão é restringir a coleta de dados pessoais ao mínimo necessário e, ao mesmo tempo, reduzir a disparidade informacional existente entre o agente de tratamento e o titular de dados por meio do desenvolvimento de tecnologias que permitam maior conhecimento dos envolvidos em torno dos aspectos relacionados à privacidade, possibilitando-se a tomada de decisões mais conscientes pelos indivíduos.

²³¹ Nessa linha, Tepedino e de Teffé sustentam que “(...) a partir desses paradigmas, entende-se que a proteção dos dados deve ser pensada desde a concepção do produto ou serviço disponibilizado, devendo ser implementadas medidas técnicas e organizacionais pelas empresas e organizações. Há de se obter a garantia de que os dados pessoais serão processados com a mais alta proteção da privacidade do titular (por exemplo, apenas os dados necessários devem ser tratados, o período de armazenamento deve ser curto e o acesso aos dados deve ser limitado), de forma que os dados sejam automaticamente (como padrão) protegidos em qualquer sistema de TI ou prática de negócios. A privacidade se torna componente essencial da funcionalidade principal do que está sendo entregue. Atua-se, assim, no sentido de incorporar fortes medidas de segurança ao ciclo dos dados para se garantir o gerenciamento seguro das informações do começo ao fim. Seja qual for a prática ou tecnologia envolvida, ela deverá colocar em primeiro lugar os interesses dos titulares dos dados e operar de acordo com as promessas e objetivos declarados, estando sujeita inclusive a uma verificação independente”. In: TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de, Consentimento e proteção de dados na LGPD, in: **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro [livro eletrônico]**, 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

²³² BIONI, **Proteção de dados pessoais a função e os limites do consentimento**; HOFFMANN-RIEM, **Teoria geral do direito digital: transformação digital: desafios para o direito**; LEMOS; BRANCO, **Privacy by design: conceito, fundamentos e aplicabilidade na LGPD**; TAVANI, Herman T.; MOOR, James H., Privacy protection, control of information, and privacy-enhancing technologies, **ACM SIGCAS Computers and Society**, v. 31, n. 1, p. 6–11, 2001.

No ponto, há que se fazer relevante distinção entre privacidade e mecanismos que propiciem o exercício do controle de privacidade.

As tecnologias de promoção da privacidade não se consubstanciam, necessariamente, em reforço da privacidade em si, uma vez que se pode ter controle, mas nenhuma privacidade e, também, privacidade, mas nenhum controle²³³. É dizer: atribuir ao indivíduo exclusivamente a obrigação de controle sobre os próprios dados e, em última análise sua própria privacidade, tende a criar paradoxal situação de fragilização desse direito, principalmente se considerados as limitações ao consentimento já abordadas. De outro lado, se impor a obrigação aos agentes de tratamento de tutela da privacidade alheia sem a possibilidade de interveniência do titular dos dados certamente configura estímulo a condutas abusivas.

Portanto, se de um lado o movimento incessante de dados retira a possibilidade de pleno e efetivo controle individual sobre as informações que circulam a respeito dos titulares, de outro, a existência de mecanismos de contenção da exposição da privacidade de cada um, já previamente à própria coleta e processamento, diminui a assimetria de poderes existente e, em última análise, estimula a própria atuação dos interessados em desenvolver a atividade de tratamento de dados dentro das balizas legais.

As tecnologias de promoção da privacidade são, portanto, instrumentos que reforçam o controle em torno da privacidade e não manifestação do direito à privacidade em si. Para melhor esclarecer esse ponto de vista, faz-se referência às recentes medidas adotadas pela empresa Apple quanto ao fortalecimento da privacidade dos usuários de seus produtos ou serviços, em especial no que diz respeito à imposição, ao fornecedor de aplicativo, de obtenção da permissão do usuário acaso se pretenda rastrear seus dados em programas ou sites de outras empresas²³⁴.

Partindo-se da premissa de que os conceitos de privacidade e controle sobre a disposição dos próprios dados não se confundem, há que se reconhecer os PETs como ferramentas

²³³ É o que acontece, por exemplo, quando se aceita a política de privacidade de determinado sítio eletrônico no que diz respeito a coleta de *cookies*. Ao usuário se confere a faculdade de aceitar e determinar quais informações serão coletadas. Acaso aceite todos os *cookies*, o usuário tem controle, mas renuncia à sua privacidade. Na hipótese de rejeição daqueles que se pode rejeitar, supostamente se terá mais privacidade, mas nenhum controle sobre a efetiva coleta e tratamento dos dados de acesso. Para Tavani e Moor, “[u]m problema fundamental sobre a definição do conceito de privacidade em termos de controle individual de informações é que ele reduz o que pode ser privado. Nós controlamos tão pouco. Como uma questão prática, não podemos controlar as vastas quantidades de informações sobre nós que circulam através de miríades de computadores, redes e bancos de dados. A atual globalização desses processos de informação agrava o problema. Se a privacidade depende, por definição, de nosso controle individual, simplesmente não temos uma privacidade significativa e nunca teremos em um mundo computadorizado”. In: TAVANI; MOOR, Privacy protection, control of information, and privacy-enhancing technologies, p. 6, livre tradução.

²³⁴ **Privacidade - Gerencie sua privacidade**, Apple (Brasil). Disponível em: <<https://www.apple.com/br/privacy/control/>>. Acesso em: 27 jul. 2021.

importantes, conquanto insuficientes, *per se*, para solucionar o problema da interferência na esfera da privacidade dos titulares pelos agentes de tratamento.

Assim, da mesma forma que a densidade constitucional do direito à proteção de dados e da autodeterminação informativa irradia efeitos sobre as relações que envolvem a coleta e o tratamento de dados e robustece a privacidade sob o prisma normativo, a existência de alternativas que conduzam ao equilíbrio entre os envolvidos nessas operações, a exemplo das PETs, a fortalecem sob o prisma material.

No que tange ao legítimo interesse, o assunto ganha relevância pois a ampliação do escopo de proteção da esfera privada dos indivíduos traz como necessária contrapartida a demanda por maior transparência dos agentes coletores de informações e as PETs podem funcionar como uma das formas de redução da assimetria informacional e do risco aos interesses dos titulares de dados²³⁵.

Nesse seguimento, o fortalecimento contínuo da proteção jurídica da privacidade sob os prismas normativo e material amplia as fronteiras de proteção do direito fundamental à proteção de dados e se abre caminho para os sujeitos, fontes de dados, disporem de instrumentos que lhes garantam a possibilidade de exigirem formas controladas de circulação de informações sem, necessariamente, se interromper seu fluxo²³⁶.

Ainda que não solucionem os problemas relacionados à disposição de dados pelos titulares, certamente as tecnologias de promoção da privacidade contribuem para a equalização das relações entabuladas entre titular e agente de tratamento e, também, para a materialização da autodeterminação informativa.

²³⁵ CIPL, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation.**

²³⁶ RODOTÁ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 94.

CAPÍTULO 2 – O LEGÍTIMO INTERESSE ENQUANTO BASE LEGAL APLICÁVEL PELOS AGENTES DE TRATAMENTO DE ACORDO COM A LGPD

O objeto principal do presente trabalho é a análise do legítimo interesse, hipótese de tratamento admitida na LGPD, razão pela qual se destinará capítulo específico para o estudo do tema.

Cuida-se de conceito aberto e, no contexto de abundância de instrumentos tecnológicos de coleta e correlação de dados, ostenta grande importância.

Ainda que o consentimento, sob o influxo do princípio da autodeterminação informativa, ocupe posição destacada, o legítimo interesse, enquanto base legal igualmente prevista pelo legislador, não pode ser concebido como a última opção para o processamento de dados.

Conforme já exposto, não se pode dizer que há hierarquia entre as bases legais para o tratamento de dados. Ao contrário, essas são complementares na medida em que a LGPD elenca as possibilidades legais e o desenvolvimento da atividade ocorre de acordo com os objetivos e condições do responsável e o enquadramento que se pretender dar àquela atividade.

Conquanto o legítimo interesse tenha passado a constar na LGPD somente em avançada discussão dos projetos de lei em trâmite no Congresso Nacional, não se cuida de novidade enquanto forma de tratamento de dados desvinculada do consentimento.

No direito comparado, já havia previsão pelo menos desde o regulamento europeu de 1995 e, nessa perspectiva, a experiência estrangeira tem muito a contribuir para o desenvolvimento da concepção brasileira acerca desse instituto jurídico.

2.1. O legítimo interesse no GDPR

Dentro do objeto de estudo do presente trabalho, é feita referência ao legítimo interesse como hipótese de tratamento de dados no âmbito do GDPR, uma vez que há aproximação terminológica entre os diplomas e a estrutura da norma europeia influenciou a elaboração da brasileira²³⁷.

²³⁷ BRASIL. Câmara Legislativa. **Relatório da Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, DE 2012 (Tratamento e Proteção de Dados Pessoais)**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305>. Acesso em: 11 abr. 2021, Pp.33-34.

De início, se identifica premissa relevante prevista nesse documento no sentido de que o direito à proteção de dados pessoais não é absoluto e deve ser funcionalizado, resguardando-se os direitos e liberdades fundamentais dos titulares de dados²³⁸.

No que diz respeito ao fundamento de licitude legítimo interesse, observa-se que a norma prevê diretrizes condicionantes²³⁹: a) prevalência dos interesses ou direitos e liberdades fundamentais do titular; b) expectativas razoáveis baseadas na relação com o responsável; c) avaliação contextual do caso concreto; d) distinção das hipóteses de tratamento de dados efetuados pela Administração Pública; e e) aderência aos princípios da necessidade e finalidade.

Ainda, o GDPR contempla situações exemplificativas de legítimo interesse admitido como fundamento para coleta e tratamento de dados as quais podem funcionar como importante norte interpretativo: i) tratamento para efeitos de comercialização direta (Considerando 47); ii) controle de condutas fraudulentas (considerando 47); iii) transmissão de informações entre responsáveis pertencentes ao mesmo grupo empresarial ou à instituição associada para fins administrativos internos (Considerando 48); e iv) desenvolvimento de medidas de segurança na rede e das informações contra "eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos" (Considerando 49)²⁴⁰.

Há, também, no regulamento, a previsão expressa do direito de oposição ao tratamento com esquite no legítimo interesse, ainda que o titular não venha a ter sua vontade atendida. Com efeito, o Considerando 69 expressamente estabelece a orientação de que incumbe ao responsável pelo tratamento a demonstração de que seus interesses legítimos prevalecem sobre os direitos e liberdades fundamentais do titular, bem como que se deve garantir a esse último o direito de se opor ao tratamento de dados que especificamente lhe digam respeito.

Em primeiro exame, o legítimo interesse pode parecer permitir o processamento dados de forma menos rígida, pois não depende do consentimento do titular e, em tese, serviria de

²³⁸ Considerando 4 do GDPR, *in verbis*: “o tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística”. UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

²³⁹ Esses aspectos são extraídos a partir da leitura conjunta dos Considerandos 47, 49 e 50 do GDPR.

²⁴⁰ UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

substrato para qualquer tratamento mediante justificativa razoável²⁴¹. Essa flexibilidade, contudo, não permite a conclusão de que se cuida de fundamento de licitude de mais fácil operacionalização.

Assim, é certo que o GDPR contempla espécie de sistema de admissibilidade do tratamento de dados com esteio no legítimo interesse e, conquanto se possa vislumbrar alguma vagueza conceitual, o legislador europeu se ocupou de prever, no próprio diploma normativo, diretrizes interpretativas e instrumentos legais viabilizadores da realização da atividade de tratamento de dados com fundamento nessa base legal.

A valoração quanto à lisura dessa atividade, contudo, somente é passível de ocorrer mediante análise contextual, consoante se extrai do Considerando 47. Segundo o dispositivo, é imprescindível que se avalie cuidadosamente, “no momento e no contexto em que os dados pessoais são recolhidos”, se os fragmentos de informação que se pretende coletar se coadunam com a finalidade do tratamento e o legítimo interesse manifestado.

Desse modo, o interessado na realização da atividade deve ser capaz de demonstrar, em cada caso concreto, que, no ato do recolhimento dos dados, se poderia considerar que o titular razoavelmente poderia prever, a partir de sua relação com o agente de tratamento, que o processamento com base no legítimo interesse seria realizado.

Portanto, a interpretação das disposições referentes ao legítimo interesse no GDPR leva à conclusão de que o exame sobre a viabilidade do tratamento com fundamento nesse permissivo legal incumbe, pelo menos em um primeiro momento, ao agente de tratamento unilateralmente. Ulteriormente é que as instâncias estatais de controle e o próprio titular de dados poderão verificar se a conduta de quem procedeu ao tratamento foi revestida de abusividade.

Cumpre apontar que a descrição, no próprio documento, de situações autorizadas de tratamento com base no legítimo interesse é salutar e facilita ao intérprete a compreensão do instituto, bem como traz alguma segurança para a atuação dos agentes de tratamento e, também, de controle.

Outrossim, calha destacar que o aspecto mais relevante parece ser a imprescindibilidade de que se realize, de forma constante, o cotejo entre o indigitado interesse legítimo do controlador, a finalidade do tratamento e as expectativas legítimas do indivíduo, fonte dos

²⁴¹ INFORMATION COMMISSIONER'S OFFICE (ICO-UK), **What is the 'legitimate interests' basis?**. Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>>. Acesso em: 28 nov. 2020.

dados, bem como o dever de se protegerem os direitos e liberdades fundamentais do cidadão, o que somente pode ser atingido a partir do chamado “teste de balanceamento”, o qual será examinado em tópico específico.

Realizado panorama do tratamento do legítimo interesse no GDPR, é oportuno se examinar a disciplina do tema no ordenamento jurídico brasileiro.

2.2. O legítimo interesse na LGPD

A partir da experiência do direito europeu, pode-se dizer que a noção de legítimo interesse tem como pontos de partida e chegada o "teste de balanceamento" entre os interesses do agente de tratamento e do titular dos dados a serem tratados.

No Brasil, entre a publicação da primeira versão do anteprojeto de lei, submetido à consulta pública em plataforma do Ministério da Justiça²⁴², e a sanção da Lei 13.709/18 (LGPD) transcorreram aproximadamente oito anos.

Nos primeiros textos postos para discussão no âmbito do Ministério da Justiça²⁴³, não se encontrou referência ao instituto legítimo interesse. Apenas na nova versão do documento se consignou disposição específica a respeito do tema²⁴⁴.

De igual sorte, no âmbito do Poder Legislativo, na Câmara dos Deputados, na primeira versão do Projeto de Lei nº 4.060/2012, apresentada pelo Deputado Milton Monti²⁴⁵, a referência que se tinha ao legítimo interesse não se consubstanciava em hipótese de tratamento de dados, mas em pressuposto lógico-normativo para o adequado desenvolvimento dessa atividade.

Já no Senado Federal, o Projeto de Lei do Senado 330/13, de autoria do Senador Antonio Carlos Valadares²⁴⁶, não continha referência ao legítimo interesse.

²⁴² De acordo com o sítio eletrônico do Ministério da Justiça, os primeiros debates sobre a proteção de dados pessoais tiveram início em 30/11/2010, enquanto a LGPD foi sancionada em 14/08/2018. Disponível em: <<http://pensando.mj.gov.br/debates/>>. Acesso em 20 abr. 2021.

²⁴³ Anteprojeto de Lei sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural. Disponível em: <http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/02/Anteprojeto_PDP.pdf>. Acesso em 20 abr. 2021.

²⁴⁴ Anteprojeto de Lei sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural. Disponível em: <<https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf>>. Acesso em 20 abr. 2021.

²⁴⁵ Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750>. Acesso em 20 abr. 2021.

²⁴⁶ Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=3927883&ts=1594000176492&disposition=inline>>. Acesso em 30/03/2021.

Nessas proposições normativas, nos dispositivos referentes ao efetivo tratamento de dados pessoais, o consentimento seria a base legal principal (art. 9º do Anteprojeto elaborado no âmbito do Ministério da Justiça, art. 12 do PL 4.060/12 e art. 4º do PLS 330/13)²⁴⁷.

Somente em julho de 2015, em Relatório Legislativo devolvido pelo Senador Aloysio Nunes Ferreira, no âmbito da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT), incluiu-se, no artigo 12, VII, do PLS 330/13, os "interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados"²⁴⁸ como hipótese legal de tratamento de dados pessoais.

A propósito, essa teria sido a primeira vez que se previu textualmente o legítimo interesse como hipótese de tratamento e se elencaram as bases legais para tratamento de dados pessoais sem a estrutura hierárquica inicialmente estabelecida²⁴⁹.

Paralelamente, o texto que tramitou na Câmara Legislativa, a partir de parecer da Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTI), manteve o legítimo interesse como requisito de idoneidade do tratamento de dados²⁵⁰.

Em momento posterior, a segunda versão da peça elaborada no âmbito do Poder Executivo trouxe abordagem mais abrangente em torno do instituto e evidenciou feição mais próxima à delineada na LGPD.

Cabe destacar que, no ano de 2018, após diversas audiências públicas e o consequente o amadurecimento das discussões em torno do instituto, na tramitação do projeto de Lei na

²⁴⁷ Consoante estudo realizado por Bioni e outros, “[a]s movimentações em torno da inserção da categoria legítimo interesse, ou interesses legítimos começaram em razão das consultas públicas a que o Anteprojeto do Poder Executivo foi submetido. Na primeira rodada, realizada em parceria com o Observatório Brasileiro de Políticas Digitais do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas do Rio de Janeiro e que durou cerca de 5 meses, foram recebidas 794 contribuições, provenientes de empresas e organizações do terceiro setor, majoritariamente. Conforme indica estudo publicado pela Associação Brasileira de Marketing Direto - ABMED, naquele momento houve poucas contribuições ou sugestões relacionadas ao legítimo interesse. Não foi, ainda, nessa ocasião que a base legal despontou”. BIONI, Bruno Ricardo; KITAYAMA, Marina; RIELLI, Mariana, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021, p. 15–16.

²⁴⁸ Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=3927917&ts=1594000176745&disposition=inlin>. Acesso em 30/03/2021.

²⁴⁹ BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 16.

²⁵⁰

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1454623&filename=PRL+1+CCTCI+%3D%3E+PL+4060/2012.

Câmara²⁵¹, o Relator da Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4.060, de 2012, Deputado Orlando Silva, consignou em seu Parecer, relativamente ao legítimo interesse, que: i) se cuida de hipótese de tratamento de dados desvinculada do consentimento, "inspirada nas práticas europeias existentes desde 1995"; ii) "sua previsão é necessária, seja para não onerar demasiadamente o titular dos dados com a necessidade de manifestação de consentimento a todo instante, seja porque em diversas situações concretas o tratamento de dados, mesmo sem consentimento, é importante para atender a uma finalidade pública ou a uma finalidade privada legítima"; e iii) "não deve ser lido como um cheque em branco. Em outras palavras, não pode ser utilizado como um subterfúgio para que todo e qualquer tratamento de dados pessoais seja autorizado"²⁵².

Referida contextualização é importante na medida em que se viabiliza reconhecer a relevância do tema e a importância do legítimo interesse como hipótese de tratamento, a qual só foi possível a partir da participação da sociedade civil no debate democrático.

Com efeito, a força conformadora da realidade dos fatos²⁵³ impõe a institucionalização de um conceito jurídico minimamente claro, sem se olvidar da importância de sua abertura hermenêutica, em ordem a se permitir ao agente de tratamento desenvolver suas atividades com segurança, sendo-lhe possível, inclusive, respeitar as expectativas em si depositadas pelo titular dos dados.

2.3. Legítimo interesse: sentido e alcance

Parte-se do seguinte questionamento: o que torna um interesse legítimo, sob o prisma normativo? Não há como se responder objetivamente à essa pergunta, contudo, é possível se

²⁵¹ Nas palavras de Bioni e outros: “[a] previsão do legítimo interesse foi objeto de uma intensa disputa. Um cabo de força foi puxado especialmente entre terceiro setor e setor privado para, respectivamente, bloquear-restringir e ampliar o espaço a ser ocupado por essa base legal. Ao final, alcançou-se um denominador comum, a partir de uma solução mediada e proposta, principalmente, pelo setor acadêmico, em que a previsão veio acompanhada de um dispositivo da lei que parametriza a sua aplicação (art. 10). Com isso, a lei brasileira inovou ao prever no seu próprio texto critérios para a aplicação de um conceito jurídico indeterminado e, assim, trazer maior previsibilidade quanto à sua aplicação e interpretação. Desde o seu nascedouro, já havia a preocupação quanto aos efeitos colaterais, em termos de segurança jurídica, da introdução do legítimo interesse, o que foi potencialmente remediado no desenho final da LGPD”. BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 20.

²⁵² BRASIL. Câmara Legislativa. **Relatório da Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, DE 2012 (Tratamento e Proteção de Dados Pessoais)**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305>. Acesso em 11 abr. 2021, Pp.33-34.

²⁵³ FACHIN, **Direito Civil sentidos, transformações e fim**.

estabelecer algumas diretrizes à luz do direito posto e da abordagem doutrinária em torno do assunto.

Na doutrina pátria, os autores que abordam o tema estruturam a compreensão do instituto a partir do reconhecimento da ausência de hierarquia entre as bases legais de tratamento²⁵⁴.

No ponto, destaca-se que alguns, embora reconheçam a juridicidade da base legal legítimo interesse, atribuem-lhe certa carga subsidiária, a exemplo de Viola e Teffé, para quem o legítimo interesse poderá ser utilizado desde que de forma “proporcional e limitada, quando trazer benefício claro e determinado para o controlador e/ou terceiro”, não cause impacto elevado aos direitos e garantias do indivíduo, sejam respeitadas as legítimas expectativas do titular e “quando não for possível ou não se desejar dar ao titular dos dados total controle ou, ainda, quando o controlador não quiser incomodá-lo com solicitações de consentimento para tratamentos que muito provavelmente seriam aceitos pelo titular”²⁵⁵.

Na mesma linha, Bioni defende, sob a óptica do princípio da necessidade, a imprescindibilidade de se verificar “se o tratamento dos dados não seria coberto por outras bases legais, que não a do interesse legítimo”²⁵⁶.

No plano doutrinário internacional, Zanfira-Fortuna e Troester-Falk, ao examinarem o GDPR, também não identificam hierarquia entre as bases legais de tratamento de dados²⁵⁷ e atribuem caráter residual ao legítimo interesse.

De acordo com o Parecer 6/2014 do Grupo de Trabalho para o Artigo 29²⁵⁸, para ser considerado legítimo, o interesse não pode ser ilegal. Além disso, deve ser claro, objetivo e

²⁵⁴ Nesse sentido: VIOLA; TEFFÉ, Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o E 11; PONCE; MATTIUZZO, O legítimo interesse e o teste da proporcionalidade; LEONARDI, Marcel, Legítimo interesse, **Revista do Advogado**, v. 144, p. 67–73, 2019; BIONI, **Proteção de dados pessoais a função e os limites do consentimento**.

²⁵⁵ TEFFÉ; VIOLA, **Tratamento de dados pessoais na LGPD**, p. 21.

²⁵⁶ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 255.

²⁵⁷ ZANFIRA-FORTUNA, Gabriela; TROESTER-FALK, Teresa, **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases, 2018**.

²⁵⁸ De acordo com o European Data Protection Board (EDPB), o Grupo de Trabalho para o Artigo 29 “é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD)”. In: EDPB, European Data Protection Board, **Grupo de Trabalho do Artigo 29.º | European Data Protection Board**. Disponível em: <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt>. Acesso em: 29 jul. 2021.

articulado de modo a permitir a realização do chamado teste de ponderação. Outrossim, o conceito não comporta especulação e deve se relacionar a interesse atual e concreto, real²⁵⁹.

Na esfera normativa, no direito comparado, o GDPR, no artigo 6º, I, *f*, estabelece a premissa da "necessidade" do tratamento, desde que não se vulnere "interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança"²⁶⁰.

Com efeito, as diretrizes interpretativas em torno do legítimo interesse no direito europeu evidenciam certo caráter subsidiário (Considerandos 47 e seguintes), de sorte que deve ser utilizada essa base legal quando o mesmo resultado não puder ser obtido por outra menos imprecisa²⁶¹.

É oportuno se deixar clara a peculiaridade desse sistema no sentido de que, embora sujeita à efetiva demonstração da necessidade pelo controlador, a opção pelo legítimo interesse não se cuida de "último recurso" para o tratamento de dados. Em verdade, o que se defende é que a escolha dessa base legal não se deve dar de forma irrefletida, no intuito de não se ampliar a sua utilização sob a falsa impressão de que se cuida de opção menos complexa²⁶².

Na LGPD não se identifica essa marca de subordinação atribuída ao legítimo interesse e, nos termos da lei, o princípio da necessidade se refere à "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"²⁶³. O legislador não limitou a escolha da base legal para a atividade de tratamento, mas, sim, o grau de interferência na privacidade do titular de dados.

A propósito, principalmente se observado o histórico legislativo, a adoção do vocábulo "necessário" para enunciar o legítimo interesse enquanto fundamento de licitude para o tratamento de dados na LGPD não parece condicionar a opção por essa base legal ao exame da

²⁵⁹ No mesmo sentido, Ponce e Mattiuzzo apontam que: "(...) antes que se questione se um interesse é legítimo, é preciso questionar e delimitar qual é esse interesse, ou o "propósito" deste tratamento de dados pessoais. O WPDP29 (2014), em Opinião relacionada ao tema do legítimo interesse, elaborou o seguinte passo-a-passo para identificar se um interesse pode ser considerado legítimo: (i) é preciso avaliar se ele é ilegal; (ii) é igualmente preciso que ele seja suficientemente claro e articulado, de modo a permitir que o teste seja realizado, isto é, o interesse deve ser suficientemente específico; (iii) é preciso que represente um interesse real e presente, isto é, não ser especulativo". PONCE; MATTIUZZO, O legítimo interesse e o teste da proporcionalidade, p. 61.

²⁶⁰ UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

²⁶¹ EDPB, European Data Protection Board - Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, 2014, p. 3.

²⁶² EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p. 3.

²⁶³ Art. 6º, III, da LGPD.

viabilidade da adoção de outras supostamente menos intrusivas²⁶⁴, uma vez que o enfoque dado pelo legislador se dá sobre os propósitos do controlador ou de terceiros e o art. 10 da mesma lei amplia as possibilidades de adoção desse fundamento de licitude ao estabelecer rol não exaustivo, conforme se verá adiante.

Leonardi considera que a escolha da base legal "representa um risco jurídico"²⁶⁵, o qual deve ser assumido pelo agente de tratamento no momento da escolha dessa base legal.

Logo, se não há superioridade entre as hipóteses legais permissivas do tratamento de dados pessoais, a escolha e o respectivo ônus de demonstrar sua higidez cabe ao agente de tratamento.

Assim, conquanto o GDPR remeta à necessidade em feição mais ampla e a LGPD, à situação concreta e necessidade do controlador ou terceiro²⁶⁶, ambas guardam similaridade na medida em que se evidencia a imperiosidade de exame individualizado sobre cada evento de tratamento.

No que tange à formalização da escolha dessa base legal, segundo a LGPD, há a obrigatoriedade de referência à situação concreta e vinculação às finalidades reconhecidas como legítimas pelo sistema normativo vigente²⁶⁷.

Portanto, escolhido o fundamento de licitude legítimo interesse, se dá sequência ao exame do teste de balanceamento ou proporcionalidade (*Legitimate Interests Assessment – LIA*). Por oportuno, calha apontar que para Ponce e Mattiuzzo “a verificação sobre o cabimento do legítimo interesse no caso concreto é uma etapa pretérita ao teste propriamente dito, já que o teste, como o próprio art. 10 preconiza, se dá uma vez que o legítimo interesse já foi identificado como cabível”²⁶⁸.

Porém, entre a opção pelo fundamento de licitude legítimo interesse para o tratamento de dados pessoais e a realização do teste de balanceamento (ou ponderação), se reconhecem vários elementos dotados de relevância jurídica que merecem abordagem específica, a qual se procurará realizar dentro deste estudo.

Diante da estrutura aberta da LGPD, não se pode extrair interpretação no sentido de o legislador brasileiro ter estabelecido rol taxativo quanto aos incisos que preveem hipóteses de finalidades compatíveis com o legítimo interesse, em especial quando se considera o

²⁶⁴ Art. 7º, IX, da LGPD.

²⁶⁵ LEONARDI, **Legítimo interesse**, p. 69.

²⁶⁶ Respectivamente, art. 6º, 1, f, do GDPR e art. 10 da LGPD.

²⁶⁷ Arts. 7º, IX, e 10 da LGPD.

²⁶⁸ PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 62.

desenvolvimento econômico, tecnológico, a inovação e a livre iniciativa como fundamentos da disciplina da proteção de dados²⁶⁹.

Logo, na realidade brasileira, o legítimo interesse, na vertente do controlador, pode, também, encontrar fundamento no tratamento de dados para a consecução de objetivos relacionados ao cumprimento de políticas de governança corporativa, para o desenvolvimento de atividades de rotina, bem como para a proteção do titular de dados desde que seus próprios interesses não suplantem os do controlador²⁷⁰.

Cuida-se, portanto, de base legal ampla e é de absoluta importância o papel desempenhado pela Autoridade Nacional de Dados, a qual, por meio de atuação independente, contribuirá de modo importante para o delineamento do conceito sob exame, em especial na ampliação do espectro de tutela do direito fundamental à proteção de dados e na edificação de mecanismos de contenção de eventuais abusos cometidos por agentes públicos e privados²⁷¹.

Não se pode olvidar, ainda, da existência de manifestações contrárias ao arcabouço normativo da proteção de dados europeia, modelo adotado pelo Brasil. Os que perfilham essa linha de pensamento consideram que o GDPR torna mais complexa a atividade desenvolvida pelas empresas que lidam com dados pessoais e impõe o desvio de recursos para funções administrativas e de registro dos atos praticados se distanciando do foco de bem atender o consumidor com produtos inovadores e a preços cada vez mais acessíveis²⁷².

Assim, se de um lado, esse diploma normativo promove, nas relações entabuladas entre agentes de tratamento e titulares de dados, valores como transparência, confiança e controle, de outro, as obrigações aos agentes de tratamento impõem às empresas a adoção de medidas de precaução e, não raro, de reelaboração de políticas de privacidade e atualização das plataformas de disponibilização de produtos e serviços a um custo financeiro e logístico relevante.

Sob essa perspectiva, há desvantagens que não podem deixar de serem observadas, pois certas disposições normativas não seriam claras e o atendimento de algumas exigências legais

²⁶⁹ Artigo 2º, V e VI, da LGPD.

²⁷⁰ Data Protection Network, **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. Disponível em: <<https://iapp.org/resources/article/guidance-on-the-use-of-legitimate-interests-under-the-eu-general-data-protection-regulation/>>. Acesso em: 3 maio 2020, p. 6.

²⁷¹ Para Rodotà, "[o] órgão de controle configura-se assim como uma instituição "que completa" o sistema de proteção de dados. (...) Contudo, não se pode concluir que a existência de um centro formal de vigilância torne o controle difuso supérfluo, porque a presença desse tipo de controle assegura a existência de um antídoto no sistema para os casos nos quais o controle forma se torne esclerosado ou sofra influência de grupos de pressão públicos ou privados". *In*: RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 86.

²⁷² DEVORE, Andrew, Statement of Andrew DeVore Vice President and Associate General Counsel Amazon.com, Inc. before the United States Senate Committee on Commerce, Science, and Transportation, 2018.

se apresentaria como um fardo, a exemplo do legítimo interesse que seria manifestação do aspecto "complexo, obtuso e de difícil interpretação"²⁷³ do GDPR.

Para os que aderem a esse ponto de vista, "a combinação de legislação longa, obscura e vaga, atrelada a um sistema rígido de sanções, cria as condições perfeitas para o aumento da litigância, na medida em que as empresas sofrem para prever quais práticas e interpretações do GDPR estariam corretas"²⁷⁴.

De acordo com Wilcox, a previsão vaga desse conceito não proporciona, de modo satisfatório, instruções detalhadas para se estabelecer o que se qualificaria, ou não, como interesse legítimo. Essa situação conduziria os agentes econômicos a preocupações desnecessárias e ao dispêndio inadequado de recursos, além de gerar o risco de perda de clientes que se sintam desconfortáveis com as atualizações constantes de políticas de privacidade²⁷⁵.

Os argumentos contrários são todos aplicáveis à LGPD, máxime se considerada a já aventada proximidade entre as duas legislações.

Não se concorda com essa orientação, pois o GDPR é expressão da vanguarda da tutela da privacidade e dos dados dos indivíduos, principalmente no atual contexto de sociedade baseada no seu comércio. Com efeito, repercussões financeiras decorrentes do dever de observância das normas protetivas das pessoas são suportadas por toda a cadeia produtiva, tanto fornecedores quanto consumidores.

Logo, diante de manifestações de cunho eminentemente patrimonial²⁷⁶, da mesma forma que seria utópico se negar a "infraestrutura informativa das nossas organizações sociais"²⁷⁷, não se pode ignorar a posição de centralidade da pessoa no ordenamento jurídico pátrio. É dizer: a lógica puramente patrimonial deve ceder lugar à dimensão constitucional da tutela da dignidade da pessoa humana sob a vertente do pleno desenvolvimento da personalidade.

²⁷³ WILCOX, Katherine M, "Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation, *Brooklyn Law Review*, v. 85, p. 30, 2019.

²⁷⁴ *Ibid.*, p. 274.

²⁷⁵ WILCOX, "Hey Alexa, Do Consumers Really Want More Data Privacy?": An Analysis of the Negative Effects of the General Data Protection Regulation.

²⁷⁶ Rodotà observa que "não se pode julgar decisivo o argumento do aumento dos custos para as empresas (e para a administração pública) ocasionado pelas normas de proteção de dados. As empresas já suportam custos por conta da tutela de interesses gerais, relacionados à segurança dos trabalhadores, tutela dos consumidores ou integridade do meio ambiente. Não se pode efetivamente estimar que os interesses ligados à proteção de dados sejam de ordem inferior". In: RODOTÀ, *A vida na sociedade da vigilância: a privacidade hoje*, p. 53.

²⁷⁷ *Ibid.*, p. 39.

Isso posto, entende-se que alegações genéricas de complexidade da legislação vigente não se revelam suficientes para a não implementação das normas relativas ao tema. Os interesses contrapostos devem ser compatibilizados.

O recurso a orientações formais de órgãos oficiais envolvidos na regulamentação da matéria e à base dogmática em torno do direito à proteção de dados parecem ser cruciais na diminuição do apontado “fardo” de proteção da privacidade, razão pela qual, no presente trabalho, se procura, também, contribuir para a clarificação de conceitos indeterminados previstos em lei.

Dessarte, destacam-se dois prismas sob os quais pode ser estudado esse instituto. Primeiro: o legítimo interesse enquanto base legal para o tratamento de dados; e segundo: o legítimo interesse como elemento irradiador de deveres que permitem o tratamento de dados com amparo nessa hipótese normativa.

2.3.1. O legítimo interesse enquanto fundamento de licitude para o processamento de dados pelos agentes de tratamento

Dentro do primeiro enfoque de estudo proposto, e à luz do já abordado princípio da vedação do tratamento, é imprescindível a existência lógico-normativa de permissivo legal que confira ao agente que pretende tratar dados pessoais o substrato jurídico necessário para desempenhar sua atividade dentro do espectro da legalidade.

Nesta senda, o tratamento com fundamento no legítimo interesse ocorre 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"²⁷⁸.

Logo, no plano objetivo, presentes os pressupostos legais relacionados ao processamento de dados com base no legítimo interesse, quais sejam: finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam ao apoio e promoção de atividades do controlador e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais²⁷⁹, se revela juridicamente viável para o controlador manejar dados pessoais com fundamento nessa hipótese legal.

²⁷⁸ Art. 7º, IX, da LGPD.

²⁷⁹ Art. 10 da LGPD.

Sob o aspecto subjetivo, não se pode olvidar que, de acordo com a lei, ao controlador incumbe tomar "as decisões referentes ao tratamento de dados pessoais"²⁸⁰.

Portanto, se pode inferir que, ao menos em um primeiro momento, a escolha dessa base legal de tratamento é realizada unilateralmente pelo controlador, quem, desde antes do início do efetivo tratamento, deve justificar sua opção, principalmente diante da redação do art. 10 que expressamente faz alusão à "situação concreta".

Desta sorte, por mais que um agente de tratamento venha a ter acesso à base de dados de outro, é imprescindível que isso se dê na qualidade de controlador dos dados, pois se for como operador, o legítimo interesse não lhe possibilita tratar aqueles fragmentos de informação com os quais teve contato²⁸¹.

Ainda neste tema, cabe referência ao art. 39 da LGPD, o qual dispõe que "o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria". Com efeito, o dispositivo deixa clara a obrigação do controlador de verificar, durante o ciclo do processamento, a observância das normas sobre a matéria, bem como das próprias instruções.

Consequentemente, se a justificativa e fiscalização do tratamento de dados com base no legítimo interesse é de responsabilidade do controlador, o tratamento dos dados realizado pelo operador independe da configuração, em relação a si, dessa base legal, desde que essa atividade esteja explicitada pelo controlador e se vincule à finalidade legítima previamente definida e manifestada.

Assim, caso o operador opte por realizar tratamento de dados fora das instruções determinadas pelo controlador é possível se vislumbrar infração tanto ao contrato entabulado com o controlador quanto à própria LGPD, ainda que sua atuação se dê sob o argumento de que se estaria atuando sob o influxo do legítimo interesse do controlador.

²⁸⁰ art. 5º, VI, da LGPD.

²⁸¹ A fim de esclarecer o ponto de vista, transcreve-se o exemplo mencionado por Oliveira e Cots: "A empresa A atua no comércio de produtos pela internet e contratou a empresa B, que presta serviços relacionados ao *Business Intelligence* (BI), para realização de estudos, segmentação do público e melhora nas vendas. Para que a empresa B execute seus serviços, deverá ter acesso integral à base de dados de clientes da empresa A, podendo, inclusive, visualizar dados pessoais de clientes. A empresa B pretende utilizar a base jurídica do legítimo interesse para copiar o banco de dados da empresa A e mantê-lo consigo para uso futuro, sem anonimização dos dados pessoais e sem finalidade específica. Questão: A empresa B poderia utilizar a base jurídica do legítimo interesse para copiar e manter consigo a base de clientes da empresa A? Resposta: Não. A base jurídica do legítimo interesse não poderia ser utilizada pela empresa B sem descaracterizar sua figura de operadora. Em outras palavras, ao copiar o banco de dados, a empresa B se transformaria em Controladora e estaria violando o contrato fechado com a empresa A". OLIVEIRA; COTS, **O legítimo interesse e a LGPD**, p. 68–69.

E isso sucede em razão do sistema de proteção de dados desenhado pelo legislador. Pois, assim como se revela um ônus desproporcional incumbir o operador de verificar o enquadramento normativo da conduta do controlador é igualmente desarrazoada a imposição a esse do dever de fiscalizar as atividades daquele fora do âmbito contratual.

Em situações de transgressão à LGPD deverá incidir o sistema de responsabilidades previstos na Lei 13.709/18, sem prejuízo da responsabilização do agente faltoso com fundamento em outros diplomas legislativos a exemplo do disposto no art. 45 dessa lei que estabelece que “nas hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”.

Desse modo, parece clara a impossibilidade de o legítimo interesse previsto na LGPD se relacionar ao interesse do operador por duas razões essenciais: i) falta de previsão legal; e ii) permitir a proteção de dados pessoais e o livre fluxo informacional sem impor aos agentes de tratamento atribuições que não lhes cabem.

Reconhecido o protagonismo do controlador no delineamento do legítimo interesse a ser utilizado como fundamento para o tratamento de dados, faz-se referência a outra discussão. Questiona-se a abrangência do legítimo interesse de sujeitos distintos dos agentes de tratamento em razão da expressão "terceiros"²⁸² constante do art. 7º, IX, da LGPD.

Bioni e outros aduzem situações que, em tese, autorizariam o tratamento de dados com base no legítimo interesse de terceiros²⁸³⁻²⁸⁴.

O exemplo mais contundente dessa conformação legal é a aplicação da hipótese do legítimo interesse para o combate a fraudes. A um só tempo, é de interesse de uma empresa evitar, por exemplo, que o cartão de crédito que ela oferece seja fraudado, e é interesse do sistema bancário e financeiro, bem como da sociedade, que a referida fraude não ocorra. Um eventual compartilhamento de dados entre agentes do sistema

²⁸² Segundo o Centre for Information Policy Leadership (CIPL), “[t]erceiros’ refere-se a quaisquer partes interessadas envolvidas ou impactadas pelas atividades de processamento. Essas incluem outras organizações públicas e privadas, indivíduos que não sejam os titulares de dados, grupos de indivíduos, e da sociedade como um todo que podem se beneficiar das atividades de processamento. Essas atividades podem ser puramente comerciais ou envolver o processamento de dados no interesse público. Este último tornou-se particularmente relevante durante a pandemia da COVID-19, uma vez que o processamento e compartilhamento de dados tornou-se indispensável para o combate eficaz do vírus, o que é do interesse não só da sociedade na UE, mas global. As organizações frequentemente perseguem objetivos que servem direta ou indiretamente ao interesse público e beneficiam terceiros e a sociedade”. *In*: CIPL, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation**, p. 14.

²⁸³ BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 22.

²⁸⁴ No mesmo sentido, Zanfir-Fortuna e Troester-Falk, Marcelo Leonardi e o Parecer 6/2014 do Grupo de Trabalho para o artigo 29, apontam que o interesse legítimo deve ser do controlador ou de terceiros. *In*: ZANFIR-FORTUNA; TROESTER-FALK, **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases**; LEONARDI, **Legítimo interesse**; EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**.

financeiro (que não a instituição financeira que presta o serviço para o titular e que seria o controlador) enquadram-se na figura de terceiros;

Outro exemplo claro de legítimo interesse de terceiros é a *due diligence* em processos de fusão e aquisição, em que terceiros que não têm nenhuma relação pré-estabelecida com os titulares de dados pessoais possuem o legítimo interesse de tratar esses dados para avaliar a viabilidade da operação societária;

(...)

Mais um exemplo seria aquele em que se publica dados para fins de transparência e *accountability*, mesmo nos casos em que não há tal obrigatoriedade por força da Lei de Acesso à Informação.

Referido entendimento não é pacífico, pelo menos em relação à LGPD, pois embora o artigo 7º, IX, permita o tratamento de dados com a base legal do legítimo interesse de "controlador ou de terceiro", o art. 10, *caput*, aparentemente limita sua incidência ao "legítimo interesse do controlador".

Ponce e Mattiuzzo ponderam que o dispositivo que versa de forma mais detalhada sobre esse fundamento de licitude ignora a posição jurídica do terceiro tornando relevante “o questionamento sobre se esse é um caso de omissão propositada ou equivocada por parte do legislador”²⁸⁵⁻²⁸⁶.

Logo, diante da amplitude das possibilidades de tratamento de dados pessoais, é impossível se definir de antemão o que seria o legítimo interesse do terceiro na LGPD.

A partir de interpretação teleológica, principalmente à luz do princípio da prevenção da ocorrência de danos no tratamento de dados (art. 6, VIII, da LGPD)²⁸⁷, a melhor interpretação parece ser no sentido de se incluir, também, terceiros como sujeitos às disposições do art. 10.

Outra possibilidade é se entender que, ainda que o interesse do terceiro possa ser utilizado, o legislador atribuiu ao controlador o poder de decisão sobre o legítimo interesse a partir do caso concreto. Desta maneira, a avaliação do interesse do terceiro se daria sob a perspectiva do próprio controlador e não propriamente daquele imediatamente alheio à relação inicial de tratamento.

Independentemente da posição adotada, a operação de tratamento deve guardar consonância com o ordenamento jurídico como um todo, ser realizável no caso concreto e não

²⁸⁵ PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 68.

²⁸⁶ No mesmo sentido, Viola e Teffé sustentam que “o art. 10 da LGPD faz referência apenas ao controlador, devendo a doutrina e a ANPD esclarecerem se sua interpretação deverá ser ampliada. O termo “terceiro” não se refere apenas a outras organizações, podendo também ser um indivíduo não envolvido inicialmente de forma direta na relação ou o público em geral”. *In*: VIOLA; TEFFÉ, **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o E 11**, p. 145.

²⁸⁷ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

pode se sobrepor aos próprios interesses e direitos e liberdade do titular a partir da sua ligação com o agente de tratamento²⁸⁸.

Assim, embora não haja, na LGPD, definição sobre a abrangência da figura do terceiro, diversamente do que ocorre no GDPR²⁸⁹, ressoa inequívoco que o exercício de contextualização é de suma importância, porquanto texto e norma devem ser pensados de forma sistemática e há abertura normativa para que o controlador, a partir de sua própria avaliação, defina que atua no interesse de terceiros ou da sociedade.

Ainda no plano subjetivo, é oportuna a referência a outra discussão relevante, a qual diz respeito à possibilidade de transferência de informações entre membros do mesmo grupo empresarial sob o pálio do legítimo interesse. O Considerando 48 do Regulamento 679/2016 dispõe que os agentes de tratamento que pertençam ao grupo empresarial de alguma instituição poderão ter interesse legítimo na transmissão de dados pessoais, inclusive relacionadas a clientes ou funcionários, dentro do grupo para finalidades internas, desde que observados os princípios gerais que regem a transmissão de dados pessoais.

Nessa hipótese, assim como em qualquer outra que adote o legítimo interesse como base legal, se deverá realizar avaliação contextual e prévia, sem se descuidar da imprescindibilidade de observância das demais disposições referentes ao tratamento de dados pessoais constantes da legislação em vigor²⁹⁰, em especial quanto à indicação da finalidade do tratamento e da realização do teste de ponderação.

Já no plano material, quanto ao próprio conteúdo, de acordo com Parecer 6/2014 do Grupo de Trabalho para o Artigo 29, o interesse ostentaria caráter anterior e mais amplo do que a própria definição da finalidade²⁹¹. Pode-se afirmar, então, que se consubstanciaria na razão subjacente da definição da finalidade do tratamento²⁹².

²⁸⁸ Na linha do que se propõe, faz-se referência ao Considerando 47 do GDPR, o qual dispõe que “os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável (...)” UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

²⁸⁹ Artigo 4º (9). *Ibid.*

²⁹⁰ INFORMATION COMMISSIONER’S OFFICE (ICO-UK), **What is the ‘legitimate interests’ basis?**

²⁹¹ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**.

²⁹² Nessa linha, para Bioni e outros: “[a] finalidade é o propósito específico do tratamento de dados pessoais, enquanto o interesse é o valor mais amplo que um tratamento de dados pessoais representa para o seu controlador (ou terceiros, ou a sociedade como um todo). Um interesse, portanto, seria a garantia da segurança e da saúde de

É relevante se destacar, também, que entre interesse e finalidade não se tem uma relação continência, porquanto os diversos anseios do responsável pelo tratamento de dados podem, ou não, se coadunar com a finalidade admitida pela LGPD como fundamento para a realização dessa atividade, mas com ela não há vínculo de identidade ou de constrição.

Neste contexto, podem-se entrever dois filtros para se aferir o legítimo interesse do controlador no tratamento de dados: i) finalidade abstratamente legítima e ii) finalidade concretamente legítima.

No que diz respeito à finalidade abstratamente legítima, se deve realizar o cotejo entre a finalidade declarada pelo controlador e sua compatibilidade com ordenamento jurídico, no intuito de se aferir sua conformidade. É dizer: deve-se verificar se o pretendido tratamento de dados não encontra vedação na ordem jurídica, a exemplo de processamento de dados sem propósito claro ou despido de adequação a alguma das bases legais.

Quanto à finalidade concretamente legítima, deve-se examinar se o tratamento de dados é admissível à luz do caso concreto. Dentro do exame das situações concretas, destacam-se, ainda, alguns vetores normativos que condicionam o tratamento de dados, a exemplo da boa-fé; do respeito à legítima expectativa do titular; e da transparência.

Com efeito, é evidente que o legislador tenta funcionalizar o interesse legítimo a partir de conceitos imprecisos e isso não é prejudicial. Rodotà identifica nesse fenômeno a diacronia do sistema de proteção de dados²⁹³. Assim, a adoção de larga base principiológica e enunciados razoavelmente abertos permitem a adaptação da lei às novas realidades, de sorte que o passar do tempo não se caracterize como um elemento distanciador entre os fatos e as normas.

Portanto, embora não se possa estabelecer previamente no que consiste propriamente o legítimo interesse, se pode reconhecer dois pressupostos básicos, quais sejam: a impossibilidade de o interesse do agente de tratamento se sobrepor aos direitos fundamentais dos titulares de dados e a necessidade de respeito aos valores consagrados no ordenamento jurídico.

Deve-se perquirir, ainda, se a atividade de tratamento com base no legítimo interesse que se pretende desenvolver se sustenta sob a óptica do controlador²⁹⁴. Em outras palavras, há

um determinado grupo de pessoas, enquanto uma finalidade seria determinado tratamento de dados que garante tal interesse, por exemplo a instalação de controles de acesso em um local". *In*: BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 21.

²⁹³ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 135.

²⁹⁴ Para Oliveira e Cots: "(...) o início da reflexão parte da pergunta se o tratamento dos dados pessoais pretendidos é importante e se justifica, em relação ao controlador, a ponto de este não ser obrigado a coletar o consentimento dos titulares". *In*: OLIVEIRA; COTS, **O legítimo interesse e a LGPD**, p. 65.

que se ter a certeza de que o procedimento é concretamente justificável e passível de exame pelo titular de dados ou outros agentes de controle.

Em determinadas hipóteses, a adoção irrefletida do fundamento de licitude legítimo interesse não necessariamente conduzirá ao resultado esperado e, além de menos adequada ao caso concreto, pode resultar em maior impacto na privacidade do titular de dados. Busca-se, portanto, a partir do exame dos elementos que constituem essa base legal, construir balizas interpretativas capazes de reduzir seu elevado grau de subjetividade.

2.3.2. O legítimo interesse enquanto elemento irradiador de deveres

O segundo prisma de compreensão do legítimo interesse guarda relação com sua funcionalização enquanto elemento irradiador de deveres. Primeiramente, cabe destacar a dimensão subjetiva do direito fundamental à proteção de dados, a qual contempla o titular como sujeito ativo na relação jurídico-subjetiva e como sujeitos passivos aqueles de quem se pode exigir a observância da LGPD²⁹⁵.

Para além da discussão quanto à amplitude subjetiva, é relevante se evidenciar que a lei deve guardar, na maior medida possível, regulação simétrica. Isto é, os dispositivos devem incidir uniformemente sobre seus destinatários.

Em caráter mais amplo, mas mediante construção lógica plenamente aplicável ao ponto, Sarlet pondera ser essencial à adequada compreensão e interpretação do direito fundamental à proteção de dados o diálogo e a interação “com outros princípios e direitos fundamentais que, dentre outros pontos a considerar, auxiliam na determinação do seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos”²⁹⁶.

Logo, as disposições da LGPD não podem ser interpretadas de forma insular. O microsistema de proteção de dados pessoais que deve ser fortalecido e operado em benefício do titular de dados. Isso fica evidente a partir da leitura do art. 1º, o qual estabelece como objetivo da LGPD proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural²⁹⁷. Nesse sentido, para Bioni e outros, ao assim se proceder, se evita “uma valoração distinta entre os destinatários da norma e, com isso,

²⁹⁵ Remete-se o leitor à discussão já abordada no Capítulo 1 sobre a amplitude subjetiva do direito fundamental à proteção de dados.

²⁹⁶ SARLET, **Fundamentos constitucionais: O direito fundamental à proteção de dados**, p. 57.

²⁹⁷ Art. 1º 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.

obtem-se uma aplicação mais uniforme da base legal do legítimo interesse, independentemente de quem seja o seu favorecido"²⁹⁸.

Eventuais tratamentos diferenciados devem ser previstos em proposições normativas específicas, consoante se extrai, exemplificativamente, do art. 55-J, X, XII, XVII, da LGPD²⁹⁹.

Quanto aos deveres irradiados em si, a partir da leitura do art. 10, se vislumbra: a) dever geral de fundamentação do tratamento (art.10, *caput*); b) dever de uso da base legal legítimo interesse atrelado à finalidades legítimas consideradas a partir de situações concretas (art. 10, *caput*); c) dever de respeito às legítimas expectativas (boa-fé) e direitos fundamentais dos titulares (art. 10, II); d) dever de uso dos dados estritamente necessários à finalidade pretendida (art. 10,§ 1º); e) dever de transparência; e f) dever de documentação do racional de tratamento de dados (art. 10, § 3º).

Em razão de sua importância, far-se-á incursão sobre cada uma das obrigações acima mencionadas.

2.3.2.1. Dever geral de fundamentação do tratamento

Quanto ao dever geral de fundamentação do tratamento, além da observância do princípio da vedação de tratamento sem base legal, o legislador impôs importante ônus argumentativo ao interessado no processamento de dados com base no legítimo interesse, principalmente no que diz respeito à sua finalidade.

Esse encargo de se desincumbir da obrigação de indicar de forma fundamentada a escolha da base legal do legítimo interesse é benéfico ao sistema e guarda consonância com a estrutura principiológica da LGPD, uma vez que, consoante já mencionado, o primeiro juízo de valor sobre o enquadramento do tratamento de dados na hipótese legal é realizado de modo unilateral pelo próprio controlador e, nos termos dos princípios da responsabilização e da prestação de contas, deve haver "demonstração, pelo agente, da adoção de medidas eficazes e

²⁹⁸ BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 25.

²⁹⁹ Art. 55-J. Compete à ANPD (...) X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (...)XII - elaborar relatórios de gestão anuais acerca de suas atividades; (...) 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; (...) XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei.

capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"³⁰⁰.

Posto isso, se o agente de tratamento conseguir demonstrar o enquadramento da base legal do legítimo interesse, bem como que o resultado do teste de ponderação é favorável ao prosseguimento do processamento dos dados, não se vislumbra óbice à adoção da referida base, principalmente se considerado o sistema de responsabilidade previsto na própria lei.

2.3.2.2. Dever de uso da base legal legítimo interesse atrelado a finalidades legítimas consideradas a partir de situações concretas

Em relação ao dever de uso da base legal legítimo interesse atrelado a finalidades legítimas consideradas a partir de situações concretas, entende-se que o tratamento deve ser justificado a partir de situação real, não se revelando suficiente se apontar situação hipotética ou tratamento de dados com base em atividade prospectiva³⁰¹.

Schreiber pondera que o princípio da especificação dos propósitos preconiza que a atividade de coleta de dados pessoais seja sempre precedida da informação, ao titular de dados, dos propósitos de sua utilização, bem como impede a utilização em finalidade distinta da exposta ao indivíduo fonte dos dados³⁰².

Bioni e outros apontam distinção entre esse aspecto da norma brasileira e o constante da europeia ao afirmarem que, diferentemente da LGPD, a regulamentação do legítimo interesse, no GDPR, estaria inserida em permissivos não vinculantes, enquanto em âmbito nacional, o legítimo interesse seria inteiramente regulado em disposições cogentes³⁰³.

³⁰⁰ Art. 6º, X, da LGPD.

³⁰¹ A propósito, essa foi uma preocupação do legislador brasileiro, manifestada no Relatório do Deputado Orlando Silva, para quem o legítimo interesse: "(...) não pode ser utilizado como um subterfúgio para que todo e qualquer tratamento de dados pessoais seja autorizado. Esta a razão dos parágrafos do artigo, mediante os quais se destaca que o legítimo interesse deve sempre vir acompanhado dos princípios da adequação, necessidade e transparência bem como da possibilidade de fiscalização. Ademais, prevemos que deverá se basear em situação concreta e desde que atendidas as legítimas expectativas do titular". *In*: BRASIL. Câmara Legislativa. **Relatório da Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, DE 2012 (Tratamento e Proteção de Dados Pessoais)**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305>. Acesso em 11 abr. 2021, pp. 34-35.

³⁰² SCHREIBER, Anderson, **Direitos da Personalidade**, 2. ed. São Paulo: Atlas, 2013, p. 157.

³⁰³ Para os autores, "[d]iferente da Diretiva 95 e do Regulamento Geral de Proteção de Dados, em que este elemento foi acoplado à disciplina do legítimo interesse por orientações/interpretações não vinculantes, no caso da norma brasileira a concretude vem estampada no próprio art. 10". *In*: BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 28.

Enquanto nas demais hipóteses legais estabelecidas a partir artigo 7º, II, da LGPD a finalidade de tratamento já é pré-estabelecida pelo legislador, o legítimo interesse contempla maior espaço de conformação e, por essa razão, deve ser justificado caso a caso.

Vale destacar que qualquer manifestação que revele interesse ilegítimo, antiético ou fora do escopo normativo da LGPD não pode ser considerado legítimo interesse³⁰⁴.

Há interessante indicação, similarmente à técnica adotada na elaboração do Parecer 6/2014, realizada pela autoridade de proteção de dados do Reino Unido (ICO-UK³⁰⁵⁻³⁰⁶), de situações nas quais se sugere que não se utilize a base legal do legítimo interesse³⁰⁷.

De acordo com a doutrina, o interesse será legítimo quando for "suficientemente claro e concreto, além de não ilegal"³⁰⁸. Essa foi a fórmula adotada pelo legislador para atender aos interesses dos agentes de tratamento e, ao mesmo tempo, "não onerar demasiadamente o titular dos dados com a necessidade de manifestação de consentimento a todo instante"³⁰⁹ e, assim, viabilizar o livre fluxo informacional.

³⁰⁴ Nesse sentido se manifestou a Information Commissioner's Office (ICO) – Autoridade de proteção de dados do Reino Unido: “[a]nything illegitimate, unethical or unlawful is not a legitimate interest”. In: ICO-UK, Information Commissioner's Office, **What is the ‘legitimate interests’ basis?**, disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>>. Acesso em: 28 nov. 2020, p. 13.

³⁰⁵ Mesmo com a saída britânica da União Europeia, o GDPR foi “mantido na legislação interna como o GDPR do Reino Unido, mas o Reino Unido tem a independência para manter o quadro sob revisão”. In: ICO-UK, Information Commissioner's Office, **The UK GDPR**. Disponível em: <<https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/>>. Acesso em: 7 out. 2021.

³⁰⁶ ICO-UK, Information Commissioner's Office, **What is the ‘legitimate interests’ basis?**. Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>>. Acesso em: 28 nov. 2020.

³⁰⁷ De acordo com documento elaborado pela autoridade britânica de dados, não se deve utilizar a base legítimo interesse nas situações de “autoridade pública interessada e o processamento é para desempenhar suas tarefas como autoridade pública; processamento em desacordo com padrões legais, éticos ou industriais mais amplos; ausência de objetivo claro - manutenção de dados "só por precaução" (neste caso, não há adequação a nenhuma base); possibilidade de se alcançar resultado final sem usar dados pessoais; ausência de vontade de assumir total responsabilidade pela proteção dos interesses do indivíduo, ou preferiria colocar o ônus sobre o indivíduo; pretensão de utilizar os dados pessoais de uma forma que as pessoas não conhecem e não esperam (a menos que se tenha uma razão mais convincente que justifica a natureza inesperada do processamento); risco de dano significativo (a menos que se tenha uma razão mais convincente que justifique o impacto); ausência de confiança no resultado do teste de equilíbrio; temor a respeito de publicidade negativa sobre a forma de utilização dos dados; ou outra base legal mais obviamente aplicável a um propósito particular. Embora, em teoria, mais de uma base legal possa se aplicar ao seu processamento, na prática é improvável que interesses legítimos sejam apropriados para qualquer finalidade de processamento onde outra base se aplique objetivamente”. Discorda-se da última ponderação à luz do princípio da livre circulação de dados e da ausência de hierarquia entre as bases legais. INFORMATION COMMISSIONER'S OFFICE (ICO-UK), **What is the ‘legitimate interests’ basis?**, p. 30.

³⁰⁸ PONCE; MATTIUZZO, O legítimo interesse e o teste da proporcionalidade, p. 61.

³⁰⁹ BRASIL. Câmara Legislativa. **Relatório da Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, DE 2012 (Tratamento e Proteção de Dados Pessoais)**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305>. Acesso em 11 abr. 2021, p.34.

Importa destacar que, em um primeiro momento, o ônus de demonstrar a finalidade legítima do processamento pode parecer limitante da atividade desempenhada pelo agente, todavia, ao assim proceder, os passos subsequentes no transcurso do procedimento de tratamento fluirão de modo mais fácil, pois, quanto mais detalhada e documentada sua ação, mais simples será a justificação racional da atividade no teste de balanceamento realizado, bem como a verificação do cumprimento dos demais deveres.

De outro lado, quanto mais genérica for a motivação do legítimo interesse, mais improvável será a demonstração de atuação em consonância com a lei, aumentando-se a possibilidade de incidência dos dispositivos referentes ao descumprimento da LGPD.

Ademais, consoante se vem defendendo no presente trabalho, o direito fundamental à proteção de dados protege o indivíduo e não os dados em si. É dizer: o referencial é a pessoa titular de dados e seus interesses devem ser preservados na maior medida possível.

Essa afirmação gera consequências diretas na atuação dos agentes de tratamento: primeiro, o fundamento de licitude adotado para tratar certos dados não autoriza novo tratamento dissociado da primeira finalidade apresentada. Segundo, as restrições para o tratamento de dados devem ser observadas durante todos os processos, sejam os já iniciados ou os que se pretende iniciar por meio da indicação de nova base legal.

Em suma, o tratamento lícito desenvolvido pelo agente não lhe garante o direito subjetivo de proceder do modo que bem entender a outras formas de processar os elementos de informação recolhidos³¹⁰. A observância do princípio da finalidade, sob essa perspectiva, funciona como instrumento redutor da assimetria informacional.

2.3.2.3. Dever de respeito às legítimas expectativas (boa-fé) e direitos fundamentais dos titulares

A boa-fé é princípio que tangencia todo o direito privado e público e deve nortear a atuação responsável daqueles que participam de qualquer relação jurídica. A atuação das partes há de ser cooperativa e todos os envolvidos devem se perceber como parceiros, os quais estão

³¹⁰ DÖHMANN, A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia, p. 120.

obrigados a se respeitar mutuamente e a dirigir suas condutas ao cumprimento do objeto da relação jurídica com absoluta lealdade³¹¹.

Deveras, há estreita correlação entre o princípio da boa-fé e o respeito às expectativas legítimas nas relações interpessoais. Essa aproximação se manifesta através do reconhecimento do princípio da confiança, o qual edifica, no plano jurídico-positivo, o liame entre esses institutos³¹². Marques destaca que a “a confiança (proteção da confiança legítima) [parece] ser o paradigma para os tempos digitais”³¹³.

Nesse diapasão, é oportuno pontuar que o princípio da boa-fé recebeu destaque do legislador no *caput* do art. 6º da LGPD³¹⁴.

A expectativa legítima, sob o influxo dos valores consagrados pela LGPD, é dotada de densidade jurídica suficiente para deslocá-la do campo retórico para o principiológico, normativo³¹⁵.

³¹¹ CARVALHO, Diógenes Faria de; MARQUES, Claudia Lima, Os significados da boa-fé nos contratos de serviços massificados: convergências entre o CDC, o CC/2002 e a Lei da Liberdade Econômica, *in*: MARQUES, Claudia Lima *et al* (Eds.), **Contratos de serviços em tempos digitais: contribuição para uma nova teoria geral dos serviços e princípios de proteção dos consumidores [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2021. Os autores consideram que “[b]oa-fé nos contratos, em especial nos contratos de serviços ou “fazeres” “massificados” significa uma atuação “refletida”, atuação refletindo, pensando no outro, no parceiro contratual, respeitando-o, respeitando seus interesses legítimos, seus direitos, respeitando os fins do contrato, agindo com lealdade, sem abuso da posição contratual, sem causar lesão ou desvantagem excessiva, com cuidado para com a pessoa e o patrimônio do parceiro contratual, cooperando para atingir o bom fim das obrigações (isto é, o cumprimento do objetivo contratual e a realização dos interesses legítimos de ambos os parceiros)”.

³¹² Para Antonio Menezes Cordeiro: “[n]as suas manifestações subjectiva e objectiva, a boa fé está ligada à confiança: a primeira dá, desta, o momento essencial; a segunda confere-lhe a base jus positiva necessária quando, para tanto, falte uma disposição legal específica. Ambas, por fim, carregam as razões sistemáticas que se realizam na confiança e justificam, explicando a sua dignidade jurídica e cuja projecção transcende o campo civil”. *In*: CORDEIRO, Antonio Menezes, **Da boa fé no direito civil**, Coimbra: Almedina, 2013, p. 1250.

³¹³ MARQUES, Claudia Lima, Função Social do contrato como limite da liberdade de contratar e a confiança legítima no resultado em tempos digitais, *in*: MARQUES, Claudia Lima *et al* (Eds.), **Contratos de serviços em tempos digitais: contribuição para uma nova teoria geral dos serviços e princípios de proteção dos consumidores [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2021.

³¹⁴ Do ponto de vista dogmático, Carvalho e Marques destacam que “a boa-fé é um princípio do ordenamento jurídico, ao qual devem se dobrar as normas de Direito estrito, a fim de se atingir a promoção da justiça na solução dos casos concretos. O entendimento da boa-fé como princípio é corroborado pelos seguintes autores: Maria Helena Diniz, Eros Grau, Caio Mário, Miguel Reale, Karl Larenz, Ruy Rosado de Aguiar, dentre outros”. *In*: CARVALHO; MARQUES, **Os significados da boa-fé nos contratos de serviços massificados: convergências entre o CDC, o CC/2002 e a Lei da Liberdade Econômica**.

³¹⁵ O princípio da confiança desponta como vetor interpretativo interessante a ser adotado, como mencionado por Oliveira e Cots: “(...) a proteção da confiança, com o Código Civil de 2002, saiu da questão meramente ética ou moral e se tornou uma necessidade do modelo jurídico e do contexto social em que se insere, e que já vinha ganhando forma desde a edição do Código de Defesa do Consumidor em 1990. A proteção da confiança legítima atua como uma proteção das legítimas expectativas, bem como justifica a vinculação entre as partes à relação jurídica. Portanto, o princípio da confiança busca proteger as expectativas legítimas criadas pela conduta de terceiros, ao proteger os indivíduos de um eventual ardil de terceiros, a quem se confiou, ao atrair para o seu plano outros dois princípios, quais sejam, da boa-fé e da segurança jurídica”. *In*: OLIVEIRA; COTS, **O legítimo interesse e a LGPD**, p. 115–116.

Desse modo, não é incorreta a premissa de que a confiança se consubstancia em estado psicológico determinante na construção de relações das mais variadas espécies e, no campo do direito, ganha especial relevância, porquanto ostenta o condão de motivar a assunção de obrigações recíproca ou unilateralmente. Essa característica denota a imprescindibilidade de se lhe atribuir proteção jurídica³¹⁶.

O Supremo Tribunal Federal entende o princípio da confiança como instituto jurídico que guarda estreita correlação com o postulado da segurança jurídica e com a própria manutenção do Estado de Direito³¹⁷. Ainda que essa abordagem se dê majoritariamente em situações envolvendo comportamentos estatais³¹⁸⁻³¹⁹, esse entendimento é plenamente aplicável à tutela da proteção de dados.

Para a doutrina especializada no campo específico do tratamento de dados, a boa-fé pode ser funcionalizada a partir do reconhecimento de deveres de conduta atribuídos ao agente de tratamento, a exemplo: a) da lealdade junto ao tratamento de dados, respeitadas as legítimas expectativas dos indivíduos, fontes de dados, ainda que em situações de uso para situações diversas das inicialmente apresentadas; e b) do exercício da posição jurídica dissociado da

³¹⁶ A propósito, vale a menção à lição de Araújo: “[p]ara merecer proteção jurídica, a confiança não deve ser identificada como um mero estado psíquico interno, mas precisa ser compreendida como um sentimento que foi capaz de se manifestar através de um comportamento específico. Isso leva THOMAS PROBST a concluir que ‘o princípio da proteção da confiança’ tem como tarefa prevenir a ocorrência de desvantagens reais e injustas e não a mera proteção do bem-estar psíquico de sujeitos jurídicos’. Deve, inclusive, existir uma relação de causalidade (kausalzusammenhang) entre a confiança do particular e os seus atos concretos. É preciso que ele tenha atuado em razão da confiança depositada no ente estatal. Se o indivíduo não tivesse acreditado na manutenção do ato estatal, não teria agido da maneira que agiu”. ARAÚJO, Valter Shuenquener de, **O princípio da proteção da confiança: uma nova forma de tutela do cidadão diante do Estado.**, Niterói: Impetus, 2009. p. 98.

³¹⁷ MARTINS-COSTA, Judith, **A Re-significação do Princípio da Segurança Jurídica na Relação entre o Estado e os Cidadãos: a segurança como crédito de confiança**, n. 27, p. 110–120, 2004.

³¹⁸ BRASIL. Supremo Tribunal Federal (1. Turma). **Segundo Recurso Extraordinário com Agravo nº 950.586**. Rel. Min. Roberto Barroso. Diário da Justiça eletrônico de 19 jun. 2019. Ementa: DIREITO ADMINISTRATIVO. SEGUNDO AGRAVO INTERNO EM RECURSO EXTRAORDINÁRIO COM AGRAVO. CONCURSO PÚBLICO. MANDADO DE SEGURANÇA. EXCEÇÃO TEORIA FATO CONSUMADO. 1. A desconstituição do ato de promoção do impetrante representa clara violação aos princípios da segurança jurídica e da confiança legítima, situação que se enquadra na excepcionalidade reconhecida no julgamento do RE 608.482-RG. 2. Inaplicável o art. 85, § 11, do CPC/2015, uma vez que não houve fixação de honorários advocatícios (art. 25 da Lei nº 12.016/2009 e Súmula 512/STF). 3. Agravo interno a que se nega provimento.

³¹⁹ Ainda relacionado ao tema, José Afonso da Silva, ao discorrer sobre a necessidade de se assegurar o valor da segurança jurídica, especialmente no que tange à estabilidade dos direitos subjetivos, preleciona que a segurança jurídica consiste no “conjunto de condições que tornam possível às pessoas o conhecimento antecipado e reflexivo das consequências diretas de seus atos e deus fatos à luz da liberdade reconhecida”. Uma importante condição da segurança jurídica está na relativa certeza de que os indivíduos têm de que as relações realizadas sob o império de uma norma devem perdurar ainda quando tal norma seja substituída”. In: SILVA, José Afonso da, **Curso de Direito Constitucional Positivo**, São Paulo: Malheiros, 2015. P.436

prática de abusos, ou seja, observada e resguardada a finalidade econômica que motivou o processamento³²⁰.

Oliveira e Cots propõem limite à compreensão da expectativa legítima ao ponderarem que esse princípio não tutela o estado de ânimo de um sujeito que espera de outro determinado comportamento com base em conduta prévia desse em relação jurídica distinta. Portanto, a conduta contrária à legítima expectativa deve abalar a relação jurídica na qual o vínculo de confiança foi construído e não outra distinta da original³²¹.

É certo que se deve garantir às pessoas condições para o livre desenvolvimento de sua personalidade, sob os prismas individual e comunitário. Assim, o estímulo à consolidação de ambiente de cooperação entre agentes de tratamento e titulares de dados também contribui para se diminuir a assimetria de forças usualmente existente nas relações dessa natureza.

Outrossim, a adoção do legítimo interesse como fundamento para o tratamento de dados pessoais, não desobriga aquele que pretende desenvolver essa atividade da observância dos princípios gerais insculpidos na LGPD e, tampouco, do dever preservar os direitos do titular (art.7º, § 6º). Neste passo, há que se garantir meios de fiscalização da aderência do processamento das informações à finalidade do tratamento.

Por conseguinte, é evidente que se cuida de conceito importante e a sua positivação em lei³²², embora sua previsão não seja novidade no ordenamento jurídico brasileiro, estabelece elemento normativo facilitador da definição de seus limites pelo Poder Judiciário, principalmente se considerada a gênese do legítimo interesse.

³²⁰ Bioni e outros consideram que “o princípio da boa-fé irradia a existência de um dever de conduta por parte do agente de tratamento de dados, com destaque para: (i) lealdade junto ao titular dos dados, de sorte que não frustre a confiança nele depositada, o que somente é aferível caso a caso; com isso, abre-se espaço para que haja novos usos (secundários) dos dados, mas que não contrariem o contexto do fluxo informacional; e (ii) cuidado, que está ligado à noção de abuso de direito, isto é, que o direito em processar dados pessoais não “exceda manifestamente os limites impostos pelo seu fim econômico ou social, [...] pelos bons costumes”. Nesse sentido, o instituto do abuso de direito seria o portal de entrada para os ‘os limites éticos e sociais impostos a uma atividade’, justamente em um momento em que se verifica uma guinada da ética em meios aos debates regulatórios sobre as novas tecnologias”. BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 30.

³²¹ Para os autores: “foge do âmbito de aplicação desse princípio aquele sujeito que confia em outro, com base no comportamento que este teve com outra situação jurídica, ainda que, nesse caso, aquele que confia esteja ou possa vir a ser protegido pela boa-fé”. OLIVEIRA; COTS, **O legítimo interesse e a LGPD**, p. 117.

³²² arts. 6º e 10, II, da LGPD.

Dessume-se, portanto, o papel central da boa-fé enquanto baliza principiológica de aplicação da LGPD. A base legal do legítimo interesse está inserida dentro desse sistema e deve observar esse postulado³²³.

O exercício disfuncional da atividade do agente de tratamento deve ser repellido e uma forma de se neutralizar esse comportamento indesejado é seguir o caminho adotado pelo legislador, ao estabelecer a obrigatoriedade de não se frustrarem as legítimas expectativas do titular de dados.

Não se ignora que os valores sociais e culturais variam conforme o tempo e o espaço, de sorte que se impõe a leitura da legítima expectativa à luz de sua categoria de cláusula geral. Por exemplo, até pouco tempo atrás não se poderia cogitar de que o consumidor que adquirisse um refrigerador³²⁴ ou aparelho de televisão³²⁵, tivesse a legítima expectativa de ter os dados de uso desses equipamentos processados. Hoje, com a realidade da internet das coisas, muitos desses dispositivos, para funcionarem segundo as prescrições do fabricante, se conectam às redes domésticas e, por via de consequência, à rede mundial de computadores e promovem alguma forma de tratamento de dados.

Certamente, a casuística é que permitirá se estabelecer se em determinado caso concreto o tratamento de dados ocorreu com quebra da legítima expectativa do titular. Por esse motivo, o art. 37 da LGPD evidencia o dever de o controlador e operador manterem "registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

³²³ Nesse diapasão, Oliveira e Cots: “[a]ssim, a legítima expectativa do titular de dados, consubstanciada no Princípio da confiança, que se encontra em diversos dispositivos da legislação brasileira e agora consolidada especificamente, quanto à proteção de dados, no art. 10 e inciso II, da Lei nº 13.709/2018, deve corresponder aos fins que lhe foram informados e para os quais consentiu com o tratamento de seus dados pessoais, como substituição do conceito subjetivo por uma análise objetiva da correspondência entre a finalidade informada ao titular e aquela efetivamente dada às informações”. OLIVEIRA; COTS, **O legítimo interesse e a LGPD**, p. 119.

³²⁴ CIPL, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation**, p. 14.

³²⁵ “Sua *smart* TV provavelmente está coletando informações através de uma tecnologia chamada “reconhecimento automático de conteúdo” (RAC). Ela tenta identificar tudo o que você assiste na TV e envia os dados para o fabricante da TV, para terceiros, ou para ambos. Pesquisadores descobriram que uma *smart* TV da Samsung havia se conectado a mais de 700 endereços distintos na internet após ter sido usada por quinze minutos”. *In*: VÉLIZ, **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**, p. 27.

Nesse contexto, o dever de transparência, associado ao de registro das operações de tratamento, viabiliza o exercício do controle, pelo titular, do tratamento de seus dados por quem quer seja³²⁶⁻³²⁷.

Afinal, não só nas situações de conflito (é possível que, por vezes, os interesses sejam convergentes) a proteção dos dados pessoais e o livre desempenho de atividade econômica pelo agente de tratamento devem se pautar pela busca do ponto de equilíbrio almejado pelo legislador.

2.3.2.4. Dever de uso dos dados estritamente necessários à finalidade pretendida.

No que tange ao dever de uso dos dados estritamente necessários à finalidade pretendida, o artigo 6º, III, da LGPD prevê o princípio da necessidade, o qual limita o "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".

Há que se fazer leitura correta da expressão "estritamente necessários" para se estabelecer o seu alcance em consonância com a lei. Portanto, considera-se que: i) o agente de tratamento não pode tratar todos os dados com os quais tenha contato ou quaisquer dados que deseje; e ii) a previsão do uso de dados estritamente necessários em relação à base legal legítimo interesse não implica ausência de obrigatoriedade desse limite em relação às outras hipóteses previstas no art. 7º.

³²⁶ Na linha do aqui defendido, o artigo 9º da LGPD dispõe, *in verbis*: art. 9º 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; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. § 2º 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 o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações. § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

³²⁷ Nesse sentido, Mario Viola e Chiara de Teffé destacam: (...) a importância dos princípios da transparência, adequação e finalidade para restringir tanto a generalidade na utilização dos dados quanto tratamentos opacos. Para diminuir as assimetrias técnica e informacional existentes entre as partes, exige-se que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados. VIOLA; TEFFÉ, **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o e 11**, p. 136.

Decerto, pretendeu o legislador reforçar o dever de os agentes de tratamento coletarem e utilizarem apenas os dados imprescindíveis ao atendimento da finalidade estabelecida.

No ponto, cumpre destacar a existência de entendimentos doutrinários que consideram, dentro da necessidade (etapa do teste de ponderação), a valoração realizada pelo agente de tratamento sobre a possibilidade de escolha de outra base legal menos intrusiva ou mais adequada em vez do legítimo interesse³²⁸.

Discorda-se de tal posicionamento. Primeiro, porque, consoante já demonstrado, não há hierarquia entre as bases legais de tratamento. Segundo, o exame da base legal adequada ao tratamento se dá em momento anterior ao da realização do teste de proporcionalidade, o qual tem por pressuposto lógico a escolha prévia do legítimo interesse como fundamento de licitude para o tratamento de dados.

Não se está a defender, contudo, que o controlador deve optar pelo legítimo interesse sempre que lhe for possível. Não há dúvidas de que sua atuação deve se pautar pelos fundamentos e princípios insculpidos na LGPD.

A escolha dessa base legal deve ser juridicamente justificável sem se perder de vista que a proteção de dados, enquanto direito fundamental, impõe a interpretação da lei à luz da Constituição. Logo, a mínima intrusão na esfera individual dos titulares deve nortear a atuação do agente de tratamento em qualquer circunstância.

Reitere-se que a opção pelo legítimo interesse não é mais ou menos idônea do que qualquer outra hipótese contida no art. 7º da LGPD. Todavia, a preferência por essa base legal deve conduzir o comportamento do agente de tratamento, de sorte que o ônus argumentativo será mais intenso, bem como o dever de documentação do processo racional de escolha pelo legítimo interesse será qualificado, nos termos do art. 37 do apontado diploma normativo³²⁹.

Com efeito, não há como estabelecer aprioristicamente o que seriam “dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento”³³⁰. A relação proporcional e não excessiva entre os dados que se pretende tratar e a finalidade que fundamenta o tratamento é determinada caso a caso, de modo contextualizado.

³²⁸ BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**; TEFFÉ; VIOLA, **Tratamento de dados pessoais na LGPD**.

³²⁹ Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

³³⁰ Art. 6º, III, LGPD.

Em suma, o controlador deve utilizar apenas os dados essenciais à consecução da finalidade de sua atividade e, somente à luz do caso concreto, é que se poderá avaliar se os dados colhidos não transbordaram os limites do estritamente necessário.

2.3.2.5. Dever de transparência

Quanto ao dever de transparência, o art. 6º, VI, da LGPD, estabelece 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".

Cuida-se de princípio que encontra larga base normativa dentro do que se pode chamar de microsistema de proteção de dados pessoais (art. 64), a exemplo do art. 4º do Código de Defesa do Consumidor³³¹. Assim, o agente de tratamento deve informar ao titular sobre sua atividade de modo claro, preciso e compreensível.

Nesse seguimento, antes, durante e, mesmo após o tratamento de dados, o controlador deve disponibilizar, de modo inequívoco e descomplicado, as informações pertinentes ao desenvolvimento dessa atividade, tais como a base legal, a finalidade e a forma que se realiza, sendo de todo aplicável a doutrina³³² e o entendimento jurisprudencial³³³ prevalecentes em torno da boa-fé contratual na relação consumerista à LGPD.

Indra Döhmman ao discorrer sobre o princípio da transparência no tratamento de dados pessoais, lhe atribui dupla dimensão. Para a autora, a transparência se desdobra em dois

³³¹ Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: (...). *In*: BRASIL. **Lei Nº 8.078, de 11 set. de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, Diário Oficial da União de 12 set. 1990, retificado em 10 de jan. de 2007.

³³² Para Leonardo Bessa: “[n]o direito obrigacional, a boa-fé objetiva molda a nova teoria contratual, exigindo das partes a construção de ambiente de solidariedade, lealdade, transparência e cooperação. A boa-fé diz respeito ao exame objetivo e geral da conduta do sujeito em todas as fases contratuais (pré-contratual, contratual e pós-contratual), servindo, a partir de suas funções, como parâmetro de interpretação dos contratos, identificação de abuso de direito e criação de deveres anexos. O contrato, embora legítimo instrumento para a circulação de riquezas e a satisfação de interesses econômicos (lucro), não deve mais ser visto sob ótica individualista. Importa analisar sua função econômica e social.”. *In*: BESSA, Leonardo Roscoe. **Código de Defesa do Consumidor comentado**. Rio de Janeiro: Forense, 2021, p.29.

³³³ BRASIL. Superior Tribunal de Justiça (1 Seção). **Recurso Especial nº 976.836**. Rel. Min. Luiz Fux. Ementa: (...) é forçoso concluir que o direito à informação tem como desígnio promover completo esclarecimento quanto à escolha plenamente consciente do consumidor, de maneira a equilibrar a relação de vulnerabilidade do consumidor, colocando-o em posição de segurança na negociação de consumo, acerca dos dados relevantes para que a compra do produto ou serviço ofertado seja feita de maneira consciente. (...). Publicação: 5 out. 2010. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=924969&num_registro=200701873706&data=20101005&formato=PDF. Acesso em 4 dez. 2021.

aspectos: a) o titular de dados deve ter condições de controlar a forma como seus dados são tratados; e b) o agente de tratamento está obrigado a, durante todo o processo de tratamento, demonstrar a licitude de sua atuação a qual deve ser documentada³³⁴. Embora a autora tenha desenvolvido a ideia à luz do GDPR, cuida-se de raciocínio aplicável à LGPD, principalmente se considerados o princípio da autodeterminação informativa e a influência do diploma europeu na gênese do brasileiro.

Nesse contexto, faz-se menção ao art. 9º, § 3º, da LGPD, segundo o qual, na hipótese de tratamento de dados pessoais como "condição para o fornecimento de produto ou de serviço ou para o exercício de direito", haverá obrigação de informação ao titular "com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 daquela Lei".

Dessume-se, portanto, a intenção do legislador de garantir a possibilidade de controle posterior da conduta do controlador, seja pelos titulares de dados, seja por agentes reguladores.

Sem transparência não é possível acompanhar e fiscalizar a atividade do agente de tratamento de dados, principalmente no que diz respeito ao teste de balanceamento. Cuida-se de instrumento viabilizador do exercício de controle do titular sobre suas próprias informações.

Nesse cenário, medidas de transparência ativa exsurtem como elementos relevantes no controle da atividade dos agentes de tratamento. Deveras, essa é a premissa para a participação efetiva dos indivíduos, fontes de dados, no processamento e circulação de informações sobre si, sendo certo, também, que a quantidade e qualidade das informações fornecidas possibilitam uma série de usos secundários pelos agentes de tratamento.

É premente a necessidade de reforço da posição jurídica do titular através da previsão da implementação de instrumentos de controle e fiscalização do tratamento de dados. A propósito, para Bioni e outros³³⁵:

(...) práticas de transparência ativa possuem fundamental relevância, pois servem como forma de controle social e não apenas individual. Adotando a perspectiva de que a proteção de dados tutela bens jurídicos de interesse da coletividade, como a não discriminação e a dignidade humana, a publicidade sobre as práticas de tratamento é de extrema importância. Há casos em que o tratamento abusivo de dados leva a

³³⁴ Segundo a autora, “o princípio da transparência, contido em essência no art. 5º, par. 1, alínea “a”, do RGD, tem dois elementos que o concretizam e encontraram fundamentos próprios em diversas passagens do Regulamento para além da formulação genérica: por um lado, o titular dos dados deve ter condições de proceder a um controle próprio da forma como se lida com os dados. Para isso, são consagrados diversos direitos no RGD. Por outro lado, porém, o responsável pelo tratamento também deve ser obrigado a proceder a uma verificação prospectiva da licitude do tratamento de dados, acompanhada de um dever de documentação”. *In*: DÖHMANN, **A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia**, p. 123.

³³⁵ BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 35.

violações de direitos afetos a todo um segmento populacional, sendo conhecidas as situações de discriminação por raça, gênero e perfil socioeconômico em virtude de usos abusivos de dados pessoais. A transparência ativa das empresas desempenha também um papel de responsabilidade social, sujeitando suas próprias práticas à apreciação pública, de um lado; e criando uma cultura que padroniza essa atitude nos mercados, de outro.

Além disso, no que diz respeito ao legítimo interesse, a transparência serve como ferramenta de contenção da prática de abusos por parte do agente de tratamento, pois não basta a indicação genérica da realização de tratamento de dados com fundamento nesse permissivo legal.

De igual sorte, a finalidade do tratamento deve ser clara o suficiente para permitir a verificabilidade do enquadramento legal proposto pelo controlador, bem como a sua observância no processamento e uso ulterior dos dados.

Ao titular de dados, portanto, se deve garantir o acompanhamento e controle das atividades de tratamento que lhe digam respeito. E não só na perspectiva individual, uma vez que os dados são tratados em grande escala. Assim, pode-se pensar, também, na possibilidade de controle por parte de toda a sociedade e na inerente dimensão coletiva do tratamento de dados³³⁶.

2.3.2.6. Dever de documentação da atividade de tratamento

No que concerne ao dever de documentação do racional de tratamento de dados, o art. 37 da LGPD prevê que a obrigatoriedade de o controlador e operador manterem registro das operações de tratamento de dados pessoais que realizarem, em especial quando o fundamento for o legítimo interesse³³⁷.

Infere-se que a LGPD, conquanto não tenha estabelecido forma pré-definida, o que pode ser um problema no momento da materialização da lei no plano concreto, estabelece o dever geral de documentação da atividade de tratamento como um todo.

³³⁶ BESSA; NUNES, **Instrumentos processuais de tutela individual e coletiva: análise do art. 22 da LGPD**.

³³⁷ Ponce e Mattiuzo apontam que o “art. 37 da LGPD estabelece um dever geral de registro de quaisquer operações de tratamento de dados pessoais realizadas. Afinal, trata-se de medida necessária para o atendimento dos direitos dos titulares, como, por exemplo, a confirmação de tratamento e o direito de acesso, e também a responsabilização e prestação de contas com relação a tratamentos já realizados. O mesmo art. 37, por sua vez, estabelece que essa disposição é especialmente aplicável no caso de tratamentos de dados pessoais realizados a partir do legítimo interesse, isto é, a lei orienta que nestas oportunidades a manutenção de registros pelo agente de tratamento é, além de obrigatória como as demais, de suma relevância”. In: PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 70.

No caso específico do legítimo interesse, o registro da atividade de tratamento ganha contorno diferenciado, principalmente quando se considera o teste de balanceamento - *Legitimate Interest Assessment* (LIA) e o dever especial de manter registro das operações de tratamento de dados pessoais quando baseado nesse fundamento de licitude.

Por se cuidar de base legal que confere ao controlador ampla discricionariedade no que concerne à opção pelo tratamento, o registro da atividade acaba por se consubstanciar em limite à sua atuação, uma vez que é seu o ônus de demonstrar a conformidade legal do tratamento cujo fundamento adotado prévia e unilateralmente foi o legítimo interesse.

Em relação ao Relatório de Impacto, de acordo com o art. 10, § 3º, da LGPD, a "autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver por base seu interesse legítimo, observados os segredos comercial e industrial".

Ressoa inequívoco que o próprio legislador condicionou a obrigatoriedade de sua elaboração à solicitação da autoridade nacional. Porém, nada impede que o controlador proceda à sua confecção de forma concomitante, enquanto se desincumbe do ônus de manter o registro de suas atividades de tratamento.

Desse modo, acaso observe o art. 37 da LGPD durante todo o desenvolvimento de sua atividade, o agente de tratamento terá todos os elementos necessários à elaboração do referido documento.

Sob essa perspectiva, a elaboração do relatório de impacto de proteção de dados mais se aproxima de um instrumento de boa prática³³⁸ de governança corporativa do que de uma obrigação para todo e qualquer tratamento que adote o legítimo interesse como base legal³³⁹.

Aqui, há mais uma diferença relevante em relação ao GDPR, pois o regime jurídico europeu traz a obrigação imediata de preparação de relatório de impacto, *Data Protection*

³³⁸ Quanto ao tema da adoção de boas práticas no tratamento de dados pessoais, Frazão, Oliva e Abilio apontam que a sua implementação "possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus *standards* e conceitos abertos". In: FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira, *Compliance de dados pessoais*, in: **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no direito brasileiro [livro eletrônico]**, 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

³³⁹ Nesse sentido, Gomes: "(...) o papel do relatório de impacto é ser uma ferramenta de governança de dados a ser internalizada no cotidiano da organização, não apenas um documento para ser utilizado durante um processo de adequação regulatória. Isso para que todos os processos que envolvam tratamento de dados, atuais e novos, possam garantir o atendimento e a preservação dos direitos dos titulares de dados". In: GOMES, Maria Cecília Oliveira, *Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD.*, **Revista do Advogado**, v. 144, 2019, p. 180.

Impact Assessment (DPIA), referente ao tratamento de dados pessoais quando esse "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares"(artigo 35º)³⁴⁰, enquanto não se pode extrair essa obrigação a partir da leitura da LGPD, em especial dos arts. 10, § 3º, e 38³⁴¹.

No que diz respeito à forma, consoante já abordado, a lei não estabeleceu solenidade específica para o relatório, e nem seria recomendável, pois a gama de atividades e de porte de agentes econômicos é imensurável. Nada obsta, todavia, que a autoridade nacional, no desempenho de sua função de implementar e fiscalizar o cumprimento da LGPD elabore, dentro dos limites legais, documentos ou atos normativos infralegais que versem sobre esse documento³⁴².

Calha destacar, ainda, que, a partir da compreensão do no art. 38, parágrafo único, da LGPD, se pode delinear o conteúdo mínimo que o relatório de impacto deve ostentar. De acordo com o dispositivo, "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 risco adotados".

Nesse trilhar, releva notar a imprescindibilidade de que se faça leitura sistemática da lei, a fim de se minimizar os riscos de responsabilização, pelo menos no caso de tratamento de dados fundamentado no legítimo interesse.

Assim, já que o controlador, enquanto registra suas atividades nos termos do preconizado pelo art. 37 da LGPD, deve buscar indicar os tipos de dados coletados e a metodologia utilizada para coleta, nada obsta a que proceda, de modo concomitante, à

³⁴⁰ UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

³⁴¹ Art. 10. 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 se limitam a: (...) § 3º 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.

Art. 38. 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 comercial e industrial.

³⁴² Destaca-se o art. 2º, XIII, do Decreto Nº 10.474, de 26 de agosto de 2020, o qual prevê ser competência da ANPD editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade e 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 Lei nº 13.709, de 2018. BRASIL. Poder Executivo. **Decreto Nº 10.474, de 26 de agosto de 2020**. Diário Oficial da União de 27/08/2020.

elaboração de esboço do relatório de impacto de tratamento, uma vez que se cuida de pressupostos para a sua operação³⁴³.

Cabe destacar, por oportuno, que o registro do tratamento não se confunde com o relatório de impacto à proteção de dados pessoais, embora ambos guardem pontos de convergência entre si.

Primeiramente, se percebe que se trata de institutos previstos em dispositivos distintos. Em segundo lugar, se distinguem em seu objetivo: enquanto o registro das atividades tem por fim permitir a subsunção entre a hipótese legal de tratamento e a situação concreta, o relatório versa sobre o tratamento do dado em si, em ordem a se permitir o escrutínio do tratamento de dados pelos órgãos de controle.

O cumprimento desses deveres identificados certamente permitirá aos titulares de dados o controle sobre os elementos de informação que lhes digam respeito, além de fortalecer a proteção contra condutas abusivas, ao mesmo tempo em que orientará a conduta dos agentes de tratamento que deverão desenvolver sua atividade de forma transparente e de acordo com os fundamentos e princípios da LGPD.

2.3.3. A impossibilidade tratamento de dados pessoais sensíveis com base no legítimo interesse à luz do art. 11 da LGPD

A proteção jurídica dos sujeitos de direitos adquire novos significados conforme as circunstâncias que cercam o homem e a vida em sociedade mudam. A cláusula geral da dignidade da pessoa humana confere ao direito fundamental à proteção de dados pessoais ductibilidade suficiente para se permitir a edificação de contramedidas à novas formas de constrição e de ameaças ao livre desenvolvimento da personalidade.

Esse fenômeno é facilmente perceptível a partir do já abordado exame da evolução da tutela da privacidade a qual, do enfoque no direito a ser deixado só, desenvolvido no século XIX, de cunho marcadamente estático, passou, nas últimas décadas do século XX, à autodeterminação informativa, sendo evidente seu caráter dinâmico.

³⁴³ Nesse sentido, Ponce e Mattiuzo: “(...) na medida em que o art. 10, §3º especificamente prevê que a ANPD poderá requisitar relatório para todo e qualquer caso de tratamento que tenha como base legal o legítimo interesse, é recomendável analisar e considerar desde o primeiro momento se um relatório deste tipo não deve ser elaborado desde o princípio do processo. Embora esta disposição não implique que o legítimo interesse seja hipótese única de demanda por relatório de impacto à proteção de dados pessoais, demonstra que o relatório é encarado como medida de transparência e accountability, particularmente relevante nos termos do dever especial de transparência previsto com relação ao legítimo interesse”. *In*: PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 70–71.

Para Rodotà, os dados sensíveis seriam o “núcleo duro” da privacidade e a proibição de sua coleta estaria atrelada à finalidade de impedir discriminações abusivas entre os cidadãos em fortalecimento do princípio da igualdade³⁴⁴.

No direito comparado, a previsão de “dato sensível”, objeto de tutela especial, existe, pelo menos, desde a Diretiva europeia de 1995³⁴⁵. No GDPR, os dados sensíveis também foram reconhecidos como categoria jurídica destinatária de proteção específica, porquanto estreitamente relacionados a direitos e liberdades fundamentais³⁴⁶.

No ordenamento pátrio, conquanto sua previsão legal não seja novidade³⁴⁷, segundo o artigo 5º, II, da LGPD, dado pessoal sensível é aquele relacionado à “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,

³⁴⁴ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 78–79.

³⁴⁵ Por oportuno, faz-se menção ao Considerando 34 daquele documento: “[c]onsiderando que, sempre que um motivo de interesse público importante o justifique, os Estados-membros devem também ser autorizados a estabelecer derrogações à proibição de tratamento de categorias de dados sensíveis em domínios como a saúde pública e a segurança social - em especial para garantir a qualidade e a rentabilidade no que toca aos métodos utilizados para regularizar os pedidos de prestações e de serviços no regime de seguro de doença - e como a investigação científica e as estatísticas públicas; que lhes incumbe, todavia, estabelecer garantias adequadas e específicas para a protecção dos direitos fundamentais e da vida privada das pessoas”. *In*: UNIÃO EUROPEIA, **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>>. Acesso em: 6 jul. 2021.

³⁴⁶ GDPR, Considerando 51: “[m]erecem protecção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de protecção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, *designadamente* quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais”. *In*: UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

³⁴⁷ É possível encontrar tratamento específico de dados considerados sensíveis em leis anteriores, a exemplo da Lei do Cadastro Positivo (Lei 12.414/11), em seu art. 3º, § 3º, II, o qual dispõe, *in verbis*: “§ 3º Ficam proibidas as anotações de: (...) II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas”. *In*: BRASIL, **Lei Nº 12.414, de 9 jun. de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF, Diário Oficial da União de 10 jun. 2011.

filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”. Entende-se que os dados pessoais sensíveis foram conceituados de forma exemplificativa³⁴⁸, similarmente ao que sucedeu no GDPR, e receberam tratamento diferenciado pelo legislador.

Tem-se, portanto, elementos de informação que compõem as convicções dos indivíduos e, por vezes, agregam aspectos de sua identidade pública. Assim, sua disciplina específica advém da necessidade de proteção do titular contra os riscos do fluxo incessante dos dados pessoais, em especial, de sua potencial utilização com fins discriminatórios abusivos.

A técnica legislativa adotada é adequada pois se potencializa a tutela jurídica de quem se coleta esses fragmentos de informação. Demais disso, a positivação dessa categoria especial de dados tem o condão de propiciar necessária diminuição da relação assimétrica entre o agente de tratamento e o titular de dados ao buscar equilíbrio entre a proteção da privacidade das pessoas naturais e a livre circulação de dados pessoais, ambos fundamentos do microsistema de proteção de dados da pessoa natural.

No art. 11 da LGPD, estão encartadas as hipóteses de tratamento de dados sensíveis. Em relação às bases de tratamento de dados que não ostentam essa qualidade, pode-se apontar algumas diferenças: a) ao consentimento se impõe diretamente no dispositivo formalidade peculiar, qual seja sua manifestação de forma específica, destacada e vinculada a finalidades determinadas (art. 11, I)³⁴⁹; e b) a fórmula adotada pelo legislador foi a de repetir as bases legais já tratadas no art. 7º, com exceção dos incisos V (para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados), IX (para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a

³⁴⁸ Nesse sentido, Ruaro e Sarlet ponderam que: “[d]e acordo com o art. 5.º, I e II, da LGPD, os dados pessoais são, então, em princípio, todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular, enquanto os dados sensíveis são aqueles que, à guisa de exemplo, tratam sobre a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados sobre a saúde, os dados genéticos e os biométricos. Os dados sensíveis são, em vista disto, nucleares para a prefiguração e para a personificação do sujeito de direito no contexto atual”. *In*: RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales, O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – lei 13.709/2018, *in*: **Tratado de proteção de dados pessoais**, Rio de Janeiro: Forense, 2021, p. 194.

³⁴⁹ A rigor, não há, do ponto de vista do sistema protetivo da LGPD, propriamente, diferença em relação ao consentimento obtido fora do tratamento de dados sensíveis, uma vez que, como regra, tem que ser fornecido por escrito e, nessa situação, deverá constar de cláusula destacada das demais cláusulas contratuais e para finalidades determinadas (art. 8º, *caput*, §§ 1º e 4º da LGPD). Todavia a redação do dispositivo denota preocupação do legislador em minimizar os riscos de interpretações equivocadas por parte dos destinatários da norma.

proteção dos dados pessoais) e X (para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente).

Calha destacar que se o que a lei protege é o titular dos dados, o regime jurídico do processamento de dados pessoais sensíveis se aplica, inclusive, quando o tratamento inicialmente se fundamentar em base legal diversa da prevista no art. 11 mas venha a revelar dado pessoal sensível³⁵⁰.

Nessa linha, Frazão, Donato e Abilio observam que “um dado *prima facie* não sensível pode o ser por revelar, indiretamente, aspectos relacionados à origem étnica (ex., com o sobrenome), à orientação sexual (ex., com o nome do companheiro), a convicções religiosas (ex., com os nomes atribuídos aos filhos)”³⁵¹⁻³⁵².

Aqui parece haver ponto de contato com o fundamento de licitude legítimo interesse. Pois, além da proibição genérica, se a partir da ligação de dados inicialmente considerados não sensíveis se puder traçar perfil do titular, embora parcial, que reflita dado sensível, o tratamento da forma como se pretende realizar não é viável em razão de expressa vedação legal.

Ainda que não houvesse tal previsão, o art. 10, II, da LGPD, ao estatuir a necessidade de respeito aos direitos e liberdades fundamentais do titular, também inviabilizaria o processamento de dados nessa hipótese, uma vez que o tratamento, conquanto inicialmente lícito, não garante ao operador o direito subjetivo de proceder da forma que bem entender.

Devem ser observados os fundamentos da proteção de dados, previstos no art. 2º da LGPD, o dever de preservação dos direitos e liberdades fundamentais dos titulares e a estrutura axiológica desse sistema.

Imagine-se como exemplo a coleta de dados, com base no legítimo interesse, relativos a histórico de compras e de pesquisas em determinada loja de aplicativos ou serviço de consumo de mídia online, os quais, uma vez correlacionados, permitam identificar a orientação sexual ou religiosa de alguém. Em situações como essas, deve incidir o regime previsto na Seção II da

³⁵⁰ Nesse sentido, dispõe o Art. 11, § 1º, *verbis*: Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

³⁵¹ FRAZÃO; OLIVA; ABILIO, Compliance de dados pessoais, *in*: FRAZÃO, Ana; TEPEDINO, Gustavo; DONEDA, Danilo (Orgs.), **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2020.

³⁵² De igual modo, Viola e Teffé entendem que “[m]esmo os dados que, aprioristicamente, não sejam sensíveis podem assim se tornar quando, em determinado contexto fático, levarem a informações sensíveis a respeito dos titulares”. *In*: VIOLA; TEFFÉ, **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o E 11**, p. 156.

LGPD³⁵³ e o aspecto existencial do sujeito deve prevalecer sobre o interesse do agente de tratamento, ainda que legítimo³⁵⁴.

Acresça-se, ainda, a previsão constante do art. 46, §1º, da LGPD que impõe, relativamente aos dados sensíveis, a adoção de padrões técnicos mínimos na adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito³⁵⁵.

Assim, embora se revele imperioso o reconhecimento de uma régua valorativa mutante, a privacidade condiciona e é condicionada pela atuação dos agentes de tratamento e pelos valores sociais prevalentes em determinado momento. Não parece suficiente a mera identificação de categoria especial de dados e a intensificação de sua proteção.

Em nenhum momento se pode desconsiderar que se está lidando com informações relativas ao indivíduo que refletem sua colocação dentro da estrutura sociopolítica que está inserido. O sistema deve ser robustecido com mecanismos de transparência e, também, de controle, de modo que se fortaleça a posição jurídica do titular de dados³⁵⁶.

Outrossim, a ausência de autorização expressa para o tratamento de dado considerado sensível deve ser cotejada com o artigo 7, §4º, da LGPD, o qual dispensa a exigência de consentimento para o tratamento de dados "tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos [naquela] Lei". Logo, ainda que se esteja diante de dado tornado manifestamente público pelo titular, não se pode falar em ausência de proteção ou perda de sua natureza jurídica de dado pessoal³⁵⁷.

³⁵³ Seção II – Do tratamento de dados pessoais sensíveis.

³⁵⁴ KONDER, Carlos Nelson, O tratamento de dados sensíveis à luz da Lei 13.709/2018, *in*: FRAZÃO, Ana; TEPEDINO, Gustavo; DONEDA, Danilo (Orgs.), **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro [livro eletrônico]**, São Paulo: Thomson Reuters Brasil, 2020.

³⁵⁵ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. (...).

³⁵⁶ RODOTÁ, **A vida na sociedade da vigilância: a privacidade hoje.**

³⁵⁷ Por oportuno, colaciona-se trecho do parecer 6/2014, cujo raciocínio é plenamente aplicável à realidade brasileira: “[a] este respeito, pode ser relevante saber se os dados já foram tornados públicos pela pessoa em causa ou por terceiros. Neste aspeto, é importante, antes de mais, salientar que os dados pessoais, mesmo que tenham sido tornados públicos, continuam a ser considerados dados pessoais, pelo que o seu tratamento continua a exigir

Desta sorte, posiciona-se, no presente trabalho, à luz do direito posto, pela impossibilidade de coleta e tratamento de dados sensíveis, inclusive quando a partir de dados aprioristicamente considerados não sensíveis se revelar informação considerada sensível pelo legislador. Deve-se garantir ao titular a possibilidade de controle da atuação dos agentes de tratamento e, também, garantia da exatidão e do uso correto de seus dados.

2.3.4. Sobre a portabilidade dos dados coletados e tratados com base no legítimo interesse

A LGPD, dentro do capítulo referente aos direitos do titular, prevê, no art. 18, V, o direito à “portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial”.

Em primeira leitura, se pode inferir que a lei não estabeleceu qualquer limite à origem do tratamento de dados, tendo apenas estabelecido a ressalva da necessidade de se observar os segredos comercial e industrial.

Todavia, em relação ao dado processado com fundamento no legítimo interesse, se impõe leitura que privilegie a teleologia da norma, porquanto se trata de base legal que autoriza o tratamento para atender aos interesses legítimos do controlador ou de terceiro e não necessariamente do titular.

Conforme já consignado, o legislador estabeleceu balizas para as finalidades desse tratamento: a) apoio e promoção de atividades do controlador; e b) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços (pelo controlador) que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais. À luz dessas diretrizes, é lícita a conclusão de que os dados coletados e tratados com esteio nesse fundamento de licitude se destinam precipuamente ao controlador e ao seu específico modelo de negócio.

É oportuno se perceber que, ao prever o direito de portabilidade dos dados, o legislador estabeleceu a possibilidade de se regular o exercício desse direito e conferiu competência à ANPD para tanto³⁵⁸.

garantias adequadas. Não existe uma permissão generalizada para reutilizar e continuar a tratar dados pessoais tornados públicos nos termos do artigo 7.º, alínea f)”. EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conformidade o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p.61.

³⁵⁸ Cabe observar que a matéria está pendente de regulamentação pela autoridade nacional de proteção de dados.

Desta sorte, acaso se cuidasse de hipótese de plena exigibilidade pelo titular e sem possibilidade de condicionamento, não haveria essa ressalva, a exemplo do que ocorre com os direitos de confirmação da existência de tratamento, de acesso aos dados, de correção de dados incompletos, inexatos ou desatualizados, de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD. Essa lógica normativa pode ser observada, também, na previsão do direito de eliminação dos dados pessoais tratados com o consentimento do titular, uma vez que há limites ao exercício desse direito (hipóteses previstas no art. 16³⁵⁹).

Assim, entende-se que a interpretação no sentido de se extrair do art. 18, V, da LGPD, a obrigação do controlador de aquiescer imediatamente ao pedido realizado pelo titular de portabilidade de dados tratados com base no legítimo interesse extrapola a o escopo normativo da norma.

A propósito, no referido diploma legal, o princípio da transparência, expressamente estabelece a necessidade de se resguardar “os segredos comercial e industrial” (art. 6º, VI, da LGPD), os quais também devem ser observados na confecção e entrega do relatório de impacto à proteção de dados pessoais (art. 10, § 3º, da LGPD).

Então, respeitada a axiologia normativa da LGPD, parece possível, mediante a edição de ato normativo, a restrição de direitos do titular. Cabe aventar que, no direito comparado, o GDPR, no Considerando 73, é expresso quanto à possibilidade de restrição de direitos do titular³⁶⁰.

³⁵⁹ Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

³⁶⁰ Considerando 73: O direito da União ou dos Estados-Membros podem impor restrições relativas a princípios específicos e aos direitos de informação, acesso e retificação ou apagamento de dados pessoais e ao direito à portabilidade dos dados, ao direito de oposição, às decisões baseadas na definição de perfis, bem como à comunicação de uma violação de dados pessoais ao titular dos dados, e a determinadas obrigações conexas dos responsáveis pelo tratamento, na medida em que sejam necessárias e proporcionadas numa sociedade democrática para garantir a segurança pública, incluindo a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, para a prevenção, a investigação e a repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ou violações da deontologia de profissões regulamentadas, para outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, para a conservação de registos públicos por motivos de interesse público geral, para posterior tratamento de dados pessoais arquivados para a prestação de informações específicas relacionadas com o

Em doutrina estrangeira, se constata algum consenso quanto à ausência do direito de portabilidade dos dados coletados e processados com fundamento no legítimo interesse. De acordo com a organização Data Protection Network, o direito à portabilidade não seria extensível aos dados pessoais processados sob a base do legítimo interesse³⁶¹. No mesmo sentido, Zanfir-Fortuna considera que os direitos do titular de dados são inteiramente aplicáveis à base legal legítimo interesse, exceto um: a portabilidade de dados³⁶².

Em âmbito legal internacional, o Considerando 68 do GDPR corrobora esse entendimento³⁶³, assim como o artigo 20º desse diploma legal, o qual prevê o direito à portabilidade dos dados apenas se o tratamento se basear no consentimento ou em um contrato e for realizado por meios automatizados³⁶⁴.

comportamento político no âmbito de antigos regimes totalitários ou para efeitos de defesa do titular dos dados ou dos direitos e liberdades de terceiros, incluindo a proteção social, a saúde pública e os fins humanitários. Essas restrições deverão respeitar as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

³⁶¹ DPN, Data Protection Network, **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**, 2018, p. 6.

³⁶² ZANFIR-FORTUNA; TROESTER-FALK, **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases**, p. 7.

³⁶³ Considerando 68: Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. Esse direito deverá aplicar-se também se o titular dos dados tiver fornecido os dados pessoais com base no seu consentimento ou se o tratamento for necessário para o cumprimento de um contrato. Não deverá ser aplicável se o tratamento se basear num fundamento jurídico que não seja o consentimento ou um contrato. Por natureza própria, esse direito não deverá ser exercido em relação aos responsáveis pelo tratamento que tratem dados pessoais na prossecução das suas atribuições públicas. Por conseguinte, esse direito não deverá ser aplicável quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de atribuições de interesse público ou para o exercício da autoridade pública de que esteja investido o responsável pelo tratamento. O direito do titular dos dados a transmitir ou receber dados pessoais que lhe digam respeito não deverá implicar para os responsáveis pelo tratamento a obrigação de adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis. Quando um determinado conjunto de dados pessoais disser respeito a mais de um titular, o direito de receber os dados pessoais não deverá prejudicar os direitos e liberdades de outros titulares de dados nos termos do presente regulamento. Além disso, esse direito também não deverá prejudicar o direito dos titulares dos dados a obter o apagamento dos dados pessoais nem as restrições a esse direito estabelecidas no presente regulamento e, nomeadamente, não deverá implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para execução de um contrato, na medida em que e enquanto os dados pessoais forem necessários para a execução do referido contrato. Sempre que seja tecnicamente possível, o titular dos dados deverá ter o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento.

³⁶⁴ Artigo 20.º Direito de portabilidade dos dados 1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a), ou num contrato

Especificamente em relação ao legítimo interesse, o Grupo de Trabalho para o Artigo 29 concebe a portabilidade como garantia complementar que pode ajudar a equilibrar a relação entre controlador e titular. Ainda, de acordo com o parecer 6/2014³⁶⁵:

A existência de mecanismos viáveis que permitam às pessoas em causa aceder, alterar, eliminar, transferir ou de outro modo proceder (ou autorizar que terceiros procedam) ao tratamento posterior dos seus próprios dados capacitará as pessoas em causa e permitir-lhes-á retirar mais benefícios dos serviços digitais.

Cabe deixar claro que não se está a defender a impossibilidade de portabilidade dos dados tratados sob essa base legal. O que se procura demonstrar é a inviabilidade de se conferir o direito ao titular de exigir a portabilidade nessa hipótese sem qualquer ponderação.

Conforme já apontado, não há óbice à abertura dessa possibilidade pelo controlador, principalmente como salvaguarda destinada a viabilizar êxito na realização do teste de balanceamento. Essa reflexão é relevante na medida em que a ANPD deve levar esses aspectos em consideração quando for elaborar o ato regulamentador previsto pelo legislador.

2.4. O Parecer 6/2014 do Grupo de Trabalho para o Artigo 29, sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados conforme o artigo 7º da Diretiva 95/46/CE: um norte interpretativo para a implementação da LGPD

A elaboração do Parecer 6/2014 se deu na circunstância de ausência de uniformidade na interpretação do artigo 7º, alínea f, da diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, conferida pelos países subscritores, relativa à proteção dos dados das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Dentro da realidade europeia, se tinha observado que, embora alguns países utilizassem o legítimo interesse como fundamento autônomo para o tratamento de dados pessoais e procedessem à realização do teste de ponderação proposto pelo legislador, o permissivo, por

referido no artigo 6.º, n.º 1, alínea b); e b) O tratamento for realizado por meios automatizados. 2 Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível. 3. O exercício do direito a que se refere o n.º 1 do presente artigo aplica-se sem prejuízo do artigo 17.º. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. 4. O direito a que se refere o n.º 1 não prejudica os direitos e as liberdades de terceiros.

³⁶⁵ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p. 75.

vezes, era utilizado como instrumento viabilizador de qualquer forma de tratamento que não se enquadrasse nas demais hipóteses previstas na diretiva 95/46/CE, então vigente.

Desta sorte, à míngua de um sistema uniforme, os indivíduos cujos dados eram tratados se encontravam em situação de fragilidade. Com efeito, consoante consta do documento, a ausência de "uma abordagem coerente pode ter como consequência a falta de segurança jurídica e de previsibilidade, pode enfraquecer a posição das pessoas em causa e pode igualmente impor uma sobrecarga regulatória desnecessária às empresas e organizações que desenvolvam atividades transnacionais"³⁶⁶.

Consoante já mencionado, é certo que frente à inexistência de hierarquia entre as bases legais e sendo o legítimo interesse um dos fundamentos para o tratamento lícito de dados pessoais, sua escolha não deve ser dissociada de reflexão e se deve abandonar a falsa concepção de que se cuida de opção menos restritiva do que as demais bases legais³⁶⁷.

Ainda, de acordo com o Parecer 6/2014, o conceito de interesse, base legal para o tratamento de dados, está ligado ao de finalidade, embora com esse não se confunda. Aqui, parece possível estabelecer correlação com a LGPD, pois, segundo a Lei 13.709/2018, a finalidade, enquanto princípio, consiste na realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades³⁶⁸ e o legítimo interesse, enquanto hipótese de tratamento, deve estar atrelado à finalidade específica.

Dessume-se, portanto, que é a finalidade, enquanto razão motivadora do tratamento de dados, que deve nortear o comportamento do agente de tratamento.

No ponto, faz-se alusão à compreensão da finalidade a partir da Convenção 108 do Conselho da Europa de 28 de janeiro de 1981³⁶⁹ e da Recomendação sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais da OCDE de 23 de setembro de 1980³⁷⁰.

³⁶⁶ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p. 7

³⁶⁷ *Ibid.* p. 3.

³⁶⁸ Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

³⁶⁹ Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108?module=treaty-detail&treaty-num=108>. Acesso em 20 jul. 2021.

³⁷⁰ Disponível em: <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprivacyandtransborderflowsfpersonaldata.htm>. Acesso em 20 jul. 2021.

Deveras, da leitura conjunta desses documentos, pode-se funcionalizar o princípio da finalidade com a identificação de características que permitem o esmaecimento da opacidade do tratamento de dados pessoais, em especial quando a base que se pretende adotar é o legítimo interesse: a) a finalidade deve ser clara, específica, relacionada aos dados que se pretende colher e indicada já em momento anterior, e nunca posterior, ao da coleta dos dados pessoais; e b) o uso posterior dos dados não pode ser incompatível com a finalidade inicialmente apontada e deve ser especificado e comunicado a cada mudança de propósito. Rodotà identifica, respectivamente, os princípios da pertinência e da utilização não abusiva³⁷¹.

Outrossim, conforme já exposto, é importante que se perceba a premissa de que o interesse seria aspecto antecedente e mais amplo do que a própria definição da finalidade³⁷². É dizer: o interesse do controlador se consubstancia no substrato fático da definição de sua finalidade sob o prisma jurídico.

É relevante, também, se repisar que a relação jurídica entre interesse e finalidade não é de continente e conteúdo, dado que a gama de interesses do responsável pelo tratamento de dados pode vir a contemplar a finalidade admitida pela legislação como fundamento para a realização da atividade de tratamento de dados, mas não se confunde ou é limitado por ela.

Assim, parece correta a conclusão no sentido de que ao se vincular o legítimo interesse à finalidade do tratamento, fortalece-se o sistema de preservação dos interesses dos indivíduos, fonte de dados, em face de comportamentos inadequados protagonizados pelos agentes de tratamento.

Todavia, a delimitação da finalidade não é suficiente para o controle da atuação do agente de tratamento.

Devem existir instrumentos que viabilizem o escrutínio da atividade do responsável pelo tratamento de dados, a exemplo do dever geral de manutenção do registro das operações de tratamento, previsto no art. 37 da LGPD, no caso do Brasil.

³⁷¹ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 59.

³⁷² A fim de se corroborar o que se defende, faz-se referência a trecho do Parecer 6/2014 do Grupo de Trabalho para o Artigo 29: “[o] conceito de «interesse» está estreitamente relacionado com o conceito de «finalidade» referido no artigo 6.º da diretiva, embora se trate de conceitos distintos. Em matéria de proteção de dados, a «finalidade» é a razão específica pela qual os dados são tratados: o objetivo ou a intenção do tratamento de dados. 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 tratamento”. *In*: EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**. p.37-38

Estabelecida a correlação entre interesse e finalidade, convém a realização de breve digressão sobre a definição de "legítimo interesse" a partir do Parecer 6/2014.

A importância é evidente na medida em que, caso não se tenha presente o interesse legítimo, o tratamento de dados não poderá ser realizado com base nesse permissivo legal, sendo, também, necessário que se dê ênfase à análise das situações concretas, consoante disposto no artigo 10 da LGPD.

É pertinente, também, que se rememore que, no ordenamento jurídico brasileiro, o interesse a ser considerado é o controlador ou de terceiros.

Todavia, conquanto a LGPD restrinja os sujeitos cujos interesses podem fundamentar o tratamento de dados nessa hipótese, ainda se tem largo espectro de possibilidades, sendo relevante, ademais, se saber quando não está presente o legítimo interesse³⁷³.

Para o Grupo de Trabalho do Artigo 29, o legítimo interesse deve ser: i) lícito; ii) definido de forma suficientemente clara para permitir a realização do teste de ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa (deve ser suficientemente específico); iii) representar um interesse real e atual (não deve ser especulativo)³⁷⁴.

Demais disso, da mesma forma que o direito fundamental à proteção de dados não pode ser concebido como direito absoluto, o legítimo interesse não representa um fim em si mesmo, mas ponto de partida para o tratamento de dados que o adote como base legal.

Assim, se de um lado o agente de tratamento interessado pode tratar dados sem o consentimento dos titulares com base no legítimo interesse, de outro, esses têm a legítima expectativa de que seus direitos e liberdades fundamentais serão respeitados por aquele no desempenho de sua atividade³⁷⁵.

Nesse diapasão, o acesso amplo às informações sobre o tratamento de dados e a indicação clara sobre a sua forma e método, inclusive quanto ao compartilhamento com

³⁷³ Por oportuno, faz-se menção ao Parecer 6/2014 no qual se elaborou um rol, não exaustivo, de situações nas quais se vislumbrou a existência do legítimo interesse: exercício do direito à liberdade de expressão ou de informação, nomeadamente nos meios de comunicação social e nas artes; marketing direto convencional e outras formas de marketing ou de publicidade; mensagens não comerciais não solicitadas, nomeadamente relativas a campanhas políticas ou a atividades de angariação de fundos para fins de beneficência; execução de créditos, incluindo cobrança de dívidas através de processos não judiciais; prevenção da fraude, utilização abusiva de serviços ou branqueamento de capitais; monitorização da atividade dos trabalhadores para fins de segurança ou de gestão; sistemas de denúncia; segurança física, tecnologias de informação e segurança das redes; tratamento para fins históricos, científicos ou estatísticos; tratamento para fins de investigação (nomeadamente pesquisas de mercado). *In: Ibid.* p.39

³⁷⁴ *Ibid.* p. 40.

³⁷⁵ Nesse sentido, o Parecer 6/2014. *Ibid.* p. 46-47

terceiros, sobressaem como elementos indispensáveis ao controle da atividade, principalmente para se permitir a avaliação sobre a aderência do tratador à finalidade explicitada.

Fazendo-se um cotejo entre o exposto no presente tópico e as diretrizes para o tratamento com base no legítimo interesse previstas na LGPD (artigos 7, IX, e 10), pode-se chegar a algumas conclusões: a) o interesse a ser considerado é o do controlador ou de terceiro e deve guardar correlação com finalidade vinculada ao apoio e promoção das atividades do controlador, com a coleta de dados estritamente necessários ao cumprimento do objetivo; b) devem ser observados o respeito aos direitos e liberdades fundamentais do titular, bem como suas legítimas expectativas; c) a análise casuística é feita de forma contextual a partir de situações concretas; e d) o registro das operações de tratamento deve estar alinhado com o dever de transparência³⁷⁶.

Cabe pontuar, ainda, que a proteção de dados pessoais deve ser pensada como um sistema, a fim de se permitir a solução de eventuais situações concretas que, em princípio, não se mostrem abrangidas pelos dispositivos referentes às hipóteses de tratamento.

Sobre a sistematicidade do direito, Claus-Wilhelm Canaris defende a imprescindibilidade de compreensão do ordenamento jurídico enquanto sistema, tanto sob perspectiva teleológica quanto sob prisma principiológico³⁷⁷. No mesmo sentido, Norberto Bobbio destaca a necessidade de se conferir ao ordenamento jurídico relação de coerência interna e externa³⁷⁸.

³⁷⁶ Quanto à última conclusão, Marcela Mattiuzo e Paula Ponce apontam que: “[r]ecorrendo ao GDPR, o Article 29 Data Protection Working Party (WPDP29), entidade criada com o objetivo de unificar a interpretação em torno das normas europeias de proteção de dados pessoais, indica que o legítimo interesse é baseado no princípio da accountability (WPDP29, 2014, p. 45). Transpondo esse entendimento para o cenário brasileiro, seria necessário concluir que o legítimo interesse exige que os princípios da transparência, responsabilização e prestação de contas, previstos nos incisos VI e X do art. 6º da LGPD, encontrem especial ressonância quando da sua utilização para o tratamento de dados”. PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 58.

³⁷⁷ Por oportuno, transcreve-se o seguinte fragmento: “[o] sistema cumpre sobretudo, em particular, duas tarefas na obtenção do Direito: ele contribui para a plena composição do conteúdo teleológico de uma norma ou de um instituto jurídico o que conduz a interpretá-los como parte do conjunto da ordem jurídica e sobre o pano de fundo das conexões relevantes; e ele serve para a garantia e a realização da adequação valorativa. e de unidade interior do Direito, porquanto mostra as inconseqüências valorativas, proporcionando, com isso, o aperfeiçoamento do Direito, tanto pela delimitação de ameaçadoras contradições de valores como pela determinação de lacunas”. In: CANARIS, Claus-Wilhelm, **Pensamento sistemático e conceito de sistema na Ciência do Direito**, 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2002. p. 283.

³⁷⁸ Para o autor: “[e]ntendemos por sistema uma totalidade ordenada, um conjunto de entes entre os quais existe uma certa ordem. Para que se possa falar em ordem, é necessário que os entes que a constituem não estejam somente em relacionamento com o todo, mas também num relacionamento de coerência em si. Quando nos perguntamos se um ordenamento jurídico constitui um sistema, nos perguntamos se as normas que o compõem estão num relacionamento de coerência entre si, e em que condições é possível essa relação”. In: BOBBIO, Norberto, **Teoria do ordenamento jurídico**, 10. ed. Brasília: Universidade de Brasília, 1999. p. 71.

Nessa linha de raciocínio, no Brasil, a experiência do direito estrangeiro pode auxiliar a compreensão e sistematização da LGPD, principalmente no que tange aos elementos interpretativos de conceitos abertos.

Do ponto de vista do direito positivo, para além da existência de um microsistema de proteção de dados, os fundamentos da disciplina da matéria³⁷⁹ conferem denso referencial hermenêutico na interpretação das situações reguladas pela norma. De igual sorte, o eixo principiológico adotado³⁸⁰ estabelece parâmetros normativos que permitem se atingir o objetivo de proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural³⁸¹.

2.5. O teste de balanceamento

Conforme se vem demonstrando, a abordagem da doutrina nacional sobre o fundamento de licitude legítimo interesse se estrutura sobre os seguintes pontos principais: a) a premissa da ausência de hierarquia entre as bases legais; b) o exame do legítimo interesse como hipótese de tratamento independente do consentimento; c) o estudo das proposições normativas alusivas ao legítimo interesse; e d) o teste de balanceamento (ou de equilíbrio e de ponderação) compreendido como a oportunidade de se verificar se houve o respeito aos preceitos normativos da LGPD durante o tratamento de dados lastreado nessa base legal³⁸².

O teste de balanceamento é a oportunidade de o agente de tratamento, objetivamente, demonstrar, em contexto e circunstâncias específicas, que desenvolveu sua atividade em estreita observância das normas aplicáveis. De acordo com Bioni, “o fio condutor de toda essa avaliação é ‘balancear’ os direitos em jogo”³⁸³.

Por meio do teste de ponderação, a um só tempo, se confere as almejadas previsibilidade e segurança jurídica na realização do tratamento com base no legítimo interesse e, também, se evita que os conceitos indeterminados que permeiam o instituto sejam utilizados como subterfúgio para fundamentar eventual processamento de dados cujas finalidades não se enquadrem nas demais hipóteses legais.

³⁷⁹ Artigo 2º da LGPD.

³⁸⁰ Artigo 6º da LGPD.

³⁸¹ Artigo 1º da LGPD.

³⁸² No mesmo sentido, cita-se, à guisa de exemplo: Bruno Bioni, Chiara de Teffé, Mario Viola e Marcel Leonardi, Ricardo Oliveira e Márcio Cots.

³⁸³ BIONI, Bruno Ricardo, **Proteção de dados pessoais a função e os limites do consentimento**, Rio de Janeiro: Forense, 2019, p. 252.

Ademais, o teste de equilíbrio, associado ao dever de registro da atividade, tem o condão estimular a aderência do agente de tratamento aos princípios e fundamentos da LGPD e, em larga medida, inviabiliza a ocorrência de efeitos indesejados decorrentes do processamento dessas informações, a exemplo de discriminações abusivas.

O Parecer do Grupo de Trabalho para o Artigo 29, enuncia que o teste de balanceamento – *Legitimate Interest Assessment* (LIA) - se subdivide em quatro etapas: a) avaliação do interesse legítimo do responsável pelo tratamento; b) impacto nas pessoas em causa (necessidade); c) equilíbrio provisório (legítima expectativa do titular); e d) garantias complementares aplicadas pelo responsável pelo tratamento para evitar qualquer impacto indevido nas pessoas em causa (salvaguardas)³⁸⁴.

Parte-se do pressuposto de que há um desalinhamento informacional entre os dados dispersos que os indivíduos produzem cotidianamente e a retenção dessas informações e sua associação por meio de variadas tecnologias³⁸⁵ pelos agentes de tratamento, o que enseja a necessidade da definição de padrões mínimos de proteção de direitos e liberdades fundamentais.

Diante disso, sobressai a imperiosidade de adoção de mecanismo de verificação da lisura do processamento de dados com fundamento no legítimo interesse, principalmente se considerado que, em uma sociedade cada vez mais datificada, o que se percebe é a elevada capacidade de coleta e cruzamento de fragmentos de informações sobre os indivíduos, possibilitando-se a empresas e governos a detenção de verdadeiros perfis sobre as pessoas com os aspectos potencialmente negativos daí decorrentes³⁸⁶.

³⁸⁴ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p. 52.

³⁸⁵ A propósito, transcreve-se excerto do Parecer 6/2014: “[n]uma época em que existe um crescente desequilíbrio na «capacidade de informação», em que quer governos quer organizações empresariais vêm acumulando volumes sem precedentes de dados sobre as pessoas e têm cada vez mais condições para elaborar perfis pormenorizados que permitirão prever os seus comportamentos (reforçando o desequilíbrio de informação e reduzindo a sua autonomia), é mais importante do que nunca assegurar que o interesse das pessoas em preservar a sua privacidade e a sua autonomia seja protegido. EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p. 47.

³⁸⁶ A título de exemplo, menciona-se a ponderação de Rodotà: “[a] resposta rápida às necessidades imediatas tem realmente como efeito a igualdade substancial ou tende muito mais a congelar cada um na posição na qual se encontra, dando origem a uma discriminação bem mais forte? Se, por exemplo, se verifica que a maioria das famílias que habitam um determinado bairro lê apenas um tipo de publicação, razões econômicas estimularão a distribuição naquela área apenas de livros e jornais correspondentes aos gostos e aos interesses individuados naquele momento particular. Por outro lado, portanto, dá-se início a um mecanismo que pode bloquear o desenvolvimento daquela comunidade, solidificando-a no seu perfil traçado em uma situação determinada. Por outro lado, penalizam-se os poucos que não correspondem ao perfil geral, iniciando-se assim um perigoso processo de discriminação de minorias”. In: RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 83.

Com arrimo no art. 10 da LGPD, considera-se que o legislador brasileiro adotou a mesma estrutura proposta pelo Grupo de Trabalho para o Artigo 29, pois se impôs diversos deveres aos agentes de tratamento, os quais, se cumpridos, aproximam sua atividade dos parâmetros trabalhados nesse teste de ponderação³⁸⁷.

Cabe registrar, ainda, a posição de parcela da doutrina pátria que entende que, conquanto não haja menção expressa na LGPD ao teste de equilíbrio, é possível reconhecê-lo no texto legal e se utilizar a "técnica do teste de proporcionalidade de direitos fundamentais, comumente utilizado e referenciado na cultura jurídica brasileira, [a qual] pode operar como aliada no momento de tradução do LIA para o ordenamento jurídico brasileiro"³⁸⁸.

Não se pode apontar, propriamente, uma incongruência entre as perspectivas propostas. Ambas são formas de enfrentar o tema por meio da utilização de parâmetros objetivos, conforme se perceberá a seguir.

Em razão da novidade da matéria no ordenamento jurídico brasileiro, a referência à experiência estrangeira se apresenta como elemento interpretativo importante, principalmente diante da reconhecida proximidade entre a LGPD e o GDPR.

Cabe apontar, também, que o LIA não tem formalidade específica, contudo, cada fase da ponderação tem que ser realizada e deve haver o respectivo registro³⁸⁹.

Já de acordo com a ICO-UK, no sistema europeu, o teste de balanceamento é extraído a partir do artigo 6º do GDPR e é composto por três partes: i) teste de propósito; ii) teste de necessidade (proporcionalidade em sentido amplo); e iii) teste de balanceamento em sentido restrito entre os interesses do titular e do agente de tratamento.

Cumprir destacar, no ponto, diferença sutil entre o modelo previsto pelo Grupo de Trabalho para o Artigo 29 e o LIA utilizado por alguns países signatários do GDPR: enquanto o padrão proposto pelo Parecer 6/2014 prevê quatro etapas: avaliação da legitimidade do interesse, exame de adequação sob o prisma da necessidade, balanceamento em sentido estrito e análise das salvaguardas para o titular de dados, a outra forma de realização do LIA, a exemplo

³⁸⁷ No mesmo sentido, cita-se, à guisa de exemplo: Bruno Bioni, Chiara de Teffé, Mario Viola e Marcel Leonardi, Ricardo Oliveira e Márcio Cots.

³⁸⁸ PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 58.

³⁸⁹ ICO-UK, **What is the 'legitimate interests' basis?**

do modelo britânico, engloba em uma só etapa a ponderação em sentido restrito e as considerações em torno das salvaguardas³⁹⁰.

Independentemente de suas variantes, entende-se que a sucessão das etapas no teste de balanceamento permite o escrutínio do tratamento de dados realizado com base no legítimo interesse e instrumentaliza a contenção da prática de abusos pelos agentes de tratamento³⁹¹.

Nesse trilhar, cada momento do teste de ponderação deve ter o seu espaço de abrangência bem delimitado, razão pela qual se procederá ao detalhamento de cada fase a partir de exemplos retirados de documento elaborado pela ICO-UK e do Parecer 6/2014 do Grupo de Trabalho para o Artigo 29 e se contextualizará, na medida do possível, com a LGPD.

No que diz respeito ao teste em si, primeiramente, se realiza o teste de prossecução³⁹². Em outras palavras, se avalia se, no plano abstrato, o interesse do agente de tratamento guarda consonância com a sua atividade. Deve-se deixar clara a finalidade que se pretende atingir, quem se beneficia daquele tratamento, a extensão e a importância do benefício, ao controlador, decorrente do processamento dos dados e, também, que se está atuando dentro dos limites éticos e legais estabelecidos pela Lei Geral de proteção de dados³⁹³.

À guisa de exemplo, imagine-se uma companhia de seguros que pretende processar dados pessoais para identificar pedidos de indenização fraudulentos com base no legítimo interesse. Em tese, é legítima a pretensão da empresa de se proteger contra fraudes de clientes e, de igual sorte, se pode presumir ser do interesse dos demais clientes e do público geral que existam e se desenvolvam constantemente ferramentas de identificação e prevenção de fraudes.

³⁹⁰ Bioni e outros destacam que “[o referido modelo] propõe uma etapa de avaliação da legitimidade do interesse, seguida de uma análise de adequação e uma avaliação da necessidade e, por fim, um balanceamento dos interesses do controlador ou terceiros com a legítima expectativa e os direitos e liberdades do titular. A última etapa, nesse caso, absorveria a análise sobre as salvaguardas do tratamento”. *In*: BIONI, Bruno Ricardo; RIELLI, Mariana Marques, **Legítimo interesse na LGPD Pano de fundo: conceito jurídico indeterminado e a sua posição na agenda regulatória da ANPD**, JOTA Info. Disponível em: <<https://www.jota.info/opiniao-e-analise/columas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-anpd-dados-01032021>>. Acesso em: 8 abr. 2021.

³⁹¹ De acordo com Bioni, “Tão importante quanto aferir se há um interesse legítimo é verificar se as legítimas expectativas e os direitos e liberdades fundamentais do cidadão serão respeitados. BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 252.

³⁹² Terminologia adotada pela Corte de Justiça da União Europeia no caso Rigas (Acórdão C-13/16). *In*: UNIÃO EUROPEIA. Corte de Justiça da União Europeia. Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contra Rīgas pašvaldības SIA «Rīgas satiksmē». **Acórdão C-13/16**, publicado em 4 mai. 2017. Disponível

em:<<https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=13%252F16&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=29533406>>. Acesso em 14 jan. 2021.

³⁹³ ICO-UK, **What is the ‘legitimate interests’ basis?**; CIPL, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation**.

Pode-se pensar, ainda, para fins de propósito legítimo: a) em situações nas quais se revele imprescindível à segurança de determinada rede de dados, bem como das informações nela contidas, a identificação do possível cometimento de crimes; b) no processamento de dados de empregados por empresas; c) marketing direto; ou d) informações administrativas referentes a empresas pertencentes ao mesmo grupo econômico³⁹⁴.

O passo subsequente, teste de necessidade, se refere à demonstração de que determinado tratamento é necessário para o interesse legítimo previamente identificado e que o impacto nos titulares não fulmina seus direitos e garantias fundamentais. Deve-se considerar se o processamento de dados, de fato, conduz ao interesse exposto e se é uma prática razoável.

Não se pode confundir a necessidade do tratamento com base no legítimo interesse com a necessidade do processamento em razão da escolha prévia da base legítimo interesse pelo agente de tratamento. Deve haver um liame entre o legítimo interesse identificado a partir do teste de prossecução e a necessidade inerente a essa justificativa legal.

Nesse sentido, a Lei Geral de Proteção de dados impõe ao controlador a referência à “situação concreta” no artigo 10. Essa previsão é salutar na medida em que inviabiliza a escolha do legítimo interesse com base em finalidades não claramente demonstradas.

A autoridade britânica de proteção de dados considera, também, que se deve decidir casuisticamente sobre a existência de alguma alternativa menos intrusiva, a exemplo da possibilidade de se atingir a finalidade do tratamento por outros meios razoáveis sem processar os dados da maneira que se pretende realizar e, também, que o processamento dos dados é proporcional e vinculado aos objetivos estabelecidos³⁹⁵.

Embora parte da doutrina nacional também defenda essa linha de raciocínio³⁹⁶, posiciona-se no sentido da prescindibilidade da constituição desse filtro neste momento do teste de balanceamento. Com efeito, à luz do princípio da ausência de hierarquia entre as hipóteses de tratamento, uma vez demonstrada e justificada a possibilidade de processamento de dados com base no legítimo interesse, deve-se franquear ao controlador, mediante a assunção dos riscos inerentes à sua opção, a decisão de prosseguir desenvolvendo sua atividade e arcar com os desdobramentos decorrentes de sua conduta.

³⁹⁴ Exemplos extraídos a partir dos Considerandos 47, 48 e 49 do GDPR.

³⁹⁵ INFORMATION COMMISSIONER'S OFFICE (ICO-UK), **What is the 'legitimate interests' basis?**, p. 14.

³⁹⁶ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**; ZANFIR-FORTUNA; TROESTER-FALK, **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases**.

Aqui ganha destaque o dever de o agente de tratamento documentar e fundamentar adequadamente a escolha pelo legítimo interesse. Somente a partir do exame contextual de sua atuação é que se poderá determinar se seu comportamento foi lícito ou não.

Mais importante do que se verificar a existência de base legal que impacte menos na esfera individual dos indivíduos é se garantir que se tenha clareza na demonstração da eleição dessa base legal pelo controlador e se assegure ao titular dos dados plenas condições de compreender a amplitude do tratamento, bem como sejam resguardadas suas legítimas expectativas.

Caso não se consiga justificar adequadamente a necessidade do tratamento, pode ser que a finalidade não esteja clara o suficiente ou mesmo seja incompatível com a atividade que enseja a coleta e tratamento dos dados³⁹⁷. Consoante se vem afirmando, as etapas são sucessivas e interdependentes, sendo certo que devem guardar harmonia entre si.

Por oportuno, reitera-se que, nos moldes da estrutura perfilhada pela LGPD, o exame da etapa da necessidade, na realidade brasileira, prescinde do caráter subsidiário emprestado pela normatização europeia ao legítimo interesse.

A ausência de preponderância e a relação de complementaridade entre as bases legais permite a adoção pelo agente de tratamento daquela que lhe parecer melhor, recaindo sobre si as consequências de sua escolha quanto ao ônus de evidenciar a adequação do tratamento à legislação e, também, a responsabilidade sobre eventual descumprimento da lei.

Na terceira fase, no teste de proporcionalidade em sentido estrito, deve-se aferir se o impacto do tratamento de dados no titular não se sobrepõe ao legítimo interesse identificado e se as suas legítimas expectativas são respeitadas.

Isso somente é possível a partir do cotejo entre diversos elementos que compõem a relação jurídica originária, a exemplo da sua natureza (por exemplo se comercial ou profissional), da circunstância de se lidar com dados particularmente sensíveis, íntimos, ou ainda, de crianças ou adolescentes, da apreciação se, a partir do conhecimento do tratamento, o titular o compreende e concorda com o processamento e, também, se a vulnerabilidade do indivíduo não se constitui em um óbice ao desenvolvimento da atividade nos moldes pretendidos³⁹⁸.

³⁹⁷ ICO-UK, **What is the 'legitimate interests' basis?**

³⁹⁸ INFORMATION COMMISSIONER'S OFFICE (ICO-UK), **What is the 'legitimate interests' basis?; CIPL, How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation.**

Assim, devem ser consideradas "a natureza dos dados pessoais, a forma como a informação é tratada, as expectativas razoáveis das pessoas em causa e o estatuto do responsável pelo tratamento e da pessoa em causa"³⁹⁹.

Essa fase se relaciona ao aspecto dinâmico do tratamento dos dados, uma vez que, consoante já mencionado, o legítimo interesse do responsável abstratamente considerado é apenas o ponto de partida.

Com efeito, é nessa etapa que se revela possível a aferição de que houve a "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais"⁴⁰⁰.

O Considerando 47 do GDPR estabelece a necessidade de avaliação minuciosa, em especial no que diz respeito à capacidade de o titular dos dados prever, dentro do espectro da razoabilidade, no momento e no contexto em que os dados pessoais foram coletados, que esses são suscetíveis de tratamento com base no legítimo interesse⁴⁰¹.

Assim, devem ser contrapostos, de forma contextualizada, os direitos e liberdades do titular de dados e os interesses do agente de tratamento e deve ser sopesada a natureza da relação estabelecida. Bioni pondera que “essa fase do teste é calibrada pelo vocabulário da teoria da privacidade contextual, devendo-se analisar as legítimas expectativas em jogo e, principalmente, se o fluxo informacional é apropriado-íntegro para o livre desenvolvimento da personalidade do titular”⁴⁰².

Deve-se, ainda, avaliar objetivamente o risco do processamento dos dados. Por oportuno, se transcreve o Considerando 75 do GDPR, o qual pode funcionar como importante auxílio na compreensão da abrangência do teste de ponderação⁴⁰³:

O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da

³⁹⁹ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p.57

⁴⁰⁰ Art. 10. 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 se limitam a:
(...)

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

⁴⁰¹ UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

⁴⁰² BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 255.

⁴⁰³ UNIÃO EUROPEIA, **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**.

identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.

Quanto maior o risco identificado, mais densa deve ser a justificativa do tratamento com base no legítimo interesse. Nessa etapa, o agente de tratamento deve demonstrar que o seu interesse predomina sobre o do titular naquele contexto específico.

Portanto, conquanto a idoneidade do tratamento com base no legítimo interesse seja examinada em momento posterior, a ponderação realizada pelo agente de tratamento deve ser prévia e é nessa etapa que se determina a higidez do comportamento do responsável, revestindo-se de peculiar importância a realização do teste de balanceamento em sentido estrito.

A implementação de salvaguardas para alguns seria fase autónoma do teste de balanceamento⁴⁰⁴, para outros estaria inserida na terceira fase⁴⁰⁵.

Independentemente da posição seguida, cuida-se da adoção de mecanismos de proteção do titular que aproximam o tratamento do espectro de legalidade, a exemplo da observância do princípio da transparência⁴⁰⁶, da instrumentalização dos já mencionados *privacy by design* e *privacy by default*, do direito de o titular interromper o tratamento de dados (*opt-out*)⁴⁰⁷, da limitação do volume de dados tratados, da exclusão de dados após o uso e, também, do robustecimento da posição jurídica do titular por meio da criação de ferramentas automatizadas que lhe permitam interferir na forma de tratamento⁴⁰⁸.

⁴⁰⁴ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**; PONCE; MATTIUZZO, O legítimo interesse e o teste da proporcionalidade.

⁴⁰⁵ Posição adotada pela ICO-UK e, também, pela Corte de Justiça da União Europeia, no caso Rigas.

⁴⁰⁶ A LGPD, no art. 10, § 2º, considera que o “controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse”

⁴⁰⁷ BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**, p. 37.

⁴⁰⁸ Mattiuzo e Ponce apontam que “as salvaguardas de proteção de dados pessoais disponíveis para os controladores estão descritas ao longo da LGPD, sendo inclusive recomendável a sua utilização

Parece despiciendo se estabelecer se as salvaguardas deverão ser adotadas em fase autônoma ou no momento do teste de proporcionalidade em sentido estrito. Primeiro, o legislador não estabeleceu um padrão para a realização do teste de balanceamento. Segundo, de acordo com o que se expôs, são garantias complementares aplicadas pelo responsável pelo tratamento para evitar qualquer impacto indevido nos indivíduos fontes de dados. Desse modo, quanto mais salvaguardas forem adotadas, maior a probabilidade de o tratamento ser possível sob a justificativa do legítimo interesse⁴⁰⁹.

Demais disso, é inarredável exame contextual da necessidade com vistas a se prevenir a utilização de dados que não se coadune com as finalidades da coleta.

Consoante já se apontou, os interesses do agente de tratamento devem ser legítimos e não podem aviltar direitos e garantias fundamentais dos titulares. É dizer: a lei não restringe a tutela dos interesses dos titulares da forma como limita a atuação do tratador dos dados. Portanto, a proteção dos sujeitos, fontes dos dados, é mais ampla em ordem a tutelar, inclusive, interesses pessoas de envolvidas em atividades ilegais⁴¹⁰.

Não se pode olvidar, ainda, que os interesses do responsável pelo tratamento de dados podem ultrapassar sua individualidade e convergir com os interesses de uma determinada coletividade, ou mesmo com o interesse público, o que, em tese, lhe avigora enquanto atividade de tratamento, mas não o torna mais ou menos legítimo a partir de exame estritamente legal.

Sobre o que se disse, tome-se como exemplos a coleta de dados referentes a consumidores de determinado serviço em cenário de investigação, pela empresa fornecedora, de fraudes, tais como a venda irregular de sinal de internet, ou uso comercial de serviços de *streaming* por meio de conta individual; ou, ainda, situação na qual alguma organização não governamental, examinando as contas publicizadas por determinado órgão público, a fim de

independentemente da base legal aplicada. Essas salvaguardas incluem: com relação à coleta e tratamento de dados, a utilização de técnicas como a anonimização⁹e pseudoanonimização (arts. 12 e 13 da LGPD), bem como a minimização dos dados coletados, encriptação e agregação dos dados pessoais tratados; com relação ao desenvolvimento de tecnologias, o desenvolvimento do *privacy by design*. (art. 49) e mecanismos simplificados de transparência e exercícios dos direitos dos titulares, incluindo o direito de oposição (art. 10, § 2º e art. 18, § 2º). Além disso, no nível da organização, é necessário discutir a existência de controles de acesso aos dados ou quaisquer medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de tratamento (art. 46)”. PONCE; MATTIUZZO, **O legítimo interesse e o teste da proporcionalidade**, p. 66–67.

⁴⁰⁹ ZANFIR-FORTUNA; TROESTER-FALK, **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases**.

⁴¹⁰ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p.47.

trazer ao conhecimento da sociedade e da imprensa possível caso de corrupção, exponha gastos extravagantes e desproporcionais de algum servidor.

Embora ostente certa flexibilidade, o legítimo interesse encontra limites estabelecidos na Constituição e na Lei e, portanto, sua utilização deve ser permeada por mecanismos de prevenção de lesões a direitos individuais. Cabe advertir, ainda, que o conflito entre os interesses do agente de tratamento e do titular não necessariamente indica que deverá prevalecer o interesse desse último.

Sob o prisma jurisprudencial, a Corte de Justiça da União Europeia, no caso *Rigas*⁴¹¹, ao decidir sobre a possibilidade de compartilhamento pela polícia local à vítima de acidente viário de dados de menor que teria causado o resultado, se manifestou no sentido da plena aplicabilidade do teste de balanceamento em 3 (três) etapas no que diz respeito ao legítimo interesse. Referida manifestação se deu no contexto da vigência da Diretiva 95/46/EC, a qual continha disposição similar ao atual artigo 6º do GDPR⁴¹². O Tribunal destacou, ainda, a necessidade de análise contextual do interesse, em especial no que diz respeito à natureza dos dados, à forma como são tratados e, também, à relação entre o caso concreto e a finalidade do tratamento⁴¹³.

Conquanto no caso concreto se tenha concluído que a proteção do menor deveria prevalecer sobre o legítimo interesse do autor, a relevância do caso está na admissão e funcionalização, no âmbito jurisdicional, dos critérios de ponderação desenvolvidos pela doutrina à luz da legislação.

⁴¹¹ UNIÃO EUROPEIA. Corte de Justiça da União Europeia. **Acórdão C-13/16**, publicado em 4 mai. 2017.

⁴¹² Para a Corte, “[o] artigo 7º, alínea f), da Diretiva 95/46 prevê três requisitos cumulativos para que um tratamento de dados pessoais seja lícito, a saber, em primeiro lugar, a prossecução de interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, em segundo lugar, a necessidade do tratamento dos dados pessoais para a realização do interesse legítimo, e, em terceiro lugar, o requisito de os direitos e as liberdades fundamentais da pessoa a que a proteção de dados diz respeito não prevalecerem”. *Ibid*, p. 6.

⁴¹³ A propósito, pondera Costa que: “[a]ssim, ao se avaliar o impacto sobre os titulares de dados, devem-se considerar (a) as circunstâncias envolvidas (ex.: situações nas quais o tratamento pretendido possa conduzir à exclusão ou à discriminação de pessoas) e a finalidade desejada (ex: qualquer finalidade lícita, como o direcionamento de propaganda, monitoramento de empregados etc.); (b) a natureza dos dados (se públicos ou privados, se de acesso restrito ou irrestrito, etc.); e (c) a forma como os dados são tratados”. *In*: COSTA, Vinícius Venâncio, **Estaria o interesse legítimo presente apenas em dados de acesso público?**, JOTA Info. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/estaria-o-interesse-legitimo-presente-apenas-em-dados-de-acesso-publico-06032020>>. Acesso em: 28 nov. 2020.

CAPÍTULO 3 – SITUAÇÕES HIPOTÉTICAS: compreendendo a dinâmica da base legal legítimo interesse

Conforme já disposto, a escolha da base legal legítimo interesse deve estar atrelada a objetivo claro e específico do agente de tratamento de dados. A finalidade deve ser legítima, relacionada a aspecto concreto da atividade do controlador e articulada de forma clara.

Com efeito, a lei não abre espaço para que se justifique o tratamento nessa base legal a partir de abstrações ou descrições imprecisas.

Podem ser vislumbradas diversas hipóteses de uso desse fundamento de licitude e, com o intento de se atribuir aplicação prática ao que abordado neste estudo, se recorrerá a situações abstratas, de fácil constatação no plano concreto, extraídas a partir de diversas fontes⁴¹⁴, bem como e se examinará o legítimo interesse do agente de tratamento sob o influxo das ideias aqui defendidas.

É oportuno se evidenciar que não se cuida de avaliações imutáveis e exaurientes sobre cada situação. A casuística e o contexto podem influenciar o resultado do teste de ponderação. Desta sorte, caso o agente de tratamento atue de forma diversa das descritas, seja por meio da adoção de salvaguardas mais amplas, ou condutas mais transparentes, o raciocínio desenvolvido pode não ser aplicável.

Além disso, ainda que em tese possa ser viável a utilização de outra base legal, não nos parece inadequado que se fundamente o tratamento no legítimo interesse, desde que se consiga se desincumbir do ônus de demonstrar a consonância com as prescrições da LGPD.

Passa-se, então, à descrição e análise dos casos hipotéticos.

3.1. Estabelecimento comercial que envia publicidade dirigida aos seus clientes sobre produtos análogos aos já adquiridos com base no histórico de consumo

Imagine-se que determinada empresa, no momento da realização do primeiro negócio com um cliente, recolha informações de contato do consumidor e, posteriormente, quando

⁴¹⁴ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**; BIONI; KITAYAMA; RIELLI, **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**; EDPB, Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29; ICO-UK, **What is the ‘legitimate interests’ basis?**; ZANFIR-FORTUNA; TROESTER-FALK, **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases**; CIPL, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation**.

disponibiliza nova linha de produtos similares aos previamente fornecidos, envie aos clientes mensagens na intenção de ampliar as possibilidades de vendas.

No teste de ponderação, na primeira fase, percebe-se situação concreta e finalidade definidas: nova linha de produtos disponíveis e intenção de aumento no número de vendas, de modo que, do ponto de vista abstrato, é possível o tratamento com base no legítimo interesse.

Na segunda fase, exame da necessidade, caso tenha ocorrido amplamente a informação de que a coleta dos dados de contato seria utilizada para o envio de publicidade e a disponibilização do dado tenha se dado voluntariamente pelo titular, não se pode falar em impacto desproporcional e tampouco em necessidade artificialmente criada em razão da escolha prévia do fundamento de licitude legítimo interesse. Aqui, há certa intersecção com o exame da legítima expectativa (terceira fase), pois se deve observar se a conduta do fornecedor foi transparente.

Na terceira fase, quanto à legítima expectativa, mais uma vez a transparência desempenha papel fundamental. Assim, se o fornecedor explicou a relação entre a coleta dos dados e a finalidade pretendida e, ainda assim, obteve acesso aos dados demandados, a legítima expectativa do titular terá sido resguardada e se pode perceber que os interesses do agente de tratamento preponderam nesse contexto específico.

Quanto às salvaguardas, pode-se pensar em, ostensivamente, se permitir ao consumidor se opor ao tratamento, sem custos, de modo simples, a exemplo da inserção de links de fácil visualização em mensagens eletrônicas ou disponibilização de canal exclusivamente destinado a isso, no caso de mensagens físicas.

3.2. Coleta de documento nacional de identificação por drogarias e formação de perfis para ofertas de produtos e “descontos exclusivos” com base nos hábitos de consumo do titular de dados/ Utilização do histórico de consumo para aprimoramento logístico

É comum, no Brasil, estabelecimentos especializados e autorizados ao comércio de fármacos condicionarem a concessão de descontos na venda de determinados medicamentos ao fornecimento de documento de identificação do consumidor, ou mesmo a dados biométricos.

Os registros de compras de medicamentos podem evidenciar muitas informações a respeito do titular e permitir a construção de perfis de saúde. A esse respeito, calha dispor que dado referente à saúde é considerado dado pessoal sensível, *ex vi*, do art. 5º, II, da LGPD.

Neste passo, se a finalidade é a construção de perfil de saúde do consumidor vinculado à determinada rede de farmácias, o legítimo interesse não pode ser utilizado para o tratamento

pretendido. É dizer: no teste de ponderação, sequer se ultrapassa a fase de prossecução, uma vez que não há que se falar em legítimo interesse para o tratamento de dados sensíveis.

Embora, em regra, nessa situação, se pretenda fundamentar a coleta dos dados no consentimento, esse, no contexto descrito, não pode ser considerado válido nos termos da LGPD⁴¹⁵. Isso não significa, todavia, que não possa ser uma alternativa desde que corretamente obtido e se observe a axiologia da LGPD.

Sob outro enfoque, acaso se deseje otimizar a logística de estoques de medicamentos e compreender a demanda por produtos específicos, a base legal legítimo interesse se revela opção viável.

Em relação à primeira etapa do teste, não se vislumbra impedimento legal, principalmente se observado que desenvolvimento logístico (apoio e promoção das atividades do controlador), além de se referir a situação concreta, está entre as finalidades consideradas legítimas pelo legislador (art. 10, I).

No que diz respeito à necessidade e ao impacto no titular de dados (segunda etapa), é imperiosa a adstrição à finalidade exposta aos consumidores, pois é possível se desvincular os consumidores dos respectivos produtos demandados e, desse modo, se minimizar os dados coletados.

No momento do teste de balanceamento em sentido estrito, é cabível se cogitar que os consumidores possuem a legítima expectativa de se dirigirem ao estabelecimento e lá encontrarem os produtos desejados. Isso somente é possível mediante adequada organização logística por parte do fornecedor e há, também, a predominância do interesse do agente de tratamento em ofertar produtos aos seus consumidores cuja demanda seja real.

Em relação às salvaguardas, medidas de pseudoanonimização dos dados são extremamente oportunas, na medida em que preservam a privacidade dos consumidores no que diz respeito à sua condição de saúde. Ademais, a transparência quanto ao tratamento e a adstrição à finalidade apresentada contribuem sobremaneira para a manutenção do equilíbrio necessário ao processamento de dados sob esse fundamento de licitude.

⁴¹⁵ Condicionar a aquisição de medicamento por preço inferior ao anunciado ao fornecimento de dados pessoais não pode ser considerado mecanismo de obtenção do consentimento compatível com os parâmetros estabelecidos pela LGPD, *in verbis*: art. 5º Para os fins desta Lei, considera-se: (...) XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

3.3 Assistente pessoal por voz

Hoje, existem diversos assistentes pessoais por voz⁴¹⁶ ofertados por várias empresas. A função principal desses dispositivos é responder, de modo preciso, às provocações realizadas pelos detentores de produtos desse tipo.

Imagine-se que o agente de tratamento não anonimiza, nos termos do art. 5º, III, da LGPD, os dados coletados (e por essa razão se sujeite às hipóteses de tratamento previstas na LGPD) e pretenda processar, ainda que parcialmente, os elementos de informação recolhidos da base de usuários, inclusive gravações, para aprimorar o sistema de inteligência artificial e implementar mecanismos de aprendizado de máquina no afã de garantir que o sistema funcione bem para todos os usuários⁴¹⁷.

Um programa de aprendizado de máquina requer "milhões ou bilhões de dados de referência para criar o seu próprio modelo estatístico de causa e efeito"⁴¹⁸, de sorte que seria extremamente caro para os fornecedores e, por via de consequência, também para os consumidores, o aperfeiçoamento do serviço sem a utilização de dados de voz dos próprios usuários, sem se olvidar da dificuldade de desenvolvimento de algoritmos que lidam com linguagem.

Certamente os destinatários finais do produto sofreriam com a menor usabilidade da inteligência artificial, habilidades mais precárias do assistente virtual e menos opções de serviço⁴¹⁹.

Isso posto, nessa situação brevemente descrita, se pode inferir o legítimo interesse dos fornecedores do serviço de assistentes virtuais por voz de manutenção e aprimoramento

⁴¹⁶ Schwab aponta que “o reconhecimento de voz e a inteligência artificial progredem em uma velocidade tão rápida que falar com computadores se tornará, em breve, a norma, criando algo que os tecnólogos chamam de computação ambiental; nela, os assistentes pessoais robotizados estão sempre disponíveis para tomar notas e responder às consultas do usuário. Cada vez mais, nossos dispositivos se tornarão parte de nosso ecossistema pessoal, nos ouvindo, antecipando nossas necessidades e nos ajudando quando necessário – mesmo que não tenhamos pedido”. SCHWAB, **A quarta Revolução Industrial [livro eletrônico]**, p. 25.

⁴¹⁷ A Amazon "utiliza gravações dos usuários para atender às demandas dos consumidores e melhorar os serviços prestados e somente compartilha dados gerais, como o CEP, com terceiros, jamais gravações ou informações pessoais específicas. Além de a exigência de consentimento do consumidor poder ser fator que atrase características e enfraqueçam outros aspectos do serviço ofertado, dos quais os consumidores gostam (a exemplo de recomendações com base no histórico de buscas)". *In*: WILCOX, “**Hey Alexa, Do Consumers Really Want More Data Privacy?**”: **An Analysis of the Negative Effects of the General Data Protection Regulation**, p. 266.

⁴¹⁸ O’NEIL, **Weapons of math destruction: How big data increases inequality and threatens democracy**, p. 76.

⁴¹⁹ CIPL, **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation**, p. 26.

constante do serviço, especialmente no que diz respeito à acurácia das respostas e adaptabilidade dos dispositivos às peculiaridades regionais.

Assim, considerada a ausência de hierarquia entre os permissivos legais, caso se opte pela base legítimo interesse à luz da LGPD, os requisitos do art. 10 estariam adimplidos, pois se teria a situação concreta: uso de assistente por voz por indivíduos, a finalidade de apoio e promoção de atividades do controlador e a prestação de serviços que o beneficiem o titular.

Em relação ao respeito às legítimas expectativas e aos direitos e liberdades fundamentais dos titulares, tem lugar o teste de balanceamento.

Na primeira fase, se deve conferir o propósito: a plausibilidade do legítimo interesse do agente de tratamento preponderar, sob a óptica abstrata, sobre os interesses dos indivíduos. Pelo exposto, entende-se presente o legítimo interesse no aprimoramento dos produtos e serviços ofertados.

Na segunda fase, exame da necessidade e impacto nas pessoas em causa, percebe-se, também, a convergência de interesses entre agente de tratamento e titulares de dados, principalmente sob a perspectiva de que o constante aperfeiçoamento dos dispositivos e do serviço deve se nortear pela forma de sua utilização pelos destinatários.

Na terceira fase, no equilíbrio provisório ou teste de balanceamento em sentido restrito, se ponderam as legítimas expectativas do titular dos dados e a conduta do controlador. Nessa situação, não há como se negar que aqueles que se utilizam de assistentes virtuais estão dispostos a ceder, ao menos em parte, aspectos relacionados à sua privacidade, seja ao solicitar que o assistente virtual reproduza determinada música ou notícias relativas a assuntos de sua preferência, ou, ainda, ao estabelecer lembrete de determinado compromisso. É da essência do serviço prestado a relação de auxílio em atividades do cotidiano de quem utiliza o serviço. Todavia, não se pode presumir que o usuário médio estaria disposto a renunciar a todos os aspectos relacionados à sua vida privada, inclusive relativos à intimidade.

Destarte, se pode constatar que, em contraposição aos interesses do controlador, os usuários de assistentes virtuais, por sua vez, detêm a legítima expectativa de terem à sua disposição serviço de qualidade que melhore na medida de sua utilização e tenha capacidade de responder adequadamente aos questionamentos formulados. Pode-se apontar, também, a legítima expectativa de não terem dados de sua intimidade violados ou "espionados" pelo dispositivo que necessariamente "escutará" o que se passa ao seu redor, pois precisa estar de prontidão para compreender a palavra de ativação.

Nesse ponto ganham ênfase salvaguardas que podem ser utilizadas pelo agente de tratamento. Medidas de transparência contribuem sobremaneira para reduzir a assimetria de poderes. Portanto, clareza quanto às políticas de uso das informações coletadas, disponibilização das gravações realizadas e introdução de mecanismos de exclusão desses dados podem contribuir para que se reconheça a higidez da conduta do agente de tratamento.

3.4 Operações societárias

Suponha-se duas empresas que pretendam fazer determinada operação societária, a exemplo de incorporação, fusão ou cisão de sociedades⁴²⁰. Usualmente, na fase de tomada de decisões, as partes envolvidas realizam análise da viabilidade do negócio, “há um processo de troca de informações (*due diligence*) como parte do processo de fusão, aquisição e cisão corporativa. Da análise financeira, fiscal, contábil, ao quatro de funcionários e da base de consumidores da organização”⁴²¹. Nessas circunstâncias é elevada a probabilidade de acesso a dados pessoais de sujeitos não envolvidos diretamente na negociação.

Dentro do teste de ponderação, na primeira fase, na análise da existência do legítimo interesse, é perceptível situação concreta e finalidade definidas: realização de operação societária determinada, sendo possível, portanto, vislumbrar o legítimo interesse sob a óptica abstrata.

Na segunda fase, necessidade, sabe-se que os contraentes precisam de subsídios para concretizarem o negócio jurídico. Nessas circunstâncias, por vezes, é inevitável o acesso a bancos de dados nos quais constem informações relativas a colaboradores, eventuais consumidores e fornecedores. Não há como se estabelecer antecipadamente quais dados seriam necessários para concretização da operação, mas é certo que o tratamento deve se cingir ao imprescindível para a materialização da avença.

Na terceira fase, não se pode presumir que o tratamento de dados será nocivo aos titulares. Em primeiro lugar, reorganizações societárias não são fatos estranhos ao desenvolvimento da atividade empresarial, de modo que, sob essa visão, a legítima expectativa

⁴²⁰ De acordo com o Código Civil: Art. 1.116. Na incorporação, uma ou várias sociedades são absorvidas por outra, que lhes sucede em todos os direitos e obrigações, devendo todas aprová-la, na forma estabelecida para os respectivos tipos; Art. 1.119. A fusão determina a extinção das sociedades que se unem, para formar sociedade nova, que a elas sucederá nos direitos e obrigações; quanto à cisão, nos termos da Lei 6.404/76: art. 229. A cisão é a operação pela qual a companhia transfere parcelas do seu patrimônio para uma ou mais sociedades, constituídas para esse fim ou já existentes, extinguindo-se a companhia cindida, se houver versão de todo o seu patrimônio, ou dividindo-se o seu capital, se parcial a versão.

⁴²¹ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 258.

dos titulares de dados não seria frustrada. Além disso, não há impacto direto sobre seus direitos e liberdades fundamentais, uma vez que os dados são coletados e examinados com o fim de permitir tomadas de decisões da forma mais segura não havendo, nessa atividade específica e nesse momento, repercussão sobre suas esferas jurídicas.

Quanto às salvaguardas, diante da ampla variabilidade de casos concretos, deve-se priorizar a adoção de ambientes seguros de armazenamento das informações e assim se evitar seu eventual vazamento. Outrossim, na maior medida possível, não devem ser utilizados dados de forma individualizada durante a realização da *due diligence*.

Aqui, há a peculiaridade, já abordada no presente trabalho de se cuidar de legítimo interesse de terceiros, uma vez que há a possibilidade de processamento de dados de sujeitos que não têm relação pré-estabelecida com as partes do negócio, as quais possuem o legítimo interesse de avaliar a possibilidade de efetivar eventual operação societária.

3.5. Empresa que pretende contratar colaboradores e terceiriza serviço de verificação da vida pregressa dos candidatos à vaga de trabalho.

Diante da necessidade de contratar novos empregados, determinada empresa decide abrir processo seletivo e, para melhor atingir seu objetivo, opta por, paralelamente, contratar entidade especializada em averiguar a vida pregressa dos potenciais candidatos.

Nesta situação, se estabelece a premissa de que a análise oferecida pela entidade de consulta aos dados dos candidatos cinge-se ao exame de antecedentes criminais, conteúdos publicados em redes sociais e contato com ex-empregadores a fim de se apresentar relatório à empresa que disponibiliza as posições de emprego.

Na primeira fase, no teste de prossecução, exame do legítimo interesse em abstrato, é factível que a preocupação em melhor selecionar quem irá compor os quadros de determinada empresa esteja dentro da finalidade “apoio e promoção de atividades do controlador” (art. 10, I).

Na segunda fase, no exame da necessidade, a análise contextual ganha destaque, pois se deve estar bem definido o que se pretende com a contratação do serviço de investigação, uma vez que a amplitude da consulta é reflexo do que se pretende conhecer sobre os aplicantes. Assim, a depender das funções que o futuro colaborador irá desempenhar, pode ser desejável que se tenha conhecimento sobre a anterior prática de ilícitos penais, das publicações em redes sociais, além das referências de empregadores anteriores.

Na terceira fase, no teste de balanceamento é que se permitirá demonstrar a ausência da tomada de decisões com conteúdo discriminatório abusivo. Assim, é razoável se considerar que, em processos seletivos, é aceitável que o potencial empregador busque confirmar as informações fornecidas pelo próprio candidato e que o aspirante à vaga, principalmente se ostensivamente informado pelo controlador durante o processo de seleção, espere a realização de consulta a alguns aspectos de sua vida.

No caso, não desborda do razoável que o indivíduo que se inscreva na disputa de certa vaga de trabalho, desde que lhe tenham sido esclarecidas a amplitude das responsabilidades da posição que pretende ocupar e a possibilidade de consulta a determinados elementos de informação a seu respeito, tenha a legítima expectativa de que o potencial empregador coletará elementos de informação que lhe deem a segurança necessária para a perfectibilização da contratação.

Há certas limitações inerentes à base legal ora tratada. Assim, por exemplo, a posição política de alguém, conhecida a partir de tratamento de dados com base no legítimo interesse, não poderia servir de fundamento para a exclusão de determinado candidato no processo seletivo. Da mesma forma, a cor da pele, o estado de gravidez, ou outros parâmetros capazes de materializar lesão ao princípio do livre desenvolvimento da personalidade não poderiam ser utilizados para fins de exclusão do certame.

As razões são diversas, mas, no presente trabalho se dará enfoque ao regime jurídico do presente fundamento de licitude para o processamento de dados. Assim, o principal motivo da impossibilidade de utilização dessa informação se dá em razão de se cuidarem de dados sensíveis (art. 5º, II, da LGPD), logo, impassíveis de tratamento com base no legítimo interesse, ainda que se trate de dado tornado manifestamente público.

Quanto às salvaguardas, certamente, mediante a demonstração objetiva de ciência prévia do titular de que dados manifestamente públicos poderão ser levados em consideração, se acrescenta variável que poderia viabilizar o uso da informação. Eventual discriminação abusiva e comportamento dissonante do preconizado pela LGPD, nessa situação, não se relacionará ao princípio da vedação de tratamento sem base legal sob o enfoque do legítimo interesse, podendo incidir o sistema de responsabilidade previsto na própria lei ou em outras normas.

3.6. Utilização de sistemas de vigilância para identificar fumantes em determinado estabelecimento

Tem-se a seguinte situação: determinada empresa utiliza câmeras ocultas para identificar fumantes em zonas proibidas dentro de suas dependências.

Na primeira etapa do teste, pode-se cogitar do interesse legítimo do controlador no cumprimento da legislação, na medida em que se cuida de atividade voltada a um só tempo para promoção e apoio de suas atividades, bem como a atividade de fiscalização beneficia a coletividade ao viabilizar a proteção da saúde daqueles que se encontram no referido lugar.

Na segunda etapa, relativa à necessidade, é improvável que se consiga justificar o tratamento, uma vez que há formas menos intrusivas de se atingir a finalidade almejada, a exemplo de sinalização ostensiva, detectores de fumaça e designação de área específica nos ambientes compatíveis e o impacto na privacidade da pessoa fumante seria desproporcional.

De igual sorte, não se lograria êxito na terceira etapa, pois o uso de câmeras ocultas para flagrar eventual transgressão à legislação, não se coaduna com o princípio da transparência e, tampouco, com o da boa-fé objetiva, além de se expor desnecessariamente os titulares à coleta de dados, tanto fumantes quanto não fumantes. De igual sorte, não se pode pensar em salvaguardas, uma vez que se está a defender a inaplicação do legítimo interesse nessa situação.

No caso, conquanto a fiscalização em si não seja, propriamente, dever legal, a atrair, de plano, a incidência do art. 7º, II, da LGPD, uma vez que a legislação sobre as restrições ao uso e à propaganda de produtos fumíferos, derivados ou não do tabaco, confere ao responsável por recinto coletivo fechado a possibilidade de advertência ou retirada do recinto do usuário recalcitrante de produtos fumígenos⁴²². Não se pode negar que a identificação do fumante transgressor é medida prévia e necessária à adoção da conduta legalmente autorizada. Assim, se a condição de fumante é informação relacionada à pessoa natural, identificada ou identificável, acaso se pretenda utilizar essa informação, deve-se observar a axiologia da LGPD.

⁴²² BRASIL. **Lei 9.294 de 15 de julho de 1996**. Dispõe sobre as restrições ao uso e à propaganda de produtos fumíferos, bebidas alcoólicas, medicamentos, terapias e defensivos agrícolas, nos termos do § 4º do art. 220 da Constituição Federal. DOU de 16.7.1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/19294.htm>. Acesso em 4 dez. 2021; e BRASIL. Poder Executivo. **Decreto nº 2.018 de 1º de outubro de 1996**. Regulamenta a Lei nº 9.294, de 15 de julho de 1996, que dispõe sobre as restrições ao uso e à propaganda de produtos fumígenos, bebidas alcoólicas, medicamentos, terapias e defensivos agrícolas, nos termos do § 4º do art. 220 da Constituição. DOU de 2 out. de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D2018.htm>. Acesso em 4 dez. 2021.

3.7. Atividade de monitoramento, detecção e prevenção de fraudes em redes de pagamento

Os agentes financeiros que compõem determinado ecossistema de pagamentos ostentam o legítimo interesse de protegerem as marcas envolvidas e, também, a própria rede. Da mesma forma, as instituições financeiras possuem interesse na prevenção da ocorrência de fraudes e minimização de suas perdas. Além disso, consumidores que utilizam esses serviços detêm interesse em utilizar ferramentas seguras e eficientes de pagamento.

Assim, no teste de prossecução, o legítimo interesse é aferível tanto pela presença de situação concreta (fiscalização de transações) quanto pelas finalidades legalmente estabelecidas (promoção de atividades do controlador e prestação de serviços em benefício do titular).

No exame da necessidade do tratamento e do respectivo impacto nos titulares, tem-se situação complexa, pois não parece adequado se estabelecer antecipadamente os dados necessários para a construção de perfil de consumo de determinado usuário dos serviços a permitir a identificação de transações fora do padrão esperado. Bioni observa que “[e]stá longe de ser simples a conciliação entre o princípio da minimização e a perspectiva de maximização de dados para formação de perfis mais precisos e, a princípio, mais refinados para o diagnóstico do que estaria fora do padrão do cliente”⁴²³. Mais uma vez se reforça a necessidade de análise contextual e quanto mais transparente for a conduta do agente de tratamento, no que diz respeito a informar e delimitar a fraude que pretende combater e os tipos de dados a serem coletados, mais fácil será justificar a necessidade do tratamento.

Quanto ao teste de proporcionalidade em sentido estrito, é possível reconhecer a legítima expectativa dos destinatários de receberem serviço de pagamento seguro, o qual beneficiará todos os envolvidos na relação e a preponderância dos interesses do agente de tratamento em manter o adequado funcionamento da rede de pagamentos.

Não se olvida que, provavelmente, os interesses do fraudador não serão atendidos, mas, consoante já explanado neste trabalho, há situações nas quais não é necessária a convergência de interesses entre o titular de dados e o controlador, em especial nas circunstâncias em que o benefício auferido ultrapassa o aspecto individual e tem potencial de abranger alguma coletividade.

⁴²³ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**, p. 260.

Ainda, nesse cenário, se pode perceber a potencial presença do legítimo interesse de terceiro, uma vez que “uma relação direta com o indivíduo não é essencial para se fundamentar o tratamento com base no legítimo interesse”⁴²⁴. Desse modo, é factível se estabelecer o compartilhamento de dados entre integrantes do sistema financeiro, além daquele que presta serviços ao cliente que se pretende proteger.

Em relação às salvaguardas, a transparência deve nortear o processo de coleta e tratamento de dados, mas essas não se adstringem a isso. Podem ser adotadas medidas de pseudoanonimização, a fim de se preservar a identidade do titular dos dados, criação de grupos com características similares e, assim, se evitar a construção e manutenção de perfis individualizados.

3.8. Promoção da segurança dos usuários de redes sociais que encorajam encontros presenciais ou permitem o compartilhamento de eventos reais dos utilizadores

Hoje, aplicativos dedicados a promover novos relacionamentos e encontros a partir de dados de localização de pessoas e do cruzamento de informações a seu respeito são utilizados por diversos indivíduos⁴²⁵. Da mesma forma, redes sociais voltadas para o compartilhamento de fotos e vídeos entre seus usuários também têm uso bastante difundido⁴²⁶.

A empresas que disponibilizam esses tipos de serviços têm o legítimo interesse de operar campanhas de *marketing* e publicidade, melhorar os serviços já prestados, bem como desenvolver novos e, também, impedir, identificar e combater fraudes e outras atividades ilegais não autorizadas.

Essas finalidades, desde que demonstradas em situações concretas, se enquadram na previsão abstrata do legítimo interesse na LGPD (art. 10, I e II). Logo, nas circunstâncias descritas, a primeira etapa do teste de ponderação estaria superada com êxito.

Em relação ao teste de necessidade e o respectivo impacto nos titulares, a análise contextual é de extrema relevância. Primeiro, se deve observar a natureza do serviço

⁴²⁴ DPN, **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**, p. 9.

⁴²⁵ A título de exemplo, menciona-se o Tinder. Segundo o site da empresa, o aplicativo está disponível em mais de 190 países e foi baixado mais de 450 milhões de vezes. *In*: MATCH GROUP, LLC. **Tinder Year in Swipe 2021™**, Tinder Newsroom. Disponível em: <<https://www.tinderpressroom.com/2021-12-06-Tinder-Year-in-Swipe-2021-TM>>. Acesso em: 13 dez. 2021.

⁴²⁶ De acordo com o sítio eletrônico da empresa, mais de um bilhão de pessoas utilizam a rede social Instagram. *In*: **About the Instagram Company**. Disponível em: <<https://about.instagram.com/about-us>>. Acesso em: 13 dez. 2021.

disponibilizado. A exposição do titular é inerente à atividade desenvolvida pelo agente de tratamento e a criação de uma conta de utilizador é ato discricionário do consumidor. Logo, na medida em que as finalidades de tratamento com base no legítimo interesse são claramente expostas ao destinatário do serviço e a coleta e tratamento dos dados do titular são realizados dentro desses parâmetros, é inarredável a conclusão de que é possível se proceder à fase subsequente.

No que diz respeito à terceira fase, proporcionalidade em sentido estrito sob o enfoque das legítimas expectativas dos titulares e da pontual preponderância dos interesses do controlador, é razoável se pressupor que os destinatários do serviço detêm a legítima expectativa de receber conteúdo adequado, de acordo com seu perfil, e, também, proteção em face de maus usuários, sendo forçoso se reconhecer que os interesses do controlador, quando não convergem, suplantam os do titular de dados.

Em relação às salvaguardas, ações de ordem técnica podem ser efetivadas, a exemplo de medidas que garantam que os endereços de IP dos usuários sejam utilizados apenas para os propósitos explicitados pelo prestador, da construção de perfis internos de utilizadores majoritariamente a partir de informações disponibilizadas pelos próprios consumidores dos serviços, transparência em relação aos elementos utilizados pelos algoritmos para a construção desses perfis, da disponibilização, de modo facilmente visualizável e compreensível, da possibilidade de exclusão da conta e dos dados disponibilizados pelo titular ao controlador.

3.9. O lucro como legítimo interesse

Poderia o lucro fundamentar o legítimo interesse à luz da LGPD? A Constituição Federal, no artigo 170, estabelece que a ordem econômica é fundada na valorização do trabalho humano e na livre iniciativa e tem por fim assegurar a todos existência digna, conforme os ditames da justiça social. Fábio Ulhoa observa que “[u]m desdobramento do princípio da livre-iniciativa é o reconhecimento da busca do lucro como o principal fator de motivação dos particulares”⁴²⁷.

No âmbito infraconstitucional, entre os elementos inerentes ao conceito de empresa está a finalidade lucrativa daquele que exerce profissionalmente atividade econômica, de forma

⁴²⁷ COELHO, Fábio Ulhoa, **Novo manual de direito comercial: direito de empresa [livro eletrônico]**, 31. ed. São Paulo: Thomson Reuters Brasil, 2020.

organizada, dirigida à produção e circulação de bens ou serviços habitualmente e mediante a assunção dos riscos de ordem técnica e econômica⁴²⁸.

Objetivamente, a partir da conjugação do art. 7º, IX, com o art. 10 da LGPD, o desenvolvimento da atividade econômica do controlador com fundamento na busca de lucros pode, em tese, sim, ser considerado legítimo interesse, uma vez que o intuito de lucro é lícito, representa um interesse real do agente de tratamento e é dotado de clareza.

A propósito, a redação dos dispositivos sob exame, os quais dispõem sobre a abrangência do legítimo interesse, parece corroborar essa conclusão, uma vez que a expressão "finalidades legítimas" está no plural, deixando clara a possibilidade de haver mais de uma finalidade legítima, bem como que se estabelece a sua identificação a partir de situações concretas, que incluem, mas não se limitam a: i) apoio e promoção de atividades do controlador; e ii) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Ainda que se defenda a necessidade de enquadramento em um dos incisos supramencionados, a intenção de gerar lucro está intimamente ligada à ideia de apoio e promoção de atividades do controlador. Logo, do ponto de vista abstrato, é possível se afirmar que o tratamento de dados com base no lucro enquanto legítimo interesse é plenamente possível.

Nesse sentido, Oliveira e Cots consideram que "é correto concluir que a busca pelo lucro permite o tratamento de dados pessoais sem o consentimento do titular e sem que tal tratamento esteja encaixado em nenhuma outra base legal, pois tal hipótese pode constituir hipótese de aplicação do legítimo interesse"⁴²⁹.

Todavia, o exame do legítimo interesse não se adstringe aos arts. 7º, IX, e 10 da LGPD. Há que se fazer leitura holística em torno de sua abrangência e coerência com o arcabouço protetivo dos dados dos indivíduos desenhado pelo legislador.

Então, deve-se considerar, também, que esse diploma legislativo estabelece como fundamentos da disciplina da proteção de dados pessoais (art. 2º), a livre iniciativa, a livre concorrência, a defesa do consumidor, o desenvolvimento econômico e tecnológico e a inovação, o respeito à privacidade, à autodeterminação informativa, às liberdades de expressão, informação, comunicação e opinião, além da inviolabilidade da intimidade, honra e imagem.

⁴²⁸ Código Civil, art. 966: Considera-se empresário quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços.

⁴²⁹ OLIVEIRA; COTS, **O legítimo interesse e a LGPD**, p. 74.

Ao lado desses fundamentos, há o dever de observância da boa-fé e de diversos princípios já abordados ao longo deste trabalho, estabelecidos no art. 6º.

Há que se esclarecer ainda que, embora reconhecido como lícito pelo ordenamento jurídico, o desígnio de auferir lucros como interesse legítimo deve ser compreendido à luz das disposições da LGPD. Logo, calha rememorar distinção entre os conceitos de interesse e finalidade dentro desse sistema.

De acordo com essa lei, o princípio da finalidade preconiza a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I).

E o interesse que autoriza a respectiva categorização como legítimo (art. 7º, IX), segundo o parâmetro do princípio da vedação do tratamento, seria o elemento material que conduz a definição da finalidade do tratamento sob o prisma jurídico.

Desta sorte, o interesse ostenta caráter prévio e mais amplo do que a própria definição da finalidade do tratamento. Aquele seria, em verdade, sua razão intrínseca e essa sua expressão jurídica.

Portanto, é a finalidade que deve guiar o comportamento do agente de tratamento e essa deve ser clara, específica e anterior ao efetivo tratamento dos dados pessoais.

Com efeito, a finalidade lucro, dissociada de elementos concretos, obscurece, também, o princípio da necessidade, uma vez que não há como se delimitar quais seriam os dados estritamente necessários ao seu atendimento.

Outrossim, quanto mais imprecisa for a fundamentação do legítimo interesse, mais improvável será a demonstração de atuação conforme a lei e, de igual sorte, ainda que existam instrumentos que permitam a avaliação da retidão da conduta do agente de tratamento (o teste de balanceamento e suas etapas sucessivas), a impossibilidade de sua utilização decorrente da ausência de objetivo claro e ligado a situações concretas inviabiliza o seu uso enquanto substrato fático.

Em consequência, o reconhecimento da idoneidade do tratamento de dados com base no legítimo interesse lucro pode abrir margem para que o agente de tratamento atue sem balizas normativas objetivas e processe os elementos de informação recolhidos da maneira que bem entender. Há possibilidade, inclusive, de atuação violadora das legítimas expectativas dos titulares.

No ponto, a dimensão do legítimo interesse enquanto elemento irradiador de deveres parece funcionar como óbice à atuação da forma como acima descrita, pois o interessado deve

se desincumbir dos deveres de fundamentar adequadamente o tratamento, de atrelar o interesse legítimo a finalidades legítimas a partir de situações concretas, de respeito às legítimas expectativas dos titulares de dados, de uso dos dados estritamente necessários à finalidade descrita e de documentação de todo o processo.

Logo, a adoção do fundamento de licitude legítimo interesse deve ser precedida de exame contextual e prévio, e resguardada a estreita consonância com as demais disposições referentes ao tratamento de dados pessoais constantes da legislação em vigor.

Nessa situação, o teste de balanceamento sequer poderia ser realizado adequadamente uma vez que o lucro é o pressuposto para o desenvolvimento de atividade empresarial e, embora não seja ilegal, não é, isoladamente considerado, suficientemente claro e concreto.

Assim sendo, na primeira fase de avaliação do interesse legítimo do responsável pelo tratamento (teste de prossecução), a ausência de finalidade concreta do tratamento levaria à falha na realização do teste. Já na segunda fase, não se revela possível mensurar o impacto nas pessoas em causa, uma vez que a intenção de lucrar pode permitir o tratamento de qualquer dado. No que diz respeito à fase de equilíbrio provisório, há o risco de frustração da legítima expectativa dos titulares na medida em que não se sabe para que o dado será utilizado, desde que gere lucro e, quanto às salvaguardas, a amplitude e vagueza do interesse não permite o seu implemento de modo preciso e eficaz.

CONCLUSÃO

As mudanças sociais são reflexo da construção da nova infraestrutura informativa⁴³⁰ e não é possível se desconsiderar a ubiquidade da coleta e tratamento de dados na dinâmica das relações interprivadas e do Estado em relação ao particular.

Não se pode partir da premissa de que o progresso tecnológico vem exclusivamente acompanhado de benefícios. A força disruptiva do crescente fluxo informacional e novas tecnologias exige contrapartida jurídica tempestiva e adequada.

Hoje os dados são elemento basilar das relações sociais e a circulação e detenção de informações a respeito dos titulares possui impactos diretos nas relações de poder entre agentes públicos e privados.

Deveras, “a preparação e gestão de programas de intervenção social, por parte dos poderes públicos, e o desenvolvimento de estratégias empresariais privadas; e o controle da conformidade dos cidadãos à gestão política dominante ou aos comportamentos prevalecentes”⁴³¹ são indissociáveis do manejo de extenso volume de informações sobre as pessoas.

Nessa conjuntura, fragmentos de informação produzidos e fornecidos pelos indivíduos a todo momento e em todo lugar ganham importância, inclusive econômica, na medida em que se estabelece uma relação de retroalimentação entre o reconhecimento do valor patrimonial dos dados e a sua crescente produção e coleta.

O conceito e a necessidade de privacidade são obscurecidos quando se observa a gama de serviços e produtos oferecidos em troca, também, do fornecimento de dados pelo titular. Estrutura-se o chamado capitalismo de vigilância⁴³².

Paradoxalmente, nenhum dado isoladamente considerado tem valor por si mesmo e, ao mesmo tempo, qualquer elemento de informação é relevante, a depender do contexto em que está inserido. Portanto, não existem dados insignificantes, uma vez que cada “pedaço de informação” contém subsídios que evidenciam fração da identidade do indivíduo que, se analisados contextualmente, permitem uma ampla visão sobre determinada pessoa.

Com efeito, ao longo de evolução de estudos sobre a privacidade, pelo menos desde a ideia do direito a ser deixado só passando pela possibilidade de "controle sobre informações de

⁴³⁰ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**, p. 38.

⁴³¹ *Ibid.*, p. 28–29.

⁴³² ZUBOFF, **The age of surveillance capitalism: the fight for a human future at the new frontier of power**.

caráter pessoal"⁴³³ se edificou larga base axiológica, conquanto não se possa afirmar que se trata de conceito uniformemente compreendido, o qual tem entre seus marcos o direito à autodeterminação informativa como um dos pilares da proteção de dados.

Esse fenômeno pode ser identificado a partir das gerações das leis que versam sobre proteção de dados que, no intento de regulamentar a possibilidade de intrusão de agentes públicos e privados no direito à privacidade de indivíduos, evoluíram da predominante adoção de linguagem técnica dirigida a estabelecer limites ao fenômeno do tratamento de dados, tendo-se estabelecido, ainda, a necessidade de, dentro de uma lógica de *accountability*, se garantir aos titulares de dados o desenvolvimento livre e consciente de sua personalidade.

Ao indivíduo, portanto, se deve assegurar o direito de saber “quando, como e em que medida”⁴³⁴ fragmentos de informação sobre si entram em circulação numa realidade socioeconômica cada vez mais orientada pela concepção do dado enquanto insumo economicamente relevante.

Hodiernamente, a sequência do fluxo informacional é "pessoa-informação-circulação-controle" (liberdade positiva), e não mais apenas "pessoa-informação-sigilo" (liberdade negativa, em torno da qual foi construída a noção clássica de privacidade)⁴³⁵. Atualmente, o titular do direito à privacidade pode exigir formas de circulação controlada de dados e não somente interromper o fluxo das informações que lhe digam respeito.

As respostas institucionais devem considerar, à luz do princípio da dignidade da pessoa humana, a posição de centralidade do indivíduo em todo o sistema, de modo que a defesa da privacidade e, também, do direito fundamental à proteção de dados, demanda a superação da lógica patrimonialista congregando-se interesses individuais e coletivos, “diferenciando a disciplina de acordo com as funções para as quais são destinadas as informações coletadas; analisando com maior profundidade os interesses envolvidos nas diversas operações e colocando em funcionamento novos critérios para o equilíbrio de tais interesses”⁴³⁶.

A propósito, o reconhecimento pelos ordenamentos jurídicos, de forma positivada ou não, do direito fundamental à proteção de dados se revela de fundamental importância sob o ângulo de sua instrumentalização.

⁴³³ BESSA, **O consumidor e os limites dos bancos de dados de proteção ao crédito**, p. 92.

⁴³⁴ WESTIN, **Privacy and Freedom**, p. 7.

⁴³⁵ RODOTÀ, **A vida na sociedade da vigilância: a privacidade hoje**.

⁴³⁶ *Ibid.*, p. 50.

Afinal, além e em razão de sua densidade constitucional, se permite o desenvolvimento de políticas públicas, a formulação de pleitos judiciais e a sua conformação por meio de manifestações jurisdicionais que considerem sua autonomia e o identifiquem como ferramenta indispensável para o pleno desenvolvimento da personalidade e componente da "cidadania do novo milênio"⁴³⁷.

No caso do Brasil, o Supremo Tribunal Federal, de forma sensível às mudanças sociais, se manifestou pela atribuição à proteção de dados da qualidade de direito fundamental e tornou a Constituição o anteparo normativo e eixo principiológico sobre o qual se edificará seu amadurecimento.

Cuida-se de manifestação revestida de absoluta importância, na medida em que "tem o Poder Judiciário um papel de extraordinária relevância, quer abrindo as portas que a inércia do legislador fechou, quer agasalhando demandas de proteção contramajoritárias, nos limites do ordenamento jurídico"⁴³⁸.

Demais disso, a previsão constitucional do direito fundamental à proteção de dados e a Lei Geral de Proteção de dados exsurtem como resposta do legislador às transformações decorrentes da reconfiguração das relações sociais em razão do avanço tecnológico e da capacidade de processamento de informações pelos agentes públicos e privados.

Trata-se de normas de elevado teor principiológico, de modo que se pode inferir sua dimensão diacrônica. Os conceitos abertos permitem a sua adaptação às modificações sociais de sorte que o transcurso do tempo não se caracterize como elemento distanciador entre a realidade dos fatos e as normas regentes.

Deve-se considerar, ainda, a existência da possibilidade de diálogo entre diplomas normativos distintos em ordem a se estabelecer o microsistema de proteção de dados sob o influxo da teoria do diálogo das fontes, principalmente diante da redação do art. 64 da LGPD.

Quanto ao processamento de dados pessoais, o princípio da vedação do tratamento de dados estabelece a impossibilidade de sua realização quando ausente fundamento de licitude previsto em lei apto justificá-lo e a opção por uma ou outra base legal impõe ao agente de tratamento o dever demonstrar a adequada subsunção entre a finalidade de tratamento e a respectiva base legal.

⁴³⁷ *Ibid.*, p. 17.

⁴³⁸ FACHIN, *Direito Civil sentidos, transformações e fim.*, p. 34.

Deveras, as hipóteses legais de tratamento de dados não podem ser compreendidas sem o conhecimento prévio da essência do direito à privacidade e da sua evolução sob a perspectiva de elemento fundante do direito fundamental à proteção de dados.

Nesta senda, a transparência é a premissa para a efetiva participação dos indivíduos, fontes de dados, no fenômeno da circulação de informações sobre si. Além disso, a demonstração de finalidade clara viabiliza o escrutínio permanente (pela sociedade e autoridades públicas) da atividade de tratamento independentemente da efetiva ocorrência de violação aos preceitos insculpidos na LGPD.

Ademais, o princípio da finalidade desempenha função relevante na medida em que serve, a um só tempo, como norte e limite da atuação do agente de tratamento, principalmente nas situações em que o fornecimento de dados pelo titular é consequência da própria utilização do serviço e o indivíduo deve ser resguardado da utilização de dados que extrapolam as finalidades da coleta.

Na sociedade da informação, o processamento de dados, em si considerado, muito dificilmente é o que efetivamente se busca ao se disponibilizar um produto ou serviço, de forma gratuita ou não. Em verdade, essa atividade acompanha o fornecimento de bens da vida pretendidos pelos titulares de dados e, a partir dos dados coletados, os agentes de tratamento desenvolvem meios de potencializar a consecução de seus objetivos.

São diversos produtos e serviços que continuamente coletam fragmentos de informação sobre o titular e o exame sobre os riscos e prejuízos decorrentes da oferta do consentimento é muito complexo, sem se olvidar que a distorção do mercado pela assimetria de forças entre o titular e os agentes de tratamento compromete a ideia de consentimento enquanto manifestação livre, informada e inequívoca da vontade do titular.

Há que se fazer um exame holístico e contextual do tratamento, o qual deve ser sindicável pelos próprios titulares e, também, pelos sujeitos legalmente incumbidos dessa tarefa.

Nesse cenário, a adoção do consentimento como *standard* para o tratamento de dados demanda de quem o concede tempo de análise e capacidade de compreensão das consequências desse ato que vão além do que se espera do indivíduo comum. Logo, o paradigma do consentimento deve ser interpretado considerando-se a condição de vulnerável do titular de dados.

Existem dez bases legais de tratamento de dados, cada uma com seu propósito e a sua escolha fica a critério do operador. Desta sorte, o consentimento não pode ser considerado como

principal base legal para o tratamento de dados, assim como nenhum outro permissivo, uma vez que não há que se falar em hierarquia entre os fundamentos de licitude para o processamento de dados pessoais.

Nessa linha de raciocínio, calha pontuar que o tratamento de dados com base no legítimo interesse nem deve ser utilizado apenas como último recurso e, tampouco, como primeira opção pelo controlador ou terceiro.

Essa base legal, a qual ostenta a mesma qualidade das demais previstas em lei, embora se mostre, em exame mais apressado, menos restritiva, é de complexa operacionalização, sendo certo que as peculiaridades de cada situação, circunstancialmente examinadas, é que definirão se o tratamento foi lícito ou não.

Neste trabalho se apontou a lacuna científica em torno do questionamento sobre a adoção do legítimo interesse para o tratamento de dados se consubstanciar em flexibilização do consentimento ou sua densificação. Para se chegar a alguma conclusão, é imprescindível se examinar as nuances dessa hipótese de tratamento.

A LGPD foi influenciada pelo GDPR e, nessa perspectiva, o recurso à abordagem pelo direito europeu dos institutos jurídicos similares serve como relevante norte hermenêutico, em especial quanto ao legítimo interesse o qual existe naquele sistema pelo menos desde a Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

No que diz respeito ao legítimo interesse em si considerado, esse pode ser compreendido sob dois aspectos: a) base legal para o tratamento de dados; e b) elemento irradiador de deveres que permitem o tratamento de dados com amparo nessa hipótese normativa.

Assim, nos termos da LGPD, impede destacar que o legítimo interesse do controlador ou de terceiros deve guardar correlação com finalidade vinculada ao apoio e promoção das atividades do controlador ou proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem.

Ainda que não haja limitação legal a essas duas hipóteses, uma vez que o art. 10 expressamente dispõe que o legítimo interesse não se limita a elas⁴³⁹, salienta-se a necessidade de ligação a essas finalidades pré-estabelecidas diante obrigatoriedade de sua inclusão na fundamentação do tratamento.

⁴³⁹ O *caput* do art. 10, da LGPD dispõe que “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 se limitam a (...)”.

Ademais, a coleta de dados deve ser restrita, cingindo-se aos dados estritamente necessários ao cumprimento do objetivo. De igual sorte, devem ser observados o respeito aos direitos e liberdades fundamentais do titular, bem como suas legítimas expectativas e deve haver o registro das operações de tratamento.

Ainda, seguindo-se a linha proposta pelo direito europeu, em especial quanto ao tratamento com base no legítimo interesse, deve ser observada a obrigação de transparência e documentação da atividade do responsável⁴⁴⁰.

Cuida-se de diretrizes que se revestem de absoluta importância, pois se permitirá o escrutínio do caso concreto com maior clareza e segurança para todas as partes envolvidas, bem como se viabiliza a elaboração de relatório de impacto à proteção de dados pessoais⁴⁴¹.

No caso da LGPD, o dever de anotação das operações de tratamento, para além de obrigação legal, é manifestação de boa prática que deve ser seguida por aqueles que se predispõem a tratar dados.

É que o registro das atividades do responsável pelo tratamento com base no legítimo interesse viabiliza o controle posterior da retidão de sua conduta, bem como a apuração de comportamento ilícito ensejador de responsabilização e, de igual forma, possibilita ao titular se insurgir contra condutas do controlador que julgue incompatíveis com seus interesses.

Há, aqui, interessante ponto de contato com o Direito do Consumidor, na medida em que a transparência se revela como instrumento de tutela do direito do titular de dados e de prevenção da prática de abusos⁴⁴².

Não se pode olvidar, ainda, da imprescindibilidade da análise quanto ao pertencimento do fragmento de informação à categoria de "dado pessoal sensível", pois essas informações encontram regulamentação em seção própria na LGPD, a partir do artigo 11⁴⁴³.

⁴⁴⁰ Artigo 37 da LGPD e Considerando 39 da RGPD.

⁴⁴¹ Artigo 10, § 3º, da LGPD.

⁴⁴² A propósito, consta do Parecer 6/2014 que: [a] este respeito, o Grupo de Trabalho salienta que a legislação em matéria de defesa do consumidor, em especial as leis que defendem os consumidores contra práticas comerciais desleais, é igualmente muito relevante neste contexto. Se o responsável pelo tratamento esconder informações importantes a respeito de uma inesperada utilização posterior dos dados, camufladas em cláusulas jurídicas escritas em caracteres reduzidos num contrato, tal pode violar as normas de defesa do consumidor relativas às cláusulas contratuais abusivas (nomeadamente a proibição de «cláusulas-surpresa») e também não preencherá os requisitos previstos no artigo 7.º, alínea a), para um consentimento válido e informado, nem os requisitos previstos no artigo 7.º, alínea f), em termos de expectativas razoáveis da pessoa em causa e de equilíbrio de interesses global aceitável. Obviamente, levanta também questões de conformidade com o artigo 6.º no que se refere à necessidade de um tratamento leal e lícito dos dados pessoais. EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conformidade com o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p. 69.

⁴⁴³ Seção II Do Tratamento de Dados Pessoais Sensíveis

A análise contextual do tratamento também desempenha importante função, pois "dados aparentemente inócuos, quando sejam tratados em grande escala e combinados com outros dados, podem dar azo a inferências sobre dados mais sensíveis"⁴⁴⁴ e cabe ao agente de tratamento justificar a sua atividade, sob pena de responsabilização.

Nesses casos, o princípio da necessidade irradia efeito limitador da atuação do tratador de dados, pois se deve perquirir sobre a possibilidade de o interessado obter a informação desejada por mecanismo diverso da intrusão na esfera individual das pessoas, em ordem a reduzir a possibilidade de a construção de perfis impactar negativamente sobre os titulares.

Não se trata de contradição, pois esse instituto limita a escolha da base legal de tratamento, mas não impede a sua opção. Dito de outra forma: o ônus de demonstrar a higidez do tratamento de dados com base no legítimo interesse é do controlador ou do terceiro e, na hipótese de sua atuação se dar em desconformidade com a lei, deverá incidir o sistema de responsabilidade previsto pelo legislador.

No que tange às expectativas razoáveis, a natureza da relação que permite o acesso aos dados do titular deve ser considerada, pois o contexto em que se deu a sua coleta é parâmetro importante na análise da amplitude e retidão do tratamento que se pretende realizar.

Desta sorte, devem ser examinadas as expectativas e o comportamento de quem realiza a coleta dos dados e do titular de dados. A situação concreta é que permitirá a análise contextual sobre o impacto do tratamento na relação dos indivíduos, uma vez que as repercussões nas esferas jurídicas dos titulares não necessariamente ocorrem na mesma intensidade.

Ademais, outros aspectos usualmente presentes nas relações de processamento de dados são, também, relevantes, porquanto contribuem para o exame amplo do comportamento do agente de tratamento, v.g.: a) o direito de oposição ao tratamento por parte do titular; e b) a possibilidade de responsabilização do agente de tratamento em caso de atuação dissonante do preconizado pela legislação de regência.

O direito de oposição ao tratamento de dados não se restringe à hipótese prevista no artigo 18, § 2º, da LGPD⁴⁴⁵. Isto é, além da oposição justificada no descumprimento do disposto em lei, o responsável pelo tratamento que permita ao titular se opor ao processamento de dados,

⁴⁴⁴ EDPB, **Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**, p.62.

⁴⁴⁵ Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

a qualquer tempo e de forma irrestrita, pode contribuir para a consolidação de uma relação menos desequilibrada.

Já a cláusula geral de responsabilização do “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 proteção de dados pessoais” associada à previsão de rol de hipóteses excludentes da responsabilidade⁴⁴⁶ exerce importante papel orientador da conduta dos agentes de tratamento.

Nesse contexto, o teste de ponderação se sobressai como instrumento que permite ao titular de dados e aos agentes competentes o escrutínio da atividade de tratamento de dados.

A sucessão das etapas para o efetivo tratamento pode ser compreendida como uma cadeia na qual a fase subsequente é interligada à anterior, de modo a se garantir a lisura do processamento de dados durante toda a sua realização.

Assim, estabelecida a finalidade em abstrato (primeira fase), passa-se, considerando-se a finalidade descrita, ao momento do exame da necessidade e do impacto sobre o titular de dados (segunda fase). A partir da conclusão da segunda fase, chega-se à terceira, na qual se verifica se se resguardaram as legítimas expectativas do titular e a prevalência dos interesses do agente de tratamento no caso concreto. As salvaguardas são utilizadas para se viabilizar a interligação das fases e, também, se proteger os direitos e liberdades fundamentais dos titulares de dados, podendo serem consideradas medidas a serem adotadas em etapa autônoma ou não.

Não se pode olvidar que o teste de balanceamento, embora evidencie o liame entre a escolha do tratamento com fundamento no legítimo interesse e o efetivo processamento, não pode conduzir a uma inviabilização do tratamento em razão de repercussão negativa sobre a esfera individual do titular de dados. Ao contrário. O aspecto preponderante é evitar um impacto desproporcional e não qualquer influência sobre a esfera individual das pessoas.

Calha destacar que o teste de equilíbrio não é um fim em si mesmo, ao passo que a proteção de dados não pode ser concebida como direito absoluto⁴⁴⁷. A funcionalização do

⁴⁴⁶ Arts. 42 e 43 da Lei Geral de Proteção de dados

⁴⁴⁷ A propósito, o Parecer 6/2014 esclarece bem esse ponto: “(...) é importante salientar que nem todos os impactos negativos nas pessoas em causa têm o mesmo «valor» na ponderação. A finalidade do exercício de ponderação previsto no artigo 7.º, alínea f), não é evitar qualquer efeito negativo na pessoa em causa. A sua finalidade é antes evitar um impacto desproporcionado. Esta diferença é essencial. Por exemplo, a publicação de um artigo de jornal elaborado com base numa investigação aprofundada e de forma cuidadosa sobre um caso de alegada corrupção governamental pode prejudicar a reputação dos funcionários governamentais envolvidos e pode ter consequências

instituto demanda o sopesamento com outros direitos fundamentais, à luz do princípio da proporcionalidade.

As manifestações doutrinárias e dos órgãos jurisdicionais, similarmente ao que ocorre com o Código de Defesa do Consumidor, desempenham papel fundamental na orientação da atividade do agente econômico sujeito às disposições da LGPD.

A situação de equilíbrio desejável deve ser demonstrada a partir do confronto entre as medidas adotadas pelo responsável pelo tratamento fundado no legítimo interesse e o impacto sobre o titular de dados.

Destarte, a solução ótima parece estar na convergência entre o compromisso com a finalidade declarada pelo controlador para o tratamento baseado no legítimo interesse e a menor repercussão na esfera individual do titular.

Portanto, a adoção da base legal legítimo interesse não refreia o consentimento, mas, tampouco, se pode dizer que o densifica.

Em verdade, a convivência de ambas as hipóteses legais permite a conclusão no sentido de que a autodeterminação informativa vai além do consentimento⁴⁴⁸ e permeia toda e qualquer atividade relacionada ao processamento de dados.

Com efeito, o legítimo interesse é hipótese de processamento de dados não sensíveis dissociada do consentimento e baseada no risco da atividade. Deve ser utilizado sempre que o agente de tratamento desejar e julgar ter condições de justificá-la dentro das balizas normativas da LGPD.

Embora não se possa dizer que o consentimento é afetado pela existência do legítimo interesse, sua previsão robustece a privacidade sob as lentes do direito fundamental à proteção de dados. Afinal, não se está diante de "cheque em branco" para o seu processamento.

Assim, sob esse ângulo, a imperiosidade de justificativa racional e conforme o direito enaltece o próprio sistema de proteção de dados dos indivíduos, pois o agente de tratamento, durante o registro de sua atividade é obrigado a lidar com elementos normativos caros ao seu funcionamento e a demonstrar o respeito a liberdades e garantias fundamentais dos indivíduos.

significativas, nomeadamente a perda de reputação, a perda de eleições ou a prisão, mas pode ainda assim encontrar fundamento no artigo 7.º, alínea f". EDPB, Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29. p.64.

⁴⁴⁸ BIONI, **Proteção de dados pessoais a função e os limites do consentimento**.

REFERÊNCIAS

- ALBERS, Marion. A complexidade da proteção de dados. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 10, n. 35, p. 19–45, 2016.
- ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5. ed. São Paulo: Malheiros, 2008.
- APPLE BRASIL. **Privacidade - Gerencie sua privacidade**. Apple (Brasil). Disponível em: <<https://www.apple.com/br/privacy/control/>>. Acesso em: 27 jul. 2021.
- ARAÚJO, Valter Shuenquener de. O princípio da proteção da confiança: uma nova forma de tutela do cidadão diante do Estado. Niterói: Impetus, 2009.
- ARNDT, A. B. Al-Khwarizmi. **The Mathematics Teacher**, v. 76, n. 9, p. 668–670, 1983.
- BAROCAS, Solon; NISSENBAUM, Helen. Big data's end run around anonymity and consent. **Privacy, Big Data, and the Public Good: Frameworks for Engagement**, 2014.
- BESSA, Leonardo Roscoe. **Nova Lei do Cadastro Positivo: comentários à Lei 12.414, com as alterações da Lei Complementar 166/2019 e de acordo com a LGPD**. São Paulo: Thomson Reuters Brasil, 2019.
- _____. **O consumidor e os limites dos bancos de dados de proteção ao crédito**. São Paulo: Revista dos Tribunais, 2003.
- _____; NUNES, Ana Luisa Tarter. Instrumentos processuais de tutela individual e coletiva: análise do art. 22 da LGPD. *In: Tratado de Proteção de Dados Pessoais*. 1. ed. Rio de Janeiro: Forense, 2021, p. 668–690.
- _____. **Lei de Proteção de Dados #1: Prof. Leonardo Bessa**. Youtube, 28 set. 2020. Disponível em: <<https://youtu.be/5clK1I2zdk>>. Acesso em: 20 out. 2021
- BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. *In: Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.
- _____. **Proteção de dados pessoais a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.
- _____; KITAYAMA, Marina; RIELLI, Mariana. **O legítimo interesse na LGPD: quadro geral e exemplos de aplicação**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.
- _____; RIELLI, Mariana Marques. **Legítimo interesse na LGPD Pano de fundo: conceito jurídico indeterminado e a sua posição na agenda regulatória da ANPD**. JOTA Info. Disponível em: <<https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-anpd-dados-01032021>>. Acesso em: 8 abr. 2021.

BOBBIO, Norberto. **Teoria do ordenamento jurídico**. Trad. Maria Celeste C. J. SANTOS. 10. ed. Brasília: Universidade de Brasília, 1999.

BRASIL. Autoridade Nacional de Proteção de Dados. **Meus dados vazaram, e agora?** Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/meus-dados-vazaram-e-agora>>. Acesso em: 15 fev. 2021.

_____. Câmara dos Deputados. **Câmara aprova em 2º turno PEC que inclui a proteção de dados pessoais na Constituição - Notícias**. Portal da Câmara dos Deputados. Disponível em: <<https://www.camara.leg.br/noticias/801696-camara-aprova-em-2o-turno-pec-que-inclui-a-protecao-de-dados-pessoais-na-constituicao/>>. Acesso em: 31 ago. 2021.

_____. Câmara Legislativa. **Relatório da Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, DE 2012 (Tratamento e Proteção de Dados Pessoais)**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305>. Acesso em 11 abr. 2021.

_____. **Lei 13.709/18, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, Diário Oficial da União de 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>. Acesso em: 15 jun. 2021.

_____. **Lei 9.294 de 15 de julho de 1996**. Dispõe sobre as restrições ao uso e à propaganda de produtos fumíferos, bebidas alcoólicas, medicamentos, terapias e defensivos agrícolas, nos termos do § 4º do art. 220 da Constituição Federal. Brasília, DF, Diário Oficial da União de 16 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/19294.htm>. Acesso em 4 dez. 2021;

_____. **Lei Nº 12.414, de 9 junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF, Diário Oficial da União de 10 jun. 2011. Acesso em 6 ago. 2021.

_____. **Lei Nº 8.078, de 11 set. de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF, Diário Oficial da União de 12 set. 1990, retificado em 10 de jan. de 2007. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm>. Acesso em: 14 abr. 2021.

_____. Ministério da Economia. **Exposição de motivos nº 00151/2020**. Brasília, DF, Diário Oficial da União de 15 abr. 2020. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Exm/Exm-MP-954-20.pdf>.

Acesso em 17 jun. 2021.

_____. Poder Executivo. **Decreto N° 10.474, de 26 de agosto de 2020**. Brasília, DF, Diário Oficial da União de 27 ago. 2020. Disponível em: <<https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>>. Acesso em 10 out. 2021.

BRASIL. Poder Executivo. **Decreto nº 2.018 de 1º de outubro de 1996**. Regulamenta a Lei nº 9.294, de 15 de julho de 1996, que dispõe sobre as restrições ao uso e à propaganda de produtos fumígenos, bebidas alcoólicas, medicamentos, terapias e defensivos agrícolas, nos termos do § 4º do art. 220 da Constituição. DOU de 2 out. de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D2018.htm>. Acesso em 4 dez. 2021

_____. Poder Executivo. **Medida Provisória nº 954 de 17 de abril de 2020**. Brasília, DF, Diário Oficial da União de 17 abr. 2020 – edição extra. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm>. Acesso em 17 jun. 2021.

_____. Senado Federal. **Parecer nº 242 de 2021-PLEN/SF**. Rel. Senadora Simone Tebet, p. 2. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=9029060&ts=1634767663452&disposition=inline>>. Acesso em 21 out. 2021.

_____. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 17 jul. 2020.

_____. Superior Tribunal de Justiça (1 Seção). **Recurso Especial nº 976.836**. Rel. Min. Luiz Fux. Publicação: 5 out. 2010. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=924969&num_registro=200701873706&data=20101005&formato=PDF>. Acesso em 4 dez. 2021.

_____. Supremo Tribunal Federal (1. Turma). **Segundo Recurso Extraordinário com Agravo nº 950.586**. Rel. Min. Roberto Barroso. Publicação: 19 jun. 2019. Disponível em: <<https://jurisprudencia.stf.jus.br/pages/search/sjur406348/false>>. Acesso em: 10 jun. 2021.

BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus nº 91.867**. Relator: Min. Gilmar Mendes. Segunda Turma. Publicação: 20 set. 2012. Disponível em <https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22HC%2091867%22>

&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 20 jul. 2020.

_____. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade nº 6.387**. Relatora: Min. Rosa Weber. Publicação: 12 nov. 2020. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true>. Acesso em: 9 dez. 2020.

_____. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade nº 6.529**. Relatora: Min. Cármen Lúcia. Publicação: 22 out. 2021. Disponível em: <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837>>, acórdão pendente de publicação. Acesso em 21 out. 2021.

_____. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário nº 1.010.606**. Relator: Min. Dias Toffoli. Publicação 20 mai. 2021. Disponível em: <<http://stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786>>. Acesso em 17/06/2021.

_____. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário nº 418.416**. Relator: Min. Sepúlveda Pertence. Publicação: 19 dez. 2006. Disponível em <https://jurisprudencia.stf.jus.br/pages/search/sjur92577/false>. Acesso em: 20 jul. 2020.

CALO, M. R. Against Notice Skepticism in Privacy (and Elsewhere). **Notre Dame Law Review**, v. 87, n. 3, p. 1027–1072, 2012.

CANARIS, Claus-Wilhelm. **Pensamento sistemático e conceito de sistema na Ciência do Direito**. Trad. A. Menezes Cordeiro. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 2002.

CARNEIRO, Ramon Mariano. “Li e aceito”: violações a direitos fundamentais nos termos de uso das plataformas digitais. **Internet & Sociedade**, v. 1, n. 1, 2020. Disponível em: <<https://revista.internetlab.org.br/li-e-aceitoviolacoes-a-direitos-fundamentais-nos-termos-de-uso-das-plataformas-digitais/>>. Acesso em: 27 jan. 2021.

CARVALHO, Diógenes Faria de; MARQUES, Claudia Lima. Os significados da boa-fé nos contratos de serviços massificados: convergências entre o CDC, o CC/2002 e a Lei da Liberdade Econômica. In: MARQUES, Claudia Lima; LORENZETTI, Ricardo Luis; CARVALHO, Diógenes Faria de; *et al* (Eds.). **Contratos de serviços em tempos digitais: contribuição para uma nova teoria geral dos serviços e princípios de proteção dos consumidores [livro eletrônico]**. São Paulo: Thomson Reuters Brasil, 2021.

CIPL, Centre for Information Policy Leadership. **How the “Legitimate Interests” Ground for Processing Enables Responsible Data Use and Innovation.** Washington-London-Brussels: Hunton Andews Kurth, 2021. Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf>.

CITRON, Danielle Keats; PASQUALE, Frank A. **The Scored Society: Due Process for Automated Predictions.** Rochester, NY: Social Science Research Network, 2014. Disponível em: <<https://papers.ssrn.com/abstract=2376209>>. Acesso em: 30 dez. 2020.

COELHO, Fábio Ulhoa. **Novo manual de direito comercial: direito de empresa [livro eletrônico].** 31. ed. São Paulo: Thomson Reuters Brasil, 2020.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, p. 1373–1438, 2000.

CONSELHO DA EUROPA. **Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais de 28 de janeiro de 1981.** Disponível em: <<https://www.coe.int/en/web/conventions/full-list>>. Acesso em: 15 fev. 2021.

_____. **Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.** Disponível em: <https://www.echr.coe.int/documents/convention_por.pdf>. Acesso em: 15 fev. 2021.

CORDEIRO, Antonio Menezes. **Da boa fé no direito civil.** Coimbra: Almedina, 2013.

CORMEN, Thomas H.; LEISERSON, Charles E.; RIVEST, Ronald L.; *et al.* **Algoritmos - teoria e prática.** Trad. Vandenberg D. De Souza. 2. ed. São Paulo: Elsevier, 2002.

COSTA, Vinícius Venâncio. **Estaria o interesse legítimo presente apenas em dados de acesso público?** JOTA Info. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/estaria-o-interesse-legitimo-presente-apenas-em-dados-de-acesso-publico-06032020>>. Acesso em: 28 nov. 2020.

DE ANDRADE, Fábio Siebeneichler. **A tutela dos direitos da personalidade no direito brasileiro em perspectiva atual.** p. 32, 2013.

DEVORE, Andrew. **Statement of Andrew DeVore Vice President and Associate General Counsel Amazon.com, Inc. before the United States Senate Committee on Commerce, Science, and Transportation.** 2018. Disponível em: <<https://www.commerce.senate.gov/services/files/0F58A430-2037-4884-9B98-5FB3CA977838>>. Acesso em: 28 jul. 2021.

DÖHMANN, Indra Spiecker Gen. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. *In: Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91–108, 2011.

_____. **Da privacidade à proteção de dados pessoais [livro eletrônico]**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

_____. Panorama histórico da proteção de dados pessoais. *In: Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

DPN, Data Protection Network. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. Disponível em: <<https://iapp.org/resources/article/guidance-on-the-use-of-legitimate-interests-under-the-eu-general-data-protection-regulation/>>. Acesso em: 3 maio 2020.

DPN, Data Protection Network. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. 2018. Disponível em: <<https://dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf>>. Acesso em: 4 dez. 2021.

DUHIGG, Charles. **O poder do hábito: por que fazemos o que fazemos na vida e nos negócios [livro eletrônico]**. Trad. Rafael Mantovani. Rio de Janeiro: Objetiva, 2012.

EDPB, European Data Protection Board. **Grupo de Trabalho do Artigo 29.º | European Data Protection Board**. Disponível em: <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_pt>. Acesso em: 29 jul. 2021.

EDPB, European Data Protection Board - **Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na conforme o artigo 7.º da Diretiva 95/46/CE do Grupo de Trabalho para o Artigo 29**. 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf>. Acesso em: 28 nov. 2020.

FACEBOOK. **Sobre configurações de cookies para o pixel do Facebook**. Central de Ajuda do Facebook para Empresas. Disponível em: <<https://pt-br.facebook.com/business/help/471978536642445>>. Acesso em: 3 maio 2021.

FACHIN, Luiz Edson. **Direito Civil sentidos, transformações e fim**. Rio de Janeiro: Renovar, 2015.

FELIX, Samantha. **How Facebook Tracks Your Web Activity**. Business Insider. Disponível em: <<https://www.businessinsider.com/this-is-how-facebook-is-tracking-your-internet-activity-2012-9>>. Acesso em: 3 maio 2021.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In: A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.

_____ ; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. *In: Lei Geral de Proteção de Dados Pessoais e suas Repercussões no direito brasileiro [livro eletrônico]*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Disponível em:

<<https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>>. Acesso em: 5 abr. 2021.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. **Revista do Advogado**, v. 144, 2019.

HARARI, Yuval Noah. **21 lições para o século 21**. Trad. Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2018.

HILGENDORF, Eric; FELDLE, Jochen. **Digitalization and the Law**. Baden-Baden: Nomos, 2018.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito**. Trad. Ítalo Fuhrmann. Rio de Janeiro: Forense, 2021.

IAPP, International Association of Privacy Professionals. **Web Beacon**. Disponível em: <<https://iapp.org/resources/article/web-beacon/>>. Acesso em: 3 maio 2021.

ICO-UK, Information Commissioner's Office. **The UK GDPR**. Disponível em: <<https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/>>. Acesso em: 7 out. 2021.

_____. **What is the 'legitimate interests' basis?** Disponível em: <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>>. Acesso em: 28 nov. 2020.

JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 88, p. 439–459, 1993.

KESSLER, Joanna. Data protection in the wake of the GDPR: California’s solution for protecting “the world’s most valuable resource”. **Southern California Law Review**, v. 93, p. 31, 2019.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; DONEDA, Danilo (Orgs.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro [livro eletrônico]**. São Paulo: Thomson Reuters Brasil, 2020.

KOSINSKI, M.; STILLWELL, D.; GRAEPEL, T. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the National Academy of Sciences**, v. 110, n. 15, p. 5802–5805, 2013.

LEMOES, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. *In*: **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado**, v. 144, p. 67–73, 2019.

LIMA, Caio César Carvalho. Estudo prático sobre as bases legais da LGPD. *In*: **Proteção de dados - desafios e soluções na adequação à Lei**. 1. ed. Rio de Janeiro: Forense, 2020.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *In*: DONEDA, Danilo (Org.). **Caderno especial: a regulação da criptografia no direito brasileiro [livro eletrônico]**. 1. ed. São Paulo: Thomson Reuters Brasil, 2018.

MARCIN, SZCZEPANSKI. **Is data the new oil? Competition issues in the digital economy**. European Parliamentary Research Service, 2020. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf). Acesso em 3 abr. 2021.

MARQUES, Claudia Lima. Diálogo das fontes, aplicação das normas e teoria do direito: a teoria do diálogo das fontes hoje no Brasil e seus novos desafios: uma homenagem à magistratura brasileira. *In*: MARQUES, Claudia Lima; MIRAGEM, Bruno (Orgs.). **Diálogo das fontes: novos estudos sobre a coordenação e aplicação das normas no direito brasileiro [livro eletrônico]**. São Paulo: Thomson Reuters Brasil, 2020.

_____. Função Social do contrato como limite da liberdade de contratar e a confiança legítima no resultado em tempos digitais. *In*: MARQUES, Claudia Lima; LORENZETTI, Ricardo Luis; CARVALHO, Diógenes Faria de; *et al* (Eds.). **Contratos de serviços em tempos digitais: contribuição para uma nova teoria geral dos serviços e princípios de proteção dos consumidores [livro eletrônico]**. São Paulo: Thomson Reuters Brasil, 2021.

MARTINS-COSTA, Judith. A Re-significação do Princípio da Segurança Jurídica na Relação entre o Estado e os Cidadãos: a segurança como crédito de confiança. **Revista CEJ**, n. 27, p. 110–120, 2004.

MATCH GROUP, LLC. **Tinder Year in Swipe 2021™**. Tinder Newsroom. Disponível em: <<https://www.tinderpressroom.com/2021-12-06-Tinder-Year-in-Swipe-2021-TM>>. Acesso em: 13 dez. 2021.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. *In*: **Technology and Privacy: The New Landscape**. Cambridge: MIT Press, 1998.

_____; CUKIER, Kenneth. **Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight**. Londres: John Murray, 2013.

MENDES, Laura Schertel. O direito Fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 20, n. 79, 2011.

_____; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. *In*: **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

_____; FONSECA, Gabriel Campos Soares da; JÚNIOR, Otavio Luiz Rodrigues. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

_____; MATTIUZZO, Marcela; FUJIMOTO, Mônica Tiemy. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *In*: **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MICHAEL, James. **Privacy and Human Rights**. Londres: Dartmouth Publishing Company, 1994.

MUCELIN, Guilherme. Transformação digital e diálogo das fontes: a interface jurídica de proteção das pessoas entre o virtual e o analógico. *In*: MARQUES, Claudia Lima; MIRAGEM, Bruno (Orgs.). **Diálogo das fontes: novos estudos sobre a coordenação e aplicação das**

normas no direito brasileiro [livro eletrônico]. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

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

OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**. São Paulo: Thomson Reuters Brasil, 2020.

O'NEIL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy**. Nova Iorque: Crown Publishers - Broadway Books, 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS, ONU. **Declaração Universal dos Direitos Humanos**. Disponível em:

<<https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>>. Acesso em: 15 fev. 2021.

OSOBA, Osonde A.; WELSER, William IV. **An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence**. Santa Monica: RAND Corporation, 2017. Disponível em: <https://www.rand.org/pubs/research_reports/RR1744.html>. Acesso em: 22 dez. 2020.

PARLAMENTO EUROPEU. **Carta de Direitos Fundamentais da União Europeia**. Disponível em: <[https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218(01)&from=EN)>. Acesso em: 15 fev. 2021.

PEREIRA, Daniel Queiroz. Direitos da personalidade e pessoa jurídica: uma abordagem contemporânea. **Revista da Faculdade de Direito da UERJ**, v. 2, n. 22, p. 1–20, 2012.

PETROLL, Martin de La Martiniere; PRADO, Paulo Henrique Muller. A theoretical essay on TV show placement and its effects on consumers/Um ensaio teórico sobre placement televisivo e seus efeitos sobre o consumidor. **Revista de Administração Contemporânea**, v. 18, n. 2, p. 176–196, 2014.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (LGPD)**. 1. ed. São Paulo: Saraiva Educação, 2018.

PONCE, Paula Pedigone; MATTIUZZO, Marcela. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. **Internet & Sociedade**, v. 1, n. 2, 2020. Disponível em: <<https://revista.internetlab.org.br/o-legitimo-interesse-e-o-teste-da-proporcionalidade-uma-proposta-interpretativa/>>. Acesso em: 2 fev. 2021.

PRINCE, Jeffrey; WALLSTEN, Scott. How Much is Privacy Worth Around the World and Across Platforms? **SSRN Electronic Journal**, 2020. Disponível em: <<https://www.ssrn.com/abstract=3528386>>. Acesso em: 19 abr. 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Trad. Danilo Doneda; Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – lei 13.709/2018. *In: Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

_____. Fundamentos constitucionais: O direito fundamental à proteção de dados. *In: Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013.

SCHWAB, Klaus. **A quarta Revolução Industrial [livro eletrônico]**. Trad. Daniel Moreira MIRANDA. São Paulo: Edipro, 2016.

SCHWARTZ, Paul M; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. **New York University Law Review**, v. 86, .

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 2015.

SILVA, Virgílio Afonso da. **Direitos Fundamentais: conteúdo essencial, restrições e eficácia**. 2. ed. São Paulo: Malheiros, 2009.

SOARES, Ricardo Maurício Freire. **O princípio constitucional da dignidade da pessoa humana em busca pelo direito justo**. São Paulo: Saraiva, 2010.

SOLON, Olivia. “Data soul” of Shawn Buckles sells for £288. **Wired UK**. Disponível em: <<https://www.wired.co.uk/article/shawn-buckles-is-worth-350-euros>>. Acesso em: 3 mai. 2021.

SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. Rochester, NY: Social Science Research Network, 2004. Disponível em: <<https://papers.ssrn.com/abstract=2899131>>. Acesso em: 21 jul. 2020.

SORO, Antonello. Vulnerable Person: Data Protection and Digital Society. **Digest: National Italian American Bar Association Law Journal**, v. 24, p. 117–132, 2016.

STEEL, Emily; LOCKE, Callum; CADMAN, Emily; *et al.* **How much is your personal data worth?** Financial Times. Disponível em: <<https://ig.ft.com/how-much-is-your-personal-data-worth/>>. Acesso em: 3 maio 2021.

TAVANI, Herman T.; MOOR, James H. Privacy protection, control of information, and privacy-enhancing technologies. **ACM SIGCAS Computers and Society**, v. 31, n. 1, p. 6–11, 2001.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1–38, 2020.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais comentada artigo por artigo**. Salvador: Juspodivm, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados na LGPD. *In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro [livro eletrônico]*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

TERRA, Aline de Miranda Valverde; MULLHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores on-line de dados pessoais. *In: FRAZÃO, Ana; TEPEDINO, Gustavo; DONEDA, Danilo (Orgs.). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro [livro eletrônico]*. São Paulo: Thomson Reuters Brasil, 2020, v. 1.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>>. Acesso em: 6 jul. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 3 maio 2021.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Digital economy report 2019: value creation and capture: implications for developing countries**. Genebra: United Nations, 2019. Disponível em: <https://unctad.org/system/files/official-document/der2019_en.pdf>. Acesso em: 23 abr. 2021.

VÉLIZ, Carissa. **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**. Trad. Samuel Oliveira. São Paulo: Contracorrente, 2021.

VIOLA, Mário; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.o E 11. *In: Tratado de Proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 131–162.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

WESTIN, Alan F. **Privacy and Freedom**. Nova Iorque: Atheneum, 1967.

WILCOX, Katherine M. “Hey Alexa, Do Consumers Really Want More Data Privacy?”: An Analysis of the Negative Effects of the General Data Protection Regulation. **Brooklyn Law Review**, v. 85, p. 30, 2019.

WU, Tim. **The Attention Merchants: The Epic Scramble to Get Inside Our Heads**. 1. ed. Nova Iorque: Alfred A. Knopf, 2016.

ZANATTA, Rafael Augusto; BIONI, Bruno; KELLER, Clara Iglesias; *et al.* Os Dados e o Vírus. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 14, n. 1, p. 231–256, 2020.

ZANFIR-FORTUNA, Gabriela; TROESTER-FALK, Teresa. **Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases. 2018**. Disponível em: <[https://www.ejtn.eu/PageFiles/17861/Deciphering_Legitimate_Interests_Under_the_GDPR%20\(1\).pdf](https://www.ejtn.eu/PageFiles/17861/Deciphering_Legitimate_Interests_Under_the_GDPR%20(1).pdf)>. Acesso em: 2 set. 2021.

ZANNIER, Frederico. **A bite of Me**. Kickstarter. Disponível em: <<https://www.kickstarter.com/projects/1461902402/a-bit-e-of-me>>. Acesso em: 3 maio 2021.

ZUBOFF, Shoshana. **It’s not that we’ve failed to rein in Facebook and Google. We’ve not even tried.** the Guardian. Disponível em: <<http://www.theguardian.com/commentisfree/2019/jul/02/facebook-google-data-change-our-behaviour-democracy>>. Acesso em: 21 abr. 2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: PublicAffairs, 2018.

About the Instagram Company. Disponível em: <<https://about.instagram.com/about-us>>. Acesso em: 13 dez. 2021.