

ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

DANIELA WENDT TONIAZZO

**O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS E O PROBLEMA DA
ASSIMETRIA INFORMACIONAL:
SOLUÇÕES A PARTIR DA CLÁUSULA GERAL DA BOA-FÉ OBJETIVA**

Porto Alegre
2022

PÓS-GRADUAÇÃO - *STRICTO SENSU*



Pontifícia Universidade Católica
do Rio Grande do Sul

DANIELA WENDT TONIAZZO

**O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS E O
PROBLEMA DA ASSIMETRIA INFORMACIONAL:
SOLUÇÕES A PARTIR DA CLÁUSULA GERAL DA BOA-FÉ OBJETIVA**

Dissertação apresentada como requisito para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Direito da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS.

Área de concentração: Fundamentos Constitucionais do Direito Público e do Direito Privado.

Orientadora: Profa. Dra. Regina Linden Ruaro

Porto Alegre

2022

Ficha Catalográfica

T665c Toniazzo, Daniela Wendt

O Consentimento na Lei Geral de Proteção de Dados e o Problema da Assimetria Informacional : soluções a partir da cláusula geral da Boa-fé Objetiva / Daniela Wendt Toniazzo. – 2022.

118 f.

Dissertação (Mestrado) – Programa de Pós-Graduação em Direito, PUCRS.

Orientadora: Profa. Dra. Regina Linden Ruaro.

1. LGPD. 2. Autodeterminação informativa. 3. Consentimento. 4. Boa-fé Objetiva. 5. Privacy by design. I. Ruaro, Regina Linden. II. Título.

DANIELA WENDT TONIAZZO

**O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS E O
PROBLEMA DA ASSIMETRIA INFORMACIONAL:
SOLUÇÕES A PARTIR DA CLÁUSULA GERAL DA BOA-FÉ OBJETIVA**

Dissertação apresentada como requisito para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Direito da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul – PUCRS.

Área de concentração: Fundamentos Constitucionais do Direito Público e do Direito Privado.

Aprovado em: 21 de junho de 2022.

BANCA EXAMINADORA:

Profa. Dra. Regina Linden Ruaro – Orientadora

Prof. Dr. Carlos Alberto Molinaro

Profa. Dra. Denise Pires Fincato

Prof. Dr. José Tadeu Neves Xavier

Profa. Dra. Têmis Limberger

À Isabel e à Manuela.

AGRADECIMENTOS

Agradeço aos meus pais, Elaine e Jose Renan, pelo estímulo contínuo, apoio incondicional e presença amorosa, neste e em todos os meus projetos de vida. Sem vocês, jamais seria possível.

Às minhas amadas filhas, Isabel e Manuela, por tolerarem tantas ausências e me ensinarem, diariamente, a ser um ser humano melhor.

À minha irmã-amiga, Josiane, pela parceria incondicional e pela tolerância, sempre que o meu bom humor esteve “um pouco” reduzido.

Às minhas amigas-irmãs, por estarem sempre por perto com palavras de incentivo e confiança.

Aos meus colegas de mestrado, pelo apoio e companheirismo durante toda a jornada, em especial, aos queridos Cláudio Damilano, Fernanda Ruaro e Tales Barbosa. Sem a amizade de vocês eu teria desistido no meio do caminho.

À Profa. Dra. Regina Linden Ruaro, minha querida orientadora, agradeço por ter me despertado para a temática pesquisada e ter aceitado meu convite de orientação; também por todas as palavras de estímulo e segurança ao longo desta trajetória. És uma mulher inspiradora! Obrigada por ter me conduzido até aqui.

Aos professores do Programa de Pós-graduação da Pontifícia Universidade Católica do Rio Grande do Sul, por todo o conhecimento compartilhado e pelo apoio no enfrentamento de um período tão atípico como o que vivenciamos, a pandemia. Em grupo fomos resilientes e criativos ao trocar conhecimentos e experiências, em busca dos nossos títulos de mestres.

“Quem corre porque quer, não cansa.”

Romilda Wendt (minha avó)

DESENHO

Traça a reta e a curva,
a quebrada e a sinuosa
Tudo é preciso.
De tudo viverás.

Cuida com exatidão da perpendicular
e das paralelas perfeitas.
Com apurado rigor.
Sem esquadro, sem nível, sem fio de prumo,
traçarás perspectivas, projetarás estruturas.
Número, ritmo, distância, dimensão.
Tens os teus olhos, o teu pulso, a tua memória.

Construirás os labirintos impermanentes
que sucessivamente habitarás.

Todos os dias estarás refazendo o teu desenho.
Não te fatigues logo. Tens trabalho para toda a vida.

Somos sempre um pouco menos do que pensávamos.
Raramente, um pouco mais.

Cecília Meireles

RESUMO

A Lei Geral de Proteção de Dados (LGPD) brasileira de n.º 13.709/18 representa importantíssimo marco legal para a proteção e garantia da pessoa humana, uma vez que facilita o controle dos dados tratados, impõe deveres e responsabilidades aos agentes envolvidos e proporciona segurança para que as informações circulem. A autodeterminação informativa foi reconhecida como um dos fundamentos da LGPD e alcança ao indivíduo o direito de decidir sobre o uso dos seus dados pessoais; sendo o consentimento principal base legal para o tratamento de dados pessoais, é instrumento fundamental para o exercício desse direito. Por sua vez, a inserção da cláusula geral da boa-fé objetiva, no *caput* do artigo 6º da LGPD, impõe um padrão ético e leal de conduta de todos os personagens envolvidos no tratamento de dados pessoais, especialmente daqueles que têm o domínio das tecnologias que coletam essas informações e que possuem a responsabilidade de zelar pela privacidade dos usuários. Nesse contexto, são identificadas as condutas legais e decorrentes da boa-fé objetiva dos controladores dos dados, a fim de se encontrar alternativas para mitigar a assimetria informacional presente nessas relações, bem como a conexão entre a boa-fé objetiva e o *privacy by design* como estrutura necessária para a proteção da confiança dos titulares sobre a segurança de suas informações no momento do consentimento.

Palavras-chave: LGPD. Autodeterminação informativa. Consentimento. Boa-fé objetiva. *Privacy by design*.

ABSTRACT

The Brazilian General Data Protection Law (LGPD) represents a very important legal framework for the protection and guarantee of the human person, since it facilitates the control of processed data, imposes duties and responsibilities on the agents involved and provides security for the information to circulate. Informative self-determination was recognized as one of the foundations of the LGPD and grants the individual the right to decide on the use of their personal data; while consent, the main legal basis for the processing of personal data, is a fundamental instrument for the exercise of this right. In turn, the insertion of the general clause of objective good faith, in the caput of article 6 of the LGPD, imposes an ethical and loyal standard of conduct for all characters involved in the processing of personal data, especially those who have mastery of technologies that collect this information and that are responsible for ensuring the privacy of users. In this context, the legal conduct resulting from the objective good faith of the data controllers will be identified, in order to find alternatives to mitigate the information asymmetry present in these relationships; as well as the connection between objective good faith and privacy by design as a necessary structure to protect the confidence of holders about the security of their information at the time of consent.

Keywords: LGPD. Informative self-determination. Consent. Objective good faith. Privacy by design.

SUMÁRIO

INTRODUÇÃO	10
1 A AUTODETERMINAÇÃO INFORMATIVA E O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS	14
1.1 BREVES CONSIDERAÇÕES SOBRE A ORIGEM DA AUTODETERMINAÇÃO INFORMATIVA.....	14
1.2 O CONSENTIMENTO COMO INSTRUMENTO DE EFETIVAÇÃO DA AUTODETERMINAÇÃO INFORMATIVA.....	22
1.3 A NATUREZA JURÍDICA DO CONSENTIMENTO.....	26
1.4 REQUISITOS DO CONSENTIMENTO VÁLIDO.....	32
1.4.1 Consentimento livre.....	36
1.4.2 Consentimento informado.....	39
1.4.3 Consentimento inequívoco e para uma finalidade determinada.....	41
2 A BOA-FÉ OBJETIVA COMO CLÁUSULA GERAL NAS RELAÇÕES REGIDAS PELA LGPD	45
2.1 CONSIDERAÇÕES INICIAIS E BREVES NOTAS SOBRE A EVOLUÇÃO HISTÓRICA DA BOA-FÉ.....	45
2.2 A BOA-FÉ NO ORDENAMENTO JURÍDICO BRASILEIRO.....	48
2.3 A BOA-FÉ OBJETIVA COMO CLÁUSULA GERAL.....	51
2.4 BOA-FÉ SUBJETIVA E BOA-FÉ OBJETIVA.....	54
2.5 AS FUNÇÕES DA BOA-FÉ OBJETIVA E OS DEVERES ANEXOS.....	56
2.6 A BOA-FÉ NA LEI GERAL DE PROTEÇÃO.....	61
3 ASSIMETRIA INFORMACIONAL E O CONSENTIMENTO NA LGPD: BUSCA DE SOLUÇÕES A PARTIR DA CLÁUSULA GERAL DA BOA-FÉ OBJETIVA	66
3.1 A IMPORTÂNCIA DO DEVER DE INFORMAÇÃO COMO SUPORTE AO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS.....	67
3.2 ASSIMETRIA INFORMACIONAL NAS RELAÇÕES DE TRATAMENTO DE DADOS E O MITO DO CONSENTIMENTO.....	74
3.3 DEVERES DE CONDUTA DOS AGENTES DE TRATAMENTO DE DADOS: EM BUSCA DA MITIGAÇÃO DA ASSIMETRIA INFORMACIONAL.....	82
3.3.1 Quem são os agentes de tratamento de dados?.....	85

3.3.2 Obrigações legais dos agentes de tratamento de dados e deveres decorrentes da cláusula geral da boa-fé objetiva no tratamento de dados pessoais.....	88
3.3.3A boa-fé e o <i>privacy by design</i>: arquitetura para a proteção do consentimento.....	96
CONCLUSÃO.....	105
REFERÊNCIAS.....	108

INTRODUÇÃO

A sociedade de informação e o intenso compartilhamento de dados exige, de todos os países do globo, sistemas jurídicos de grande mobilidade e constante adequação. Ao longo de pelo menos cinco décadas, a disciplina jurídica da proteção de dados pessoais vem sendo construída e ganhando contornos bastante específicos, principalmente em razão da massiva utilização de tecnologias que os manejam, nem sempre de forma apropriada e respeitando os limites da vida privada.

No Brasil, o marco legal da disciplina da proteção de dados ocorreu na promulgação da Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, e sua consolidação com o reconhecimento do direito à proteção de dados como um direito fundamental autônomo, a partir da Emenda Constitucional 115, de fevereiro de 2022, passando a constar no inciso LXXIX do artigo 5ª da Constituição brasileira, rol dos direitos e garantias fundamentais.

Assim como nas legislações europeias, o arcabouço legislativo nacional alcançou ao titular dos dados um grande protagonismo, procurando assegurar ao indivíduo domínio de todos os movimentos dos seus dados pessoais, desde a coleta até o compartilhamento, uma vez que positivou a autodeterminação informativa como um de seus fundamentos (artigo 2º, II, da Lei n.º 13.709/2018), ou seja, consignou o ideal de efetivo controle do titular sobre seus dados pessoais, implicando o poder de decisão sobre “o que”, “como”, “quando” e “onde” expô-los a tratamento.

Nesse influxo, o consentimento, como instrumento legitimador do uso de dados pessoais e garantidor da autodeterminação do indivíduo, merece destaque, ainda que outras bases legais possam ser utilizadas para o tratamento de dados, conforme o artigo 7º, incisos II ao X, da LGPD.

A política protetiva dos dados elegeu o consentimento como o grande instrumento para a proteção do indivíduo, condicionando a utilização de dados pessoais à sua existência e validade; assim, o presente estudo pretende aprofundar a análise das características do consentimento, que, de fato, garantem ao indivíduo a autodeterminação informativa, ou seja, o consentimento livre, informado, inequívoco e para uma finalidade determinada, e quais as condições necessárias para que todas essas características se perfectibilizem.

No entanto, mais do que o extensivo rol de adjetivos que devem qualificar o consentimento, parece indispensável a análise do contexto no qual ele ocorre e dos

pressupostos para a sua efetivação, porquanto o desequilíbrio informacional nas relações de tratamento de dados é incontroverso e o consentimento, por vezes, pode ser idealizado.

Atualmente, (i) as pessoas permanecem grande parte do dia conectadas à rede, seja através de seus dispositivos móveis, seja em computadores; (ii) existem programas e aplicativos, normalmente “gratuitos”, voltados a todas as esferas da vida privada, sejam eles para ouvir música, assistir filmes, ler livros, monitorar gastos, monitorar investimentos, monitorar dados de saúde, facilitar relações interpessoais (redes sociais), dentre outros; e (iii) a grande maioria desses programas e aplicativos exige permissão para acessar, coletar, armazenar, processar e transferir diversos dados do usuário, em outras palavras, exige o consentimento do titular dos dados para o seu tratamento.

Nesse cenário, não é exagero afirmar que as informações coletadas de um indivíduo, não raro, são suficientes para conhecer todos os aspectos da sua vida, como sua orientação política, religiosa, sexual, suas preferências esportivas, distrações, relacionamentos, seu histórico médico, seus interesses, opções de consumo, condições financeiras, dentre tantos outros. O conhecimento dessas informações pode ser utilizado de diversas formas, desde as mais impessoais, como para indicar nichos de mercado e interesses gerais, bem como para direcionar propaganda (desde a comercial à eleitoral) e até mesmo discriminar e chantagear.

A disponibilização de dados pessoais a partir do consentimento, em um contexto de marcante discrepância informacional e dificuldade cognitiva de seus titulares, remete a um problema: como garantir o direito à autodeterminação informativa dos indivíduos nesse contexto?

A própria Lei Geral de Proteção de Dados parece ter instrumentos para a busca dessa maior proteção ao consentimento, como expressão da autodeterminação informativa; uma delas parece ser a cláusula geral da boa-fé objetiva, prevista no *caput* do artigo 6º da lei.

De fato, o consentimento nas situações legais em que é exigido deve se perfectibilizar em um cenário marcado pela boa-fé objetiva, como princípio norteador das relações jurídicas e impositivo de condutas probas, leais e transparentes entre os envolvidos nas relações que envolvem tratamento de dados.

Nos sistemas jurídicos de formação ou inspiração germânica, a boa-fé é princípio que se assenta na ideia de fidelidade no agir. Assumindo um conteúdo de

juramento de honra, garantindo a manutenção e o cumprimento da palavra dada, levando-se em conta dois aspectos: a lealdade no cumprimento exato da obrigação e a necessidade de observância dos interesses da outra parte.

Nesse cenário, o consentimento, considerado comportamento central quando se aborda a disciplina de proteção de dados, merece ser analisado sob um enfoque ainda mais amplo do que o de costume, pretendendo-se investigar qual o comportamento esperado daqueles que participam das relações que envolvem tratamento de dados.

Em especial, questionam-se quais são os padrões de conduta coerentes com a boa-fé objetiva que devem ser observados pelos agentes de tratamento de dados pessoais para que a assimetria informacional, nessas relações, seja mitigada e se preserve a autodeterminação informativa dos indivíduos, através de um cenário ético, honesto e leal, onde se dará o consentimento.

Tal cláusula geral impõe, conjuntamente com os deveres legais, deveres que protegem a autodeterminação informativa, a adequação e a qualidade da interação do usuário com as tecnologias que captam seus dados, bem como dever de gerar confiança nesses usuários sobre o bom uso que se fará de seus dados.

Nesse sentido, na busca de se garantir um consentimento qualificado, identificar-se-ão os deveres dos agentes de tratamento de dados, legais e oriundos da boa-fé, bem como uma alternativa para a mitigação da assimetria informacional marcante nessas relações; ou seja, pretender-se-á demonstrar que uma arquitetura de rede amparada na cláusula geral da boa-fé, e em seus consectários, informação, transparência, lealdade e confiança, pode ser um caminho para resguardar um consentimento qualificado para o tratamento de dados pessoais.

Nesse contexto, a pesquisa será estruturada em três capítulos, sendo que, no primeiro, serão feitas breves considerações sobre a origem da autodeterminação informativa; será analisado o consentimento como instrumento de efetivação desse direito, bem como identificados os adjetivos para que o consentimento seja considerado válido e apto a amparar o tratamento de dados pessoais.

No segundo capítulo será delineado um breve histórico da boa-fé objetiva, sua evolução no ordenamento jurídico brasileiro, destacando sua modernidade e evolução conceitual e o seu papel como cláusula geral na Lei Geral de Proteção de Dados.

No terceiro capítulo da pesquisa o dever de informação, por ser destaque na disciplina de proteção de dados e suporte ao consentimento, será analisado

destacadamente para, na sequência, analisar-se o cenário de assimetria informacional no qual acontece a manifestação de vontade que autoriza o tratamento de dados pessoais, indagando-se se, no ambiente digital, é realmente possível a adjetivação plena do consentimento. Serão identificados os deveres de conduta dos agentes de tratamento de dados e as potencialidades da boa-fé objetiva como balizadora das condutas desses agentes e suas implicações na arquitetura de rede para a mitigação da assimetria informacional. E, por fim, identificadas as condutas legais e as decorrentes da cláusula geral da boa-fé a serem observadas pelos controladores para minimizar riscos à proteção de dados, analisar-se-á a conexão entre o *privacy by design* e a boa-fé como uma estrutura necessária para a proteção da confiança dos titulares sobre a segurança de suas informações no momento do consentimento.

A metodologia utilizada para a realização da presente pesquisa será a hipotético-dedutiva e, também, o método dialético, de maneira que se considera a constante evolução do direito e de seus institutos e sua implicação no cenário contemporâneo. Como método de interpretação, adotar-se-á o exegético, pois permite que se busque o verdadeiro sentido do alcance dos conceitos de consentimento e da cláusula geral da boa-fé objetiva. No que diz respeito aos tipos e técnicas de pesquisa, a técnica de pesquisa bibliográfica será amplamente utilizada, com vistas à consulta da literatura nacional e estrangeira.

A presente pesquisa insere-se na Área de Concentração “Fundamentos Constitucionais do Direito Público e do Direito Privado” do Programa de Pós-Graduação em Direito da PUCRS, e está ancorada na Linha de Pesquisa “Direito, Ciência, Tecnologia e Inovação”.

1 A AUTODETERMINAÇÃO INFORMATIVA E O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/2018, em seu artigo 2º, II, indica a autodeterminação informativa como um dos fundamentos da disciplina de proteção de dados pessoais em âmbito nacional¹ e foi definida por Stefano Rodotà como “[...] o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular”².

A autodeterminação informativa reconhece o direito do indivíduo de decidir sobre a divulgação e a utilização de seus dados pessoais, e possui no consentimento seu principal instrumento de efetivação.

Neste capítulo serão feitas breves considerações sobre a origem da autodeterminação informativa; será analisado o consentimento como instrumento de efetivação desse direito, bem como serão identificados os adjetivos para que o consentimento seja considerado válido e apto a amparar o tratamento de dados pessoais.

1.1 BREVES CONSIDERAÇÕES SOBRE A ORIGEM DA AUTODETERMINAÇÃO INFORMATIVA

O controle sobre os próprios dados constitui-se no direito à autodeterminação informativa e está no centro dos debates sobre a proteção de dados pessoais. Seu conceito surgiu na Alemanha e influenciou diversos ordenamentos jurídicos pelo mundo, sendo fundamento da Lei Geral de Proteção de Dados brasileira (artigo 2º, II).

A autodeterminação informacional foi reconhecida³ na decisão do Tribunal Constitucional alemão (*Bundesverfassungsgericht* – BVerfG), de 15 de dezembro de

¹ LGPD – Artigo 2º. A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

² RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 15.

³ Laura Mendes, em completo estudo sobre a história do conceito da autodeterminação informativa, afirma que, “[...] embora o direito à autodeterminação informativa tenha sido reconhecido constitucionalmente, pela primeira vez, na sentença referente ao recenseamento da população, em

1983, conhecida como a Decisão do Censo (*Volkszählungsurteil* 272 – BVerfGE 65,1). A decisão foi uma resposta da Corte a diversas reclamações constitucionais apresentadas contra a Lei do Recenseamento, que previa a realização do censo da população, identificando dados pessoais de ocupação, habitação e local de trabalho⁴, para fins de planejamento em todos os níveis de governo.

Os dados seriam úteis para a organização das políticas públicas⁵ e definição de escolhas administrativas. No entanto, o legislativo alemão decidiu aproveitar o ensejo para tentar atualizar e ampliar seus próprios cadastros de informações de cada cidadão. A Lei estabelecia quais dados seriam coletados e quem estava obrigado a fornecer as informações, previa a possibilidade de cruzamento de informações obtidas nesse recenseamento com as informações constantes nos bancos públicos, além de estabelecer a transmissão de dados tornados anônimos a repartições públicas da Federação, Estados e Municípios para a utilização administrativa⁶.

O BVerfG julgou o caso e afirmou que

[...] o processamento automatizado dos dados ameaçaria o poder do indivíduo de decidir por si mesmo se, e como ele desejaria fornecer a terceiros os seus dados pessoais, considerando que o processamento de dados possibilitaria a elaboração de um “perfil completo da personalidade” por meio de “sistemas automatizados integrados sem que o interessado pudesse controlar de forma suficiente sua correção e utilização”.

Tal utilização ampliaria a influência do Estado sobre o comportamento do indivíduo, que não mais seria capaz de tomar decisões livres em virtude “da pressão psíquica de participação pública”. Uma sociedade, “na qual os cidadãos não mais são capazes de saber quem sabe o que sobre eles, quando e em que situação”, seria contrária ao direito à autodeterminação informativa, algo prejudicial tanto para a personalidade quanto para o bem comum de uma sociedade democrática (BVerfGE 65,1 (42), Recenseamento).⁷

1983, seu desenvolvimento ocorreu ao longo de distintos julgados do Tribunal Constitucional da Alemanha e faz completa análise de cada um deles”. MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. p. 2. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 18 jun. 2021.

⁴ MARTINS, Leonardo. **Tribunal Constitucional Federal alemão**: decisões anotadas sobre direitos fundamentais. Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung, 2016. p. 55.

⁵ “Os motivos são razoavelmente claros: basta a constatação de que um pressuposto da administração pública eficiente é o conhecimento tão acurado e profundo quanto possível da população [...]” DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 34.

⁶ MARTINS, *op. cit.*, p. 55.

⁷ MENDES, *op. cit.*, p. 11.

O Tribunal Constitucional alemão concluiu que a combinação do direito ao livre desenvolvimento da personalidade com o princípio da dignidade da pessoa humana resulta em um direito à autodeterminação informativa, que alcança ao indivíduo o poder de determinar sobre a coleta e utilização de seus dados pessoais.

Na sentença referente ao recenseamento da população, o Tribunal Constitucional retoma tanto a abordagem da autodeterminação quanto a noção da limitação do comportamento por meio do processamento não transparente dos dados, a fim de conceber a partir do art. 2º, §1º combinado com o art. 1º, §1º, LF (dignidade da pessoa humana), o direito fundamental à autodeterminação informativa.⁸

Destarte, o direito à autodeterminação informativa constitui-se em desdobramento do direito geral da personalidade, e teve sua origem na necessidade de proteção do indivíduo contra o processamento automatizado de dados.

O processamento de dados configura potencial ameaça à personalidade do indivíduo e à sua dignidade na medida em que a combinação dos diversos dados armazenados possui o potencial de formar um retrato completo da pessoa sem a sua participação ou conhecimento.⁹

Esse cenário deixa o titular dos dados extremamente vulnerável, retirando-lhe a possibilidade de inferir sobre a interpretação e aplicação das informações que terceiro detém sobre ele, o que resulta em uma perigosa assimetria entre as partes.

Fabiano Menke, explicando sobre as origens alemãs e o significado da autodeterminação informativa, conclui que:

Uma das preocupações fundamentais da disciplina da proteção de dados é a de que o indivíduo não seja manipulado por informações que os seus interlocutores (sejam eles entes estatais ou privados) tenham sobre a sua pessoa, sem que ele saiba disso. Nestes casos de conhecimento prévio das informações sobre a outra parte, o detentor da informação invariavelmente se coloca numa posição privilegiada. Ele atalha os caminhos, adquirindo a possibilidade de manipulação e direcionamento. Pode fazer colocações e perguntas dirigidas, pois todo um caminho que teria de ser traçado para que chegasse a uma informação não precisa ser percorrido. Em suma, a relação não se desenvolve como no caso de um encontro que inicia “do zero”: perde sua espontaneidade e o seu natural desenvolvimento. É por isso que na dogmática da área, a expressão livre desenvolvimento da personalidade, do art. 2º, I, da Lei Fundamental, ganha realce, significando

⁸ MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. p. 11. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 18 jun. 2022.

⁹ *Id.* **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 31.

que o indivíduo deve ter a liberdade de ‘desdobrar’ a sua personalidade, no sentido de ele próprio se desenvolver: não deve ser permitido que tenha a sua personalidade encolhida.

Não é sem razão, que a LGPD, da mesma forma, e muito embora em nível infraconstitucional, contemplou a previsão do livre desenvolvimento da personalidade da pessoa natural, tanto como objetivo (art. 1º), quanto como fundamento da lei (art. 2º, VII). É por isso que é a chave da melhor compreensão da autodeterminação informativa é a de sua leitura conjunta como denominado livre desenvolvimento da personalidade.¹⁰

A partir da decisão do Tribunal Constitucional alemão, portanto, reconhece-se a existência de um direito à autodeterminação informacional, formulado a partir do direito geral de personalidade e voltado a garantir ao cidadão o direito de controlar a amplitude da divulgação ou utilização de seus dados pessoais¹¹. O reconhecimento do direito à autodeterminação informativa está intimamente ligado à própria história da proteção da personalidade como direito fundamental¹².

Ingo Sarlet¹³ também afirma haver uma conexão entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção de dados, destacando o princípio da autodeterminação e os direitos da personalidade, representados na decisão da Corte alemã pelo direito de natureza geral ao livre desenvolvimento e à autodeterminação informativa.

Apesar do grande destaque da decisão do Tribunal Constitucional alemão, que, sem qualquer dúvida, colocou na vitrine o direito à autodeterminação informacional, alguns autores¹⁴ apontam a origem do conceito ainda antes da decisão alemã. É o caso do professor José Piñar Mañas, que aponta:

¹⁰ MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). **Lei Geral de Proteção de Dados: aspectos relevantes**. Indaiatuba: Foco, 2021. p. 13-22. p. 16.

¹¹ DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.); BIONI, Bruno (coord. Executivo). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 3-20. p. 9.

¹² MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. p. 2. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 18 jun. 2021.

¹³ SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES; DONEDA; SARLET; RODRIGUES JÚNIOR, BIONI, *op. cit.*, p. 21-59.

¹⁴ Veridiana Alimonti destaca que a ideia de autodeterminação já estava presente na obra de Alan Westin, *Privacy and Freedom*, de 1967, bem como em outras iniciativas normativas norte-americanas e europeias. ALIMONTI, Veridiana. Autodeterminação informacional na LGPD: antecedentes, influências e desafios. *In*: VILLAS BÔAS CUEVA, Ricardo; DONEDA, Danilo; MENDES, Laura Schertel (org.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020. p. 177-192.

[...] no debe olvidarse que ya en 1973 el Departamento de Salud, Educación y Bienestar de Estados Unidos elaboró un Informe sobre las bases de datos telemáticas del Gobierno y propuso un Código de buenas prácticas que recogería los principios que habrían de regir el uso de información por parte del Gobierno (*Fair Information Practices* o *Fair Information Principles*): no deben existir bases de datos secretas, se ha de reconocer el derecho de acceso y rectificación de los datos personales, ha de respetarse el principio de finalidad, debe respetarse el principio de calidad y han de adoptarse medidas de seguridad. Un año más tarde, y en base a tal Informe, se aprueba la *Privacy Act* de Estados Unidos, y van poniéndose las bases de los principios esenciales configuradores del núcleo esencial del derecho a la privacidad. Como se ha señalado, de los *privacy principles* se pasa a las *privacy laws*.¹⁵

É verdade que, já em 1967, na clássica obra *Privacy and Freedom*, Alan Westin¹⁶ advertia que, para manter a privacidade na era moderna, o indivíduo precisava ter a possibilidade de definir quando, como e quais informações pessoais poderiam ser comunicadas a terceiros.

De fato, a evolução tecnológica possibilitou um armazenamento e fluxo massivo de dados pessoais que, graças a algoritmos cada vez mais eficientes, são interpretados para as mais diversas finalidades, como fornecimento de padrões comportamentais e estatísticos, transformando os dados pessoais em bens de elevado valor para o mercado.

Sem dúvida, a coleta e o intercâmbio de dados pessoais aumentaram de maneira exponencial nas últimas décadas, “[...] e o progresso qualitativo na organização das informações impactou significativamente as liberdades individuais”¹⁷. A tecnologia permite que, tanto as empresas privadas como as autoridades públicas, utilizem essas informações para realizarem suas atividades, em uma escala sem precedentes. O próprio Tribunal Constitucional destacou que não há tratamento de dados que não possa, ao fim e ao cabo, levar ao comprometimento da esfera íntima¹⁸.

¹⁵ MURILLO DE LA CUEVA, Pablo Lucas; PIÑAR MAÑAS, José Luis. **El derecho a la autodeterminación informativa**. Fundación Colóquio Jurídico Europeo. Madrid: J. San José S.A, 2009. p. 85.

¹⁶ WESTIN, Alan F. Science, privacy and freedom: issues and proposals for the 1970's. Part I – The current impact of surveillance on privacy. **Columbia Law Review**, n. 6, v. 66, jun. 1966. Disponível em: https://www.jstor.org/stable/1120997?seq=1&cid=pdfreference#references_tab_contents. Acesso em: 29 mar. 2022.

¹⁷ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 98.

¹⁸ Conforme a conhecida frase que constou na decisão original: “[...] *gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‘belangloses’ Datum mehr*” (Volkszählungsurteil, p. 48. Em tradução livre: Sob as condições do tratamento automatizado de dados, não existem mais dados triviais. BUNDESVERFASSUNGSGERICHT. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em 02 jun. 2022.

O processamento de dados configura potencial ameaça à personalidade do indivíduo e à sua dignidade, na medida em que a combinação dos diversos dados armazenados possui o potencial de formar um retrato completo da pessoa sem a sua participação ou conhecimento¹⁹.

Daniel Solove explica que a depreensão de informações novas a partir de informações previamente adquiridas cria o que ele chama de problema de “combinação”.

Um pedaço de informação aqui e ali não diz muito, mas quando combinados, fragmentos e porções de dados iniciam a formação de um retrato de uma pessoa. O todo torna-se maior do que as partes. Isso ocorre porque a combinação de informações cria sinergias. Quando analisadas, informações combinadas podem revelar novos fatos sobre a pessoa, os quais essa não esperava que fossem sabidos sobre ela quando os dados originais, isolados, foram coletados.²⁰ (Tradução nossa).

A decisão alemã confirmou que a coleta e o uso de dados pessoais têm dimensão potencialmente ameaçadora, porque pode ser usada para esquematizar o comportamento do indivíduo sem que o mesmo tenha domínio sobre o processo. E aqui já se alerta para um dos problemas que adiante será enfrentado: são dados derivados de informações que nem sempre o indivíduo sabe como foram coletados, como serão processados e usados no futuro.

Essa evidente assimetria entre as partes leva à fragilidade do titular dos dados, que não tem qualquer condição de gerenciar sobre a interpretação e utilização das informações que terceiro detém sobre ele.

Nesse sentido, o direito à autodeterminação informativa guarda em si a ideia de que o indivíduo deve ter a liberdade de desenvolver sua personalidade, ser livre para revelar suas informações e fazer as suas escolhas. Diante disso, o tribunal decidiu que o direito da personalidade também subsume o direito do indivíduo de decidir como e em que limites questões pessoais da vida serão tornadas públicas, de

¹⁹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 31.

²⁰ No original: “A piece of information here or there is not very telling, but when combined, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected”. SOLOVE, Daniel J. **Understanding privacy**. Cambridge: Harvard University Press, 2009. p. 118.

modo a evitar que seja manipulado por informações que os seus interlocutores tenham sobre a sua pessoa.

Fabiano Menke²¹ defende, inclusive, que a autodeterminação informacional, por ser elemento estrutural de comunicação na sociedade, deva ser exercida livremente, pois, do contrário, haverá retração dos indivíduos, inviabilizando a própria comunicação democrática.

Essa substancial mudança nas relações humanas, oriunda do contexto da sociedade de dados, exige, para o livre desenvolvimento da personalidade, a proteção do indivíduo da descontrolada coleta, armazenamento e transferência de dados pessoais, pois disso também depende a preservação da dignidade da pessoa humana.

A autodeterminação informacional pode ser compreendida, portanto, como um direito fundamental²², que garante ao indivíduo o poder de decidir sobre a divulgação e utilização de seus dados pessoais.

A importância da autodeterminação informacional foi reconhecida no ordenamento jurídico brasileiro, que adotou o instituto como um de seus fundamentos, nos termos do artigo 2º, II, da Lei n.º 13.709/2018.

A lei brasileira inspirou-se fortemente no modelo europeu de proteção de dados, que, a partir da Carta dos Direitos Fundamentais da União Europeia²³, o reconheceu como um direito fundamental autônomo²⁴, por possuir intrínseca relação

²¹ MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2014. p. 205-230. p. 212.

²² “Direitos Fundamentais são, portanto, todas aquelas disposições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo, foram, por seu conteúdo e importância (fundamentalidade em sentido material), integradas ao texto da Constituição e, portanto, retiradas da esfera de disponibilidade dos poderes constituídos (fundamentalidade formal), bem como as que, por seu conteúdo e significado, possam lhe ser equiparadas, agregando-se à Constituição material, tendo, ou não, assento na Constituição formal (aqui considerada a abertura material do Catálogo).” SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2009. p. 77.

²³ Artigo 8º. Protecção de dados pessoais. 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 2000/C 364/01. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 19 nov. 2020.

²⁴ Percebe-se, ademais, que a proteção de dados, muito embora herdeira da tutela da privacidade, é mais ampla que essa e apresenta características próprias. Por isso, deve ser reconhecida como um

com a proteção da dignidade da pessoa humana, dos direitos da personalidade e da privacidade²⁵.

Embora, em momento posterior à edição da LGPD, o direito à proteção de dados também tenha sido reconhecido como direito fundamental pela Emenda Constitucional 115, de fevereiro de 2022, e passado a constar no inciso LXXIX do artigo 5º da Constituição, rol dos direitos e garantias fundamentais, esse incremento na proteção da privacidade agregou a esfera individual de direitos de personalidade em relação ao uso automatizado de informações de ordem pessoal, alcançando ao titular de dados o poder de disposição sobre o uso e tratamento desses.

Antes mesmo de o direito à proteção de dados ganhar reforço constitucional, Bruno Bioni defendia que:

O direito à proteção dos dados pessoais deve ser alocado como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. Caso contrário, corre-se o risco de ele não se desprender das amarras conceituais e da dinâmica do direito à privacidade e, em última análise, inviabilizar uma normatização própria para regular o fluxo informacional como fator promocional da pessoa humana.²⁶

Um dos elementos característicos dos regimes de proteção de dados pessoais é o reforço do controle do indivíduo em relação aos seus próprios dados pessoais, ou seja, a centralidade do direito à autodeterminação informativa, delineada a partir do direito geral de personalidade, impõe que a atividade de processamento de dados deve ter limites, exigindo um cenário de proteção contra o consentimento meramente aparente (fictício), a coleta de dados, além do mínimo necessário e obstáculos ao uso dos dados para fins diversos dos autorizados.

direito autônomo. DONEDA, Danilo. A proteção de dados como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

²⁵ A proteção de dados, segundo Regina Ruaro, Daniel Rodriguez e Brunize Finger, para além da defesa da privacidade, protege e regula o direito de acesso e o poder de controle das informações pessoais. RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito** (UFPR), Curitiba, v. 53, p. 45-66, 2012. p. 64.

²⁶ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 96.

1.2 O CONSENTIMENTO COMO INSTRUMENTO DE EFETIVAÇÃO DA AUTODETERMINAÇÃO INFORMATIVA

Diante da utilização maciça de tecnologias disruptivas, que se valem de algoritmos e inteligência artificial para formular perfis e diagnosticar comportamentos, o que evidencia a fragilidade do titular dos dados no cenário de hiperconectividade em que vivemos, Finn Brunston e Helen Nissenbaum destacam que:

Aqueles que sabem sobre nós têm poder sobre nós. Eles podem nos negar emprego, privar-nos de crédito, restringir nossos movimentos, recusar-nos abrigo, associação ou educação, manipular nosso pensamento, suprimir nossa autonomia e limitar nosso acesso a uma vida digna²⁷. (Tradução nossa).

Conforme observado nos parágrafos anteriores, a partir do reconhecimento de que o tratamento de dados oferece risco potencial aos direitos da personalidade e à dignidade do indivíduo e da centralidade do direito à autodeterminação informacional, é importante refletir sobre a aptidão do consentimento, como instrumento jurídico de concretização do direito do titular de manter o controle sobre seus dados.

Bruno Bioni²⁸ fez boa digressão sobre as gerações de leis sobre proteção de dados, explicando que, a partir do entendimento da máquina administrativa de que os dados da população seriam úteis para coordenar e planejar as ações estatais (*primeira geração*), evoluiu-se para a preocupação com as bases de dados na esfera privada, transferindo-se para o próprio titular dos dados a responsabilidade de protegê-los (*segunda geração*). A partir da *terceira geração* de leis, ampliou-se o protagonismo do titular dos dados, garantido a participação do indivíduo sobre todos os movimentos dos seus dados pessoais, da coleta ao compartilhamento, num reflexo perfeito da autodeterminação informacional.

Contudo, e ainda segundo Bruno Bioni²⁹, esse protagonismo do indivíduo no gerenciamento de seus dados carrega consigo diversos complicadores, porque, verdadeiramente, nem sempre há poder de escolha na sua divulgação. Eis, então, a *quarta geração* de leis protetivas de dados, que ambiciona corrigir as deficiências das

²⁷ BRUNTON, Finn e NISSENBAUM, Helen. **The Fantasy of Opting Out**. Disponível em: <https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/>. Acesso em: 02 jun. 2021.

²⁸ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 113-115.

²⁹ *Ibid.*, p. 116.

anteriores, com normas que não deixam exclusivamente ao indivíduo a escolha sobre o processamento de certos tipos de dados pessoais, relativizando a centralidade do consentimento.

Ao mesmo tempo, contudo, esse progresso geracional não eliminou o protagonismo do consentimento. A sua centralidade permaneceu sendo o traço marcante da abordagem regulatória. Tanto é verdade que, em meio a esse processo evolutivo, o consentimento passou a ser adjetivado, como devendo ser livre, informado, inequívoco, explícito e/ou específico, tal como ocorreu no direito comunitário europeu. Essa distribuição de qualificadores acaba, portanto, por desenhar um movimento refratário em torno do papel de destaque do consentimento quase como sendo sinônimo de autodeterminação informacional.³⁰

A evolução normativa, embora tenha reformulado a dimensão do consentimento, de forma alguma lhe retirou o papel de principal instrumento de efetivação da autodeterminação informacional como alicerce das normas a respeito da proteção de dados pessoais. Esse direito implica o controle do indivíduo dos seus dados pessoais antes da coleta desses (consentimento), e depois, pelo direito de revogação do consentimento, retificação e apagamento de dados, passando, também, pelo direito de transparência. Assim, conforme Angel Lalana e José Felix Soros: *“El consentimiento es, así, una de las vías principales que la legislación utiliza para proporcionar a todo individuo un control razonablemente amplio sobre su información”*³¹.

O desenvolvimento da disciplina de proteção de dados, principalmente a partir da proteção à autodeterminação informacional, evidencia o risco potencial aos direitos da personalidade e à dignidade da pessoa humana, conforme já se disse anteriormente, sempre que se estiver diante de uma situação que enseje o tratamento de dados. Dessa afirmação decorre uma exigência legal, qual seja, para que o tratamento de dados não seja considerado uma invasão à privacidade do indivíduo é preciso um fundamento de legitimação para sua ocorrência. Esse fundamento de legitimação é o consentimento ou uma prescrição legal, sob pena de o tratamento ser ilícito.

³⁰ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 117.

³¹ LALANA, Angel Daniel; SORO, José Felix Muñoz. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. In: VALERO TORRIJOS, Julian. **La protección de datos personales en internet ante la innovación tecnológica**. Riesgos, amenazas y respuestas desde la perspectiva jurídica. Navarra: Aranzadi, 2013. p. 153-196. p. 154.

No âmbito do regulamento europeu (GDPR/2016/679)³², são seis as situações que legitimam o tratamento de dados, e estão descritas nas alíneas de “a” a “f” do artigo 6º³³. Nos termos do RGPD o tratamento de dados poderá ocorrer se houver o consentimento para o tratamento de dados pessoais para uma ou mais finalidades específicas, a necessidade de tratamento para a execução de um contrato no qual o titular dos dados é parte, para o cumprimento de uma obrigação jurídica, para a defesa de interesses vitais do titular dos dados ou de outra pessoa, no exercício de funções de interesse público, ou com base no legítimo interesse do responsável pelo tratamento dos dados.

No Brasil, o artigo 7º da Lei n.º 13.709/2018 elenca dez hipóteses para a legitimação do tratamento de dados, fazendo constar o consentimento também como a primeira delas. A segunda hipótese é quando o tratamento é necessário ao cumprimento de obrigação legal ou regulatória do controlador³⁴. A terceira é o tratamento pela administração pública para a finalidade de execução de políticas públicas. A quarta é o tratamento para fins de pesquisas, pugnando pela anonimização dos dados sempre que possível. A quinta é quando o tratamento for necessário à execução de contrato ou aos procedimentos preliminares relacionados quando o titular dos dados for parte. A sexta possibilidade é para o exercício regular de direitos em processo, seja judicial, administrativo ou arbitral. A sétima e oitava

³² UNIÃO EUROPEIA. Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

³³ RGPD – Artigo 6º - Licitude do tratamento: 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos perseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

³⁴ Nesse sentido, deve-se ter em mente que o Marco Civil da Internet (Lei n.º 11.965/2014) criou obrigações aos provedores de conexão e de aplicação da internet, de modo que esses têm o dever de manter, respectivamente, os registros de conexão (artigo 13) e os registros de acesso a aplicações na internet (artigo 339), pelos prazos respectivos de um ano e de seis meses.

hipóteses são aquelas em que o tratamento de dados é realizado para a proteção da vida, integridade física do titular ou mesmo para a tutela da sua saúde.

Entre todas as hipóteses de legitimação do tratamento de dados, o consentimento é a única na qual a manifestação da vontade do indivíduo é determinante. É essa manifestação de vontade que garante ao titular dos dados o livre desenvolvimento da personalidade e o exercício da autodeterminação informacional, na sociedade informatizada na qual está inserido. É por meio do consentimento que o titular revela o direito de determinar se, e de que forma, seus dados pessoais serão tratados.

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações.³⁵

Laura Mendes³⁶ afirma que o consentimento é o instituto jurídico por meio do qual o indivíduo expressa a sua vontade de autorizar ou não o processamento de seus dados pessoais.

Danilo Doneda explica a estreita relação entre o consentimento e a autodeterminação informativa:

O consentimento é o instrumento por excelência dessa autodeterminação e, portanto, de um aspecto da tutela da pessoa. Em outro plano, porém, o consentimento representa o papel de instrumento de legitimação para que esses dados sejam, em alguma medida, utilizados por outra pessoa.³⁷

Bruno Bioni ressalta a posição de destaque do consentimento na proteção de dados e refere-se a ele como sendo uma “carta coringa regulatória”³⁸, o que, para

³⁵ TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 281-318. p. 293.

³⁶ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 60.

³⁷ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 302.

³⁸ BIONI, Bruno Ricardo. **Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPai/USP, 2015. Disponível em: https://www.researchgate.net/publication/328266374_Xequemate_o_tripé_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 31 mar. 2022.

Stefano Rodotà, seria “[...] uma saída fácil frente à complexidade de estabelecimento de um sistema completo de autorizações e proibições para regular o tratamento dos dados pessoais”³⁹.

O consentimento, então, configura-se como a forma de autorizar, legitimar as técnicas de processamento e dar algum poder de controle ao cidadão, de forma que ele não seja um mero “fornecedor de dados”⁴⁰. E, dessa forma, ele é elemento central ao longo da evolução da proteção de dados pessoais, ao ponto de essa proteção ser equiparada “[...] ao direito de o cidadão autogerenciar as suas informações pessoais”⁴¹.

Daí a importância da análise do papel do consentimento na proteção dos dados pessoais e dos esforços que se tem feito para buscar garantir que esse corresponda de fato à legítima vontade do indivíduo.

1.3 A NATUREZA JURÍDICA DO CONSENTIMENTO

“O consentimento é um típico elemento do direito contratual”, por meio do qual “[...] os indivíduos exprimem sua vontade de contratar, dando ciência uma à outra da sua intenção negocial para que seja selado um compromisso entre elas”⁴².

No âmbito da disciplina da proteção de dados, no entanto, a identificação da natureza jurídica do consentimento é um assunto que gera debates e não possui unanimidade. Danilo Doneda afirma que:

A qualificação jurídica do consentimento para o tratamento de dados pessoais não deve ser tomada como um mero enquadramento da sua disciplina em um esquema preconcebido, pelo qual o tratamento de dados deva submeter-se aos cânones de uma determinada concepção da autonomia privada. A especificidade do consentimento para o tratamento de dados pessoais pede uma funcionalização de sua própria natureza jurídica, e ao intérprete cabe integrar esta disciplina do consentimento com os efeitos que dela são pretendidos.⁴³

³⁹ RODOTÀ, Stefano. **A vida na sociedade da vigilância**. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 76.

⁴⁰ *Ibid.*, p. 76.

⁴¹ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 116.

⁴² GOMES, Orlando. **Contratos**. 26. ed. 2. tiragem. Rio de Janeiro: Forense, 2008 *apud* BIONI, Bruno Ricardo. **Xeque-mate**, *op. cit.*

⁴³ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 301.

Nesse sentido, o consentimento aproxima-se mais da área do direito da personalidade do que efetivamente de uma estrutura contratual, em que pese ter direta vinculação com essa última⁴⁴. Assim, o consentimento poderia ser analisado sob duas dimensões ou óticas, quais sejam: a) o consentimento como instrumento por excelência para a autodeterminação informacional e, portanto, um aspecto relacionado à tutela pessoal; e b) o consentimento como instrumento de legitimação para que os dados pessoais sejam parcialmente tratados por terceiros⁴⁵.

A não consideração do consentimento como o negócio jurídico justifica-se, “[...] já que essa opção reforçaria o sinalagma entre o consentimento para o tratamento dos dados pessoais e uma determinada vantagem obtida por aquele que consente, reforçando a índole contratual desse fenômeno”⁴⁶.

Segundo Laura Mendes⁴⁷, na doutrina alemã, onde são avançados os debates sobre a proteção de dados, três enquadramentos são defendidos para identificar a natureza jurídica do consentimento: (i) declaração de vontade negocial (*rechtsgeschäftliche Erklärung*), (ii) ato jurídico unilateral sem natureza negocial (*Realhandlung/Realakt*), e (iii) ato que se assemelha ao negócio jurídico, sem o ser (*geschäftsähnliche Handlung*).

A primeira corrente, do consentimento como uma declaração de vontade negocial, encara o ato de consentir como se fosse uma declaração de vontade em um negócio jurídico. O efeito jurídico da declaração é um reflexo do que queriam as partes, da sua vontade, de modo que são necessários todos os requisitos ao negócio jurídico e aplicáveis todos os dispositivos concernentes aos vícios da vontade⁴⁸.

A ideia do consentimento como um ato jurídico unilateral sem natureza negocial, ou ato real (*Realakt*)⁴⁹, é sustentada pelo entendimento de que o

⁴⁴ RÍSPOLI, Afonso Fratti Penna; QUADRADO, Hebert Fabricio Tortorelli. Fluxo informacional e autodeterminação informativa: o dilema do consentimento informado. In: LIMA, Cíntia Rosa Pereira (coord.). **ANPD e LGPD: desafios e perspectivas**. São Paulo: Almedina, 2021. p. 331-347.

⁴⁵ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 302.

⁴⁶ *Ibid.*, p. 303.

⁴⁷ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 62.

⁴⁸ RADLANSKI, Philip. Das Konzept der Einwilligung in der datenschutzrechtlichen Realität. Mohr Siebeck: Tübingen, 2016, p. 121 *apud* MANTOVANI, Alexandre Casanova. **O consentimento na disciplina da proteção dos dados pessoais: uma análise dos seus fundamentos e elementos**. 2019. 171 f. Dissertação (Mestrado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019. p.118.

⁴⁹ *Ibid.*

consentimento que legitima o tratamento de dados é um mero processo que resulta em um suporte fático independente da vontade das partes.

Por sua vez, a concepção do consentimento como um ato semelhante ao negocial (*geschäftsähnliche Handlung*)⁵⁰ faz uma espécie de meio termo. Por compreender o consentimento na proteção de dados como uma declaração de vontade que se relaciona com ato material/ato real (*tatsächliche Handlung*) – o processamento de dados –, qualifica-se o ato de consentir como jurídico, semelhante a um ato negocial. Trata-se de um suporte fático composto por pelo menos uma vontade exteriorizada a um resultado fático que, sozinho ou em conjunto com outros suportes fáticos, atinge uma consequência jurídica.

Nas palavras de Wolfhard Kohte, a categorização como manifestação de vontade negocial não seria suficiente, pois:

Em geral, o consentimento individual é indispensável, mas às vezes não é suficiente. Se a situação não for suficientemente clara/transparente/compreensível, ele [o titular dos dados] não pode decidir livremente, seja por inferioridade econômica, seja pessoal, ou a invasão/interferência é especialmente significativa ou perigosa, de modo que seu direito de autodeterminação deve ser assegurado através de procedimentos adicionais e critérios fáticos.⁵¹ (Tradução nossa).

Reconhecidas as características negociais do consentimento e sua intrínseca ligação com os direitos da personalidade, a doutrina defende que o consentimento para o tratamento de dados pessoais possui uma natureza “atípica”⁵² e que o ideal seria uma análise caso a caso para a avaliação da aplicabilidade das regras vigentes para os negócios jurídicos, pois ambos visam à autodeterminação da pessoa⁵³.

No direito pátrio, da estrutura do artigo 5º da LGPD se infere que dado pessoal é qualquer informação relativa à pessoa natural identificada ou identificável. Diante disso, a concessão de seu uso está condicionada ao consentimento, que é a

⁵⁰ ROßNAGEL, Alexander. Handbuch Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung. München: Verlag C. H. Beck, 2003. p. 686-687 *apud* MANTOVANI, *op. cit.*, p. 120.

⁵¹ KOHTE, Wolfhard. Die Rechtfertigende Einwilligung. **Archiv für Zivilistische praxis**, v. 185, n. 2, 1985. p. 155 *apud* MANTOVANI, Alexandre Casanova. **O consentimento na disciplina da proteção dos dados pessoais: uma análise dos seus fundamentos e elementos**. 2019. 171 f. Dissertação (Mestrado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019.

⁵² MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 63.

⁵³ KOHTE, *op. cit.*, p. 155 *apud* MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 63.

manifestação livre, informada e inequívoca pela qual o titular concorda como o tratamento de seus dados pessoais para uma finalidade determinada.

Fica evidente, portanto, a relevância do controle de gestão do consentimento, como base de legitimação para a coleta e tratamento de dados no ambiente virtual e, por isso, a importância de se indagar qual é a natureza jurídica do consentimento, nos termos da LGPD, especialmente para se avaliar o alcance da vontade expressa pelo titular de dados, seus efeitos e validade.

Para tanto, utilizar-se-á a classificação dos fatos jurídicos entre as espécies de fatos jurídicos lícitos e ilícitos, e, nesse prisma, o consentimento é espécie de fato jurídico lícito, conquanto previsto expressamente na legislação brasileira. Logo, interessam as diversas modalidades de fatos lícitos, a saber: (i) ato-fato jurídico e (ii) ato jurídico *lato sensu* e suas subespécies: ato jurídico *stricto sensu* e negócio jurídico.

O ato-fato jurídico deriva de uma situação de fato, a qual é resultante de uma conduta humana, ou seja, da ação (voluntária ou involuntária) ou da omissão, como exemplo, a caça, a pesca, a prescrição e a decadência, entre outras hipóteses; como a conduta que está à base da ocorrência do fato é da substância do fato jurídico, a norma jurídica que a recebe é a volitiva, abstraindo dele qualquer elemento volitivo que, porventura, possa existir em sua origem⁵⁴. Paulo Lôbo explica que “[...] são atos ou comportamentos humanos em que não houve vontade, ou, se houve, o direito a abstraiu”⁵⁵.

O ato jurídico *lato sensu* é o fato jurídico em cujo suporte fático haja manifestação humana consciente para a obtenção da finalidade lícita. O ato jurídico *lato sensu* possui duas subespécies: ato jurídico *stricto sensu* e o negócio jurídico, ambas caracterizadas pela existência de conduta humana volitiva, ou seja, constituem-se em atos de vontade dirigidos a um fim específico; a forma de manifestação de vontade ocorre de forma consciente em busca de um fim definido.

A declaração de vontade no ato jurídico *stricto sensu* constitui um “[...] comportamento humano deflagrador de efeitos previamente estabelecidos por lei”⁵⁶. Existe, nele, a manifestação de vontade, mas falta o poder de autorregramento⁵⁷. O

⁵⁴ MELLO, Bernardes de. **Teoria do fato jurídico**: plano da existência. 22. ed. São Paulo: Saraiva, 2019. p. 198.

⁵⁵ LÔBO, Paulo Luiz Netto. **Direito civil** – parte geral. 6. ed. São Paulo: Saraiva, 2017. p. 247.

⁵⁶ GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**: parte geral. São Paulo: Saraiva, 2002. p. 307.

⁵⁷ MELLO, *op. cit.*, p. 131.

querer é condicionado pela norma legal, que exige sua prática e predetermina seus efeitos. A vontade não goza de autonomia para estruturar o ato jurídico; ela é apenas condição de atuação do regramento legal⁵⁸.

No ato jurídico *stricto sensu* a liberdade existe apenas quanto à vontade ou não de praticar o ato, mas não se pode estabelecer os efeitos que dele se pretendem, pois são *ex lege*. Por outro lado, no negócio jurídico se vislumbra a liberdade de celebração e de estipulação, vale dizer, o indivíduo pode modular os efeitos que espera da declaração de vontade.⁵⁹

O que distingue o ato jurídico *stricto sensu* do negócio jurídico é que, no primeiro, o poder de escolha da categoria jurídica é quase inexistente, enquanto no negócio jurídico há maior fluidez no exercício da autonomia privada. O negócio jurídico consiste em manifestação ou declaração de vontade, na qual o ordenamento jurídico, respeitando certos limites predeterminados, faculta às pessoas “[...] o poder de escolha de categorias jurídicas e de estruturação de conteúdo eficaz das relações jurídicas respectivas, quanto ao seu surgimento, permanência e intensidade no mundo jurídico”⁶⁰.

Pode-se dizer que o consentimento para a divulgação de dados pessoais é exercício de direito autônomo⁶¹, tratando-se de um direito potestativo, que, segundo Orlando Gomes, “[...] é a faculdade de agir do titular que não se relaciona a uma pretensão de outrem”⁶².

Enquadrar o consentimento na categoria do ato jurídico *stricto sensu* não parece ser a melhor opção, porque os efeitos jurídicos desses atos são prefixados pela norma invariável, não se admitindo a composição de seu conteúdo de acordo com os interesses tutelados⁶³. Por outro lado, o consentimento para o uso e tratamento de dados pessoais pode ser modulado de acordo com a finalidade para o qual foi concedido, ensejando outras situações ou negócios jurídicos derivados, de

⁵⁸ THEODORO JÚNIOR, Humberto; FIGUEIREDO, Helena Lanna. **Negócio jurídico**. Rio de Janeiro: Forense, 2021. p. 08.

⁵⁹ *Ibid.*, p. 09.

⁶⁰ MELLO, Bernardes de. **Teoria do fato jurídico**: plano da existência. 22. ed. São Paulo: Saraiva, 2019. p. 230.

⁶¹ DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados: ensaio à luz da teoria do fato jurídico. *In*: EHRHARDT JÚNIOR, Marco; CATALAN, Marcos; MALHEIROS, Pablo. **Direito civil e tecnologia**. Belo Horizonte: Fórum, 2020. p. 69-88.

⁶² GOMES, Orlando. **Introdução ao direito civil**. 20. ed. Rio de Janeiro: Forense, 2010. p. 91.

⁶³ DANTAS; COSTA, *op. cit.*

caráter patrimonial ou não; autorizando, assim, a afirmação de que a sua natureza jurídica está muito próxima do negócio jurídico.

Laura Mendes afirma que esse último posicionamento é atualmente o dominante e lhe parece também ser o mais correto.

Afinal, resta nítida a natureza atípica do consentimento para o processamento de dados, que tem características negociais, ao mesmo tempo em que possui também um caráter personalíssimo. Por isso, segundo Kothe, é preciso fazer uma análise caso a caso para se decidir quais são as normas aplicáveis. De acordo com ele, a função do consentimento para o tratamento de dados pessoais é a mesma da declaração de vontade no âmbito de um negócio jurídico, pois ambos visam à autodeterminação da pessoa. Nesse sentido, é possível aplicar as regras referentes aos negócios jurídicos e contratos em geral a esse consentimento, sempre que essa aplicação se mostrar cabível e adequada.⁶⁴

Na realidade brasileira, portanto, entende-se que o consentimento pode ser enquadrado na categoria dos negócios jurídicos ou a eles associados. Corrobora esse entendimento também a característica de revogabilidade do negócio jurídico, porquanto também o consentimento pode ser revogado, nos termos do artigo 8º da Lei Geral de Proteção de Dados. Assim, o titular dos dados concede o seu uso para um fim previamente informado em relação ao qual está de acordo, sendo, contudo, permitida sua revogação.

Outrossim, do reconhecimento do direito à autodeterminação informacional decorre o direito de o titular dos dados determinar a extensão do tratamento desses, inclusive com a possibilidade de que o consentimento seja parcial, de modo que esse não pode ser reduzido a uma simples aceitação de uma consequência jurídica.

Nesse contexto, o consentimento, como instrumento da autodeterminação informativa, confere ao titular autonomia em relação aos seus dados. O consentimento é, portanto, a própria manifestação de vontade, a consciência do indivíduo em relação aos dados pessoais disponibilizados. Sendo uma manifestação de vontade qualificada, dirigida a um fim prévio e suficientemente esclarecido, o consentimento integra a categoria de ato jurídico *lato sensu*, enquadrando-se na subespécie de negócio jurídico, pois a esse conceito melhor se amolda.

Definida a natureza do consentimento, é preciso identificar quais os requisitos indispensáveis para que se constitua em manifestação genuína de vontade, apta a

⁶⁴ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 63.

amparar o tratamento de dados pessoais, num cenário de grande assimetria informacional ofertada pelo uso da informação em rede e da inteligência artificial.

Diante disso, na sequência deste estudo, analisar-se-ão os requisitos exigidos para que o consentimento se constitua, verdadeiramente, como manifestação de vontade livre, informada e inequívoca, nos termos do artigo 5º, XII, da LGPD.

1.4 REQUISITOS DO CONSENTIMENTO VÁLIDO

Um dos preceitos fundamentais da LGPD é que o tratamento de dados não pode ser realizado sem uma base normativa que o autorize, e, sendo o consentimento o suporte escolhido, ele deve estar dotado das características referidas na Lei para ser válido, sob pena de violação à legislação protetiva de dados.

Nesse sentido, o consentimento, como elemento de autorização do tratamento de dados, nos termos do artigo 5º, XII, deve ser livre, informado e inequívoco. Essas qualidades⁶⁵, exigidas para que se tenha um consentimento válido, são indispensáveis para garantir que a manifestação de vontade que autoriza o tratamento de dados signifique, de fato, o exercício da autodeterminação informativa, e não se constitua em mera ficção.

Historicamente, no direito privado brasileiro, a figura do consentimento sempre esteve incubada no tema dos defeitos do negócio jurídico. Do erro à lesão, o bem jurídico tutelado é justamente assegurar que a declaração de vontade da pessoa seja “livre e consciente”. A formação imperfeita desse elemento volitivo é considerada como “vício de consentimento”, sendo o negócio jurídico decorrente anulável.⁶⁶

As normas voltadas ao regramento do consentimento, sempre atreladas à ideia da autodeterminação informacional, facultam ao indivíduo não apenas autorizar o uso e tratamento de seus dados pessoais, mas, também, retificar, emendar, apagar e/ou completá-los. São normas que dão grande protagonismo ao titular dos dados

⁶⁵ Sobre as qualidades do consentimento no RGPD: Article 29 Working Party Guidelines on consent under Regulation 2016/679. EUROPEAN COMMISSION. **Article 29 Working Party Guidelines on consent under Regulation 2016/679**. 2017. p. 14. Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051/en>. Acesso em: 06 abr. 2022.

⁶⁶ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 179.

personais, ensejando a ideia de que um tratamento de dados justo e lícito⁶⁷ está vinculado a um consentimento válido e eficiente.

O consentimento do titular para o tratamento de seus dados pessoais é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; por meio dele, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão.⁶⁸

No ambiente digital, do qual não é possível fazer parte sem deixar rastros sobre as preferências, os interesses, as características e, até, sobre a forma de pensar dos indivíduos, a principal base de tratamento de dados é o consentimento. Esse consentimento, na imensa maioria das vezes, é facilitado por um simples *click*, diante de uma estrutura que oferece benefícios aos usuários, sem maiores informações, ou com informações ininteligíveis ou, ainda, condicionando o acesso àqueles conteúdos à aquiescência ao uso das informações fornecidas.

O confronto com situações reais revela que, em tais situações, a alternativa à não revelação dos dados pessoais pelo seu titular costuma ser uma – por vezes, brutal – renúncia a determinados bens ou serviços. A disparidade de meios e de poder entre a pessoa de quem é demandado o consentimento para utilização dos dados pessoais em contemplação da realização de um contrato e aquele que os pede faz com que a verdadeira opção que lhe reste seja, tantas vezes, a de “tudo ou nada”, “pegar ou largar”.⁶⁹

Portanto, a entrega de dados pessoais nas redes, a partir desse “aceite”, muitas vezes está longe de constituir uma “manifestação livre, informada e inequívoca” de vontade, tendo substancial impacto na privacidade de usuários, ainda que não tenham consciência disso. É nesse ponto, precisamente, que se investiga a base legal chamada de “consentimento” para o tratamento de dados, como expressão primeira da autodeterminação informativa.

Existem inúmeros exemplos de onde o consentimento é solicitado para o processamento de nossos dados; exemplos óbvios são uma solicitação para aceitar cookies quando visitamos um site, enviando dados para comprar qualquer coisa online, de produtos a serviços, preenchendo uma pesquisa online, usando mídia social, usando um sistema operacional de smartphone

⁶⁷ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 115.

⁶⁸ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 296-297.

⁶⁹ *Ibid.*, p. 298-299.

e muitos aplicativos de telefone celular. Essa lista não é exaustiva, mas oferece uma indicação da escala do problema enfrentado pelos processadores de dados e titulares dos dados. O desafio de cumprir a nova lei é desenvolver mecanismos para que todos esses pedidos de consentimento sejam claros, simples e não inconvenientes para o titular dos dados, uma das razões pelas quais muitas pessoas simplesmente marcam os termos e condições é que eles não possuem tempo para ler uma longa página de termos que muitas vezes está em linguagem densa e ininteligível para a maioria.⁷⁰ (Tradução nossa).

A autodeterminação informativa pressupõe exatamente isto: o fornecimento consciente de dados e a possibilidade de impedir que venham a ser utilizados de forma incorreta ou para fins diversos daqueles para os quais foram coletados⁷¹.

É certo que o consentimento válido compreende a existência das características referidas na LGPD, porquanto são elas que, ao menos neste momento histórico, qualificam a manifestação de vontade como expressão da autodeterminação informativa, a qual se reveste de fundamentalidade⁷². Dito de outra forma, a proteção da privacidade somente se concretiza quando existentes as condições para um consentimento efetivo⁷³.

Esse conjunto de características permite caracterizar esse consentimento, se o cotejarmos com a função que dele se pretende, qual seja a de ser um instrumento para a livre construção da esfera privada, “uma ficção”. Sua utilização pode ser instrumentalizada pelos interesses que pretendem que seja não mais que uma via para legitimar a inserção dos dados pessoais no mercado.⁷⁴

⁷⁰ “There are numerous examples of where consent is requested for processing our data, obvious examples are a request to accept cookies when we visit a website, submitting data to purchase anything online from goods to services, completing an online survey, using social media, using a smartphone OS and many mobile phone apps. This list is not exhaustive but offers an indication of the scale of the problem faced by data processors and Data Subjects. The challenge in complying to the new regulation is to develop mechanisms for all these requests for consent which are clear, simple and not inconvenient to the Data Subject, one of the reasons why many people simply tick boxes for terms and conditions is that they do not have time to read a long page of terms which is often in dense language unintelligible to most.” BREEN, Stephen; OUZZANE, Karim Ouazzane e PATEL, Preeti. GDPR: is your consent valid? **Business Information Review**, London: London Metropolitan University, v. 37, p. 19-24, 2020. p. 22. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0266382120903254>. Acesso em: 05 jun. 2021.

⁷¹ FACCHINI NETO, Eugênio e DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito**, n. IX, p. 119-140, 2º sem. 2019.

⁷² RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jun. 2015.

⁷³ COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52., p. 1373-1438, 2000. Disponível em: <https://scholarship.law.georgetown.edu/facpub/810>. Acesso em: 01 jun. 2021.

⁷⁴ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 300.

Bruno Bioni, refletindo sobre o processo de adjetivação do consentimento, pondera, com boa razão, que:

A multiplicidade de adjetivos atribuídos ao consentimento não detém outra finalidade senão a de apontar que deve haver um processo de tomada de decisão, o qual o titular do dado por si só é incapaz de atingir sem a cooperação da contraparte que processa seus dados. A partir dessa perspectiva obrigacional, emerge-se uma série de deveres para os agentes de tratamento de dados, em especial o controlador.⁷⁵

Apesar das dificuldades de se implementar a atual noção de consentimento válido, parece impositivo, nos termos da LGPD, que o agente de dados deve envidar todos os esforços de estrutura e prevenção para garantir que a manifestação de vontade seja livre, informada, inequívoca e para uma finalidade determinada, sob pena de violar a legislação protetiva de dados.

Considerando que a LGPD possui forte inspiração no Regulamento Geral de Proteção de Dados (RGPD), parece importante referir que também lá o consentimento recebe essas qualificadoras, nos termos do artigo 4.11:

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

Já nas considerações iniciais, o Regulamento Europeu determina as linhas pelas quais deve ser interpretado o consentimento, descrevendo-o como fruto de um “[...] ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular dos dados consente com o tratamento dos dados que lhe digam respeito”⁷⁶.

⁷⁵ BIONI, Bruno Ricardo. O consentimento como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 145-161. p. 152.

⁷⁶ Considerando 32 do RGPD: O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins

Traçadas essas considerações, cumpre a análise dos requisitos ou adjetivos que são verdadeiras condições *sine qua non* de validade do consentimento como base normativa apta a amparar o tratamento de dados pessoais.

1.4.1 Consentimento livre

O adjetivo “livre”⁷⁷ remete à ideia de liberdade de escolha, oportunidade de decisão, entre outras possíveis. Trata-se de uma ação espontânea⁷⁸, no sentido de o titular poder escolher entre aceitar ou recusar a utilização de seu dado, sem intervenções ou situações que viciem o seu consentimento⁷⁹. A possibilidade de escolha é que define se alguém é livre ou não.

O elemento “livre” implica uma escolha real e controle sobre a decisão para os titulares dos dados, ou seja, se o titular dos dados não tiver escolha real ou se sentir compelido a consentir sob pena de sofrer consequências negativas, o consentimento não será válido. Da mesma forma, o consentimento não será considerado livre se o titular dos dados for incapaz de retificar ou retirar o seu consentimento sem prejuízo.

Afirmar que a manifestação de vontade deve ser livre significa que o titular deve ter uma liberdade de escolha genuína. Nesse sentido, não se considera a manifestação de vontade livre se o titular não poderia se negar a consentir ou mesmo

múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

⁷⁷ O Considerando 43 do RGPD assim estabelece, sobre o consentimento livre: “*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*”. FREELY Given Consent. Recital 43. General Data Protection Regulation (GDPR). **Intersoft Consulting**, Disponível em: <https://gdpr-info.eu/recitals/no-43/>. Acesso em: 02 jun. 2021.

⁷⁸ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 185.

⁷⁹ TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 281-318. p. 294.

desistir do consentimento dado⁸⁰. Para que o exercício de escolha seja livre, o titular deve poder ver como alternativa a possibilidade de não consentir. Se não for viável recusar consentir com os termos, seja por “fraude, intimidação, coerção ou consequências significativamente negativas” em não consentir, não há uma verdadeira liberdade de consentimento.

O consentimento livremente dado significa que o titular dos dados deve poder escolher entre o consentimento ou a falta do mesmo, sem afetar sua relação com o controlador em áreas não cobertas pelo consentimento. O consentimento livre será dado por iniciativa própria, por uma pessoa em pleno estado mental de saúde e sem qualquer coação de natureza social, financeira, psicológica ou de outra natureza. Respectivamente, um consentimento não deve ser considerado dado livremente se o titular dos dados não tiver livre escolha e não puder recusar ou retirar o consentimento sem consequências adversas.⁸¹ (Tradução nossa).

Em termos gerais, qualquer elemento de pressão ou influência inadequada sobre o titular dos dados (que pode ocorrer de muitas formas) que o impeçam de exercer a sua vontade, tornará o consentimento inválido.

A LGPD faz referência ao consentimento livre; no entanto, não o conceitua, como o faz o Considerando 43 do RGPD:

A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do

⁸⁰ Considerando 42 do regulamento: “Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado”. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

⁸¹ “*Freely given means that the data subject must be able to choose between consent or lack thereof, without affecting its relationship with the controller in areas not covered by consent. Freely given consent shall be freely given on one's own initiative by a person in full mental health and without any coercion of a social, financial, psychological or other nature. Respectively, a consent should not be considered freely given if the data subject has no real or free choice and cannot refuse or withdraw consent without adverse consequences.*” TYBURSKA, Justyna. Criterion of legitimacy of consent for processing personal data in e-commerce. Disponível em: <https://czasopisma.uksw.edu.pl/index.php/cwc/article/view/6033>. Acesso em: 06 abr. 2022.

consentimento apesar de o consentimento não ser necessário para a mesma execução.⁸²

Mónica Vilasau Solana comenta sobre o consentimento no RGPD:

*El término libre implica elección y control por parte de los interesados. Por lo tanto, si el sujeto se siente obligado o compelido de algún modo, o bien puede sufrir consecuencias negativas si no proporciona el consentimiento, este no puede considerarse libre.*⁸³

Bruno Bioni sugere que, para a verificação de um consentimento livre é preciso “[...] investigar qual o nível de assimetria de poder em jogo”⁸⁴, porque o reconhecimento de submissão pode impedir que o consentimento seja livre. Nesse sentido, a noção de desequilíbrio entre o controlador e o titular dos dados deve ser levada em consideração para a verificação de adequação do consentimento.

Um exemplo de manifestação de vontade que não pode ser considerada livre é quando a relação é com o poder público, que, ou goza do monopólio da exploração de uma atividade, ou desempenha com exclusividade uma função pública da qual o indivíduo não pode prescindir (por exemplo, a expedição de documentos oficiais).

O conceito pode, no entanto, ser estendido a situações de eventuais monopólios/oligopólios, prestação de serviços essenciais (fornecimento de água, energia, telefonia, internet etc.), mesmo quando privatizada, relações de trabalho e quando há grande disparidade entre as partes⁸⁵, como em alguns casos no direito do consumidor⁸⁶.

⁸² UNIÃO EUROPEIA. Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

⁸³ SOLANA, Mónica Vilasau. Menores. Centros docentes y datos: decisiones conflictivas. *In*: MALLÉN, Beatriz Tomáz; MAHAMUT, Rosario Garcia; CHULVI, Cristina Pauner. **Las cláusulas específicas del Reglamento General de Protección de Datos en el Ordenameto Jurídico Español**. Valencia: Tirant lo Blanch, 2021. p. 179-212. p. 181.

⁸⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 185.

⁸⁵ Considerando 43: A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa [...]. UNIÃO EUROPEIA. *Op. cit.*

⁸⁶ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 65.

Na última parte do Considerando 43⁸⁷, destaca-se a referência de que o consentimento, para ser considerado livre, deve respeitar as interconexões vertical e horizontal. A necessidade de interconexão vertical também está expressa no item 4⁸⁸ do artigo 7º, do RGPD, e vincula a validade do consentimento à necessidade do tratamento de dados para a execução do contrato para o qual o consentimento foi requerido.

Por sua vez, a necessidade de interconexão horizontal cria a presunção legal de que o consentimento não é dado livremente se, ainda que apropriado⁸⁹, ele é geral, ou seja, se não é permitido um consentimento individual para as diferentes operações de tratamentos de dados.

1.4.2 Consentimento informado

Informado será o consentimento quando o titular dominar todos os elementos necessários para decidir sobre a autorização de utilização e tratamento de seus dados. A informação é pressuposto essencial para que haja qualquer tipo de processo de tomada de decisão por parte do titular dos dados⁹⁰.

A análise do consentimento informado deve ser estudada conjuntamente com o adjetivo específico; e, para a manifestação de vontade ser específica, “[...] ela deve ser inteligível, deve fazer uma clara e precisa referência ao escopo e às

⁸⁷ Considerando 43: Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

⁸⁸ RGPD - Artigo 7º. 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato. *Ibid.*

⁸⁹ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 185.

⁹⁰ *Ibid.*, p. 80.

consequências do processamento de dados [...], não pode ser aplicada a um rol aberto/indefinido de atividades de tratamento de dados”⁹¹.

As finalidades informadas ao titular dos dados quando esse consentir serão um limite ao tratamento de dados que será realizado. O responsável pelo tratamento se autolimita quando redige o termo de adesão que submeterá ao titular dos dados. O consentimento específico é o que dá anuência a um determinado tratamento de dados, de modo que, para o titular dos dados poder consentir, ele deve estar ciente, ser informado, de quais dos seus dados serão tratados e de que forma.

No RGPD, a informação é fundamental para que o consentimento seja considerado válido, assim determina o artigo 5.1.a, em conjunto com os artigos 12⁹², 13 e 14, e as exigências recaem sobre aspectos relacionados ao conteúdo e sobre a forma de fornecer a informação.

No Considerando 42, o regulamento determina que, para manifestação de vontade ser informada, o sujeito deve estar ciente da identidade do controlador e do propósito do tratamento de dados⁹³. Além disso, o titular dos dados deve ser informado também da possibilidade de revogar o consentimento, que é uma prerrogativa incondicionada e deve ser tão fácil de exercer quanto foi consentir⁹⁴.

⁹¹ “[t]o be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of data processing. It cannot apply to an open-ended set of processing activities” EUROPEAN COMMISSION. **Article 29 Working Party Guidelines on consent under Regulation 2016/679**. 2017. p. 14. Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051/en>. Acesso em: 06 abr. 2022.

⁹² Destaca-se o texto do artigo 12 do RGPD por sua precisão: Artigo 12. 1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13 e 14 e qualquer comunicação prevista nos artigos 15 a 22 e 34 a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

⁹³ Considerando 42: Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

⁹⁴ RGPD - Artigo 7º, 3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.

Nos termos do artigo 9º⁹⁵ da LGPD, o titular tem direito a informações claras, adequadas e ostensivas sobre a finalidade, forma e duração do tratamento, identificação do controlador, possibilidade do uso compartilhado dos dados, entre outras informações pertinentes para a tomada de decisão. Será considerado nulo o consentimento apoiado em conteúdo enganoso ou abusivo e que não tenha sido antecedido por informações adequadas.

A LGPD não prescreve a forma ou formato no qual as informações devem ser fornecidas a fim de cumprir o requisito do consentimento informado. Isso significa que informações podem ser apresentadas em várias formas, como declarações orais ou escritas, mensagens de áudio ou vídeo, entre outras. No entanto, a LGPD exige que os controladores usem linguagem clara e simples para informar o titular sobre o conteúdo e a dimensão do seu consentimento. Isso significa que o objeto da informação deve ser facilmente compreensível para a pessoa média. Se o agente de tratamento de dados não fornecer informações acessíveis, o controle do usuário se tornará ilusório e o consentimento será uma base inválida para o processamento.

1.4.3 Consentimento inequívoco e para uma finalidade determinada

A expressão “inequívoca” exige que a manifestação de vontade não seja ambígua, que não haja dúvidas sobre a intenção do titular em consentir. Essa característica do consentimento relaciona-se estritamente ao princípio da finalidade, que enuncia que a realização do tratamento de dados deverá se dar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de

⁹⁵ LGPD - Artigo 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 ao 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.

tratamento posterior de forma incompatível com essas finalidades. Ou seja, “[...] qualquer declaração de vontade deve ter um direcionamento, já que não se consente no vazio e de forma genérica”⁹⁶.

Consentimento inequívoco implica uma ação afirmativa clara, o que significa que o titular dos dados deve implementar uma ação deliberada para consentir aquele processamento. Silêncio ou inatividade por parte do titular dos dados, bem como apenas o prosseguimento de um serviço, não pode ser considerado como uma indicação ativa de escolha.

O RGPD deixa claro que o consentimento requer uma declaração do titular dos dados ou um ato afirmativo claro; o que significa que deve sempre ser dado através de uma moção ou declaração ativa. Deve ser óbvio que o titular dos dados consentiu com o processamento específico. O artigo 2(h) da Diretiva 95/46/EC descreveu o consentimento como uma “indicação de vontade pela qual o sujeito informa que concorda com o tratamento dos dados pessoais que lhe dizem respeito”. O artigo 4 (11) do RGPD se baseia nessa definição, esclarecendo que o consentimento válido requer uma indicação inequívoca por meio de declaração ou de ação afirmativa clara.⁹⁷ (Tradução nossa).

É inequívoco o consentimento quando o formulário através do qual o titular deu seu consentimento não pode deixar dúvidas da sua intenção de consentir. Se houver uma dúvida razoável da intenção do titular, haverá ambiguidade e a manifestação de vontade não pode ser considerada válida.

Um “ato afirmativo claro” significa que o titular dos dados deve ter tomado uma ação deliberada para consentir no tratamento específico. A consideração 32 do RGPD estabelece orientações adicionais sobre esse assunto; informa que o consentimento pode ser coletado por meio de declaração escrita ou oral (gravada), inclusive por meio

⁹⁶ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020. p. 186.

⁹⁷ “*The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing. Article 2(h) of Directive 95/46/EC described consent as an “indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed”. Article 4 (11) GDPR builds on this definition, by clarifying that valid consent requires an unambiguous indication by means of a statement or by a clear affirmative action.*” EUROPEAN COMMISSION. **Article 29 Working Party Guidelines on consent under Regulation 2016/679**. 2017. p. 14. Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051/en>. Acesso em: 06 abr. 2022.

eletrônico. Silêncio ou inatividade por parte do titular dos dados não pode ser considerado como uma indicação ativa de escolha⁹⁸.

Na lei brasileira, assim como no regulamento europeu, o ônus de comprovar que o consentimento foi obtido é do “controlador”⁹⁹, ou seja, de quem tratará os dados pessoais. Levando em consideração esse ônus – bem como a condição de que, se por escrito, deve ser dado por cláusula destacada –, ainda que o consentimento possa ser dado através de outro meio que demonstre a manifestação de vontade do titular (para além do escrito), entende-se que o sistema *opt-out*, condições pré-validadas e mesmo a omissão do titular não configuram o ato de consentir¹⁰⁰.

Desde o Marco Civil da Internet, Lei n.º 12.965/2014, o sistema adotado pelo ordenamento jurídico brasileiro é o do *opt-in*¹⁰¹, ou seja, o consentimento deve ser dado para que os dados sejam tratados. O sistema de *opt-out* – aquele no qual o titular dos dados tem o ônus de buscar os meios de retirar seus dados do tratamento, pois a concordância com o tratamento é automática – é incompatível com os fundamentos da proteção de dados e com os princípios atinentes à disciplina, pois enseja a existência de bancos de dados e mesmo tratamento desses sem que o titular tenha conhecimento, pois não optou por consentir¹⁰².

Além disso, a manifestação de vontade não pode se constituir em autorização genérica; deve, também, se referir a uma *finalidade determinada*. Nessa característica, que também representa um reflexo direto do princípio da finalidade, o

⁹⁸ Considerando 32: O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

⁹⁹ LGPD – Artigo 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. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

¹⁰⁰ LIMA, Marco Antonio; BARRETO JÚNIOR, Irineu Francisco. Marco civil de internet: limites da previsão legal de consentimento expresso e inequívoco como proteção jurídica dos dados pessoais na internet. **Revista de Direito**, Governança e Novas Tecnologias, Brasília, v. 1, n. 2, p. 241-260, jan./jun. 2016.

¹⁰¹ *Ibid.*

¹⁰² *Ibid.*

titular dos dados deve ter ciência do escopo perseguido pelo agente, ou seja, o objetivo da coleta e a utilização dos dados não devem se desconectar.

A definição de uma finalidade é o que permitirá analisar regressivamente se o cidadão foi adequadamente informado para iniciar um processo de tomada de uma decisão livre. Dito de outra forma, os adjetivos informado e livre são calibrados pela locução “finalidades determinadas”, ainda que sejam a ela antecedentes.¹⁰³

A manifestação de vontade deve possuir um direcionamento, não podendo se constituir em um “cheque em branco”, porque isso significaria o esvaziamento de qualquer esfera de controle do cidadão sobre seus dados¹⁰⁴.

Essa é a mesma exigência que consta no artigo 4.11 do RGPD, ao adjetivar o consentimento como específico, ou seja:

*[...] ello está estrechamente relacionado com el Principio de limitación de la finalidad: los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.*¹⁰⁵

¹⁰³ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 186.

¹⁰⁴ *Ibid.*, p. 190.

¹⁰⁵ SOLANA, Mònica Vilasau. Menores. Centros docentes y datos: decisiones conflictivas. *In*: MALLÉN, Beatriz Tomáz; MAHAMUT, Rosario Garcia; CHULVI, Cristina Pauner. **Las cláusulas específicas del Reglamento General de Protección de Datos en el Ordenameto Jurídico Español**. Valencia: Tirant lo Blanch, 2021. p. 179-212. p. 182.

2 A BOA-FÉ OBJETIVA COMO CLÁUSULA GERAL NAS RELAÇÕES REGIDAS PELA LGPD

A inserção da cláusula geral da boa-fé na Lei Geral de Proteção de Dados fortalece a sua necessidade de observância nas mais diversas relações jurídicas, não estando mais limitada ao direito privado e às relações meramente contratuais. Consiste na adoção de uma conduta correta, leal e honesta no agir em sociedade. Por meio de suas funções e deveres ético-jurídicos de conduta, imbuídos pela percepção de igualdade substancial nas relações, e, tendo por arcabouço os preceitos sociais preconizados pelo Estado Democrático de Direito, sua observância nas relações de tratamento de dados repercute especialmente na mitigação da assimetria informacional que permeia esse cenário.

Neste capítulo será delineado um breve histórico desse importante instituto jurídico e sua evolução no ordenamento jurídico brasileiro, para, ao fim, destacar sua modernidade e evolução conceitual, uma vez que reconhecida como cláusula geral na LGPD.

2.1 CONSIDERAÇÕES INICIAIS E BREVES NOTAS SOBRE A EVOLUÇÃO HISTÓRICA DA BOA-FÉ

A expressão “boa-fé” permeia o universo jurídico de modo multifacetado¹⁰⁶, aparecendo na legislação em diversas situações e com vários significados, nomeando fenômenos jurídicos distintos. Por vezes, externa sua acepção objetiva, como *standard* de conduta e regra de comportamento, e, em outras, apresenta sua acepção subjetiva, como crença ou estado de ignorância.

Embora a coincidência gramatical, as acepções da boa-fé são absolutamente diferentes em suas funções e aplicações jurídicas. Neste estudo, a boa-fé que interessa aprofundar e melhor compreender, no contexto da proteção de dados pessoais, é a boa-fé objetiva, embora a boa-fé subjetiva deva ser mencionada ao longo do trabalho, porque é indispensável sua referência na explanação histórica do instituto e nas pontuais necessidades de distinção entre elas.

¹⁰⁶ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 41.

As reflexões que se farão, a partir do *caput* do artigo 6º da Lei Geral de Proteção de Dados, tomam por base o agir segundo a boa-fé objetiva, concretizando as exigências de probidade, correção e comportamento leal hábeis a viabilizar um adequado tráfico negocial¹⁰⁷, consideradas as relações em análise.

Os principais fundamentos da noção de boa-fé encontram suas raízes históricas no Direito Romano, no qual a chamada *fides*¹⁰⁸ constituía um conceito de confiança associado ao cumprimento dos pactos celebrados e a ética na execução das convenções assumidas.

Segundo Judith Martins-Costa:

Expressão polissêmica, a *fides* será entendida, amplamente, como confiança, mas, igualmente, como colaboração e auxílio mútuo (na relação entre iguais) e como amparo ou proteção (na relação entre desiguais); como lealdade e respeito à palavra dada; como fundamento da justiça e da virtude cívica; como o liame que une entre si os membros da *societas inter ipsos*, e, ainda, como instrumento técnico-jurídico, seja por meio de exceções, seja, de modo especial por via dos *iudicia ex fide bona*, sua vigência se manifestando “de maneira fluida e elástica em todos os níveis jurídicos, políticos e sociológicos” da cultura romana, constituindo o seu valor ético fundante.¹⁰⁹

A ideia de *fides* restou adjetivada surgindo a expressão *fides bona*, referindo-se à lealdade à palavra dada, ao agir correto, ao cumprimento preciso do que foi assumido, evidenciando uma norma de comportamento e associando sentido objetivo ao termo.

Ainda na ordem jurídica romana, a *fides bona* ganhou significado diverso, sendo compreendida como um estado psicológico, utilizada no campo dos Direitos Reais, especificamente em matéria de usucapião, e que revelava uma intenção ou estado de ignorância do possuidor, alcançando sentido subjetivo a expressão¹¹⁰.

No Direito Germânico, contudo, é que se encontra a formatação do princípio da boa-fé como se conhece contemporaneamente. A expressão *Treu und Glauben*

¹⁰⁷ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 43.

¹⁰⁸ António Menezes Cordeiro ressalta a existência de três espécies originárias, quais sejam: (i) *fides-sacra*; (ii) *fides-facto* e (iii) *fides-ética*. A *fides-sacra* estaria presente na Lei das XII Tábuas, no culto da deusa Fides, bem como na limitação aos poderes atribuídos ao pater. A *fides-ética* tinha uma conotação moral, implicando o sentido de dever, inclusive nos casos não previstos em lei. A *fides-facto*, por sua vez, sem o caráter religioso ou moral reparado nas duas primeiras concepções, representava a ideia de garantia. CORDEIRO, António Menezes. **Da boa fé no direito civil**. São Paulo: Almedina, 2017. p. 54-58.

¹⁰⁹ MARTINS-COSTA, *op. cit.*, p. 53-54.

¹¹⁰ CORDEIRO, *op. cit.*, p. 106-107.

(lealdade e crença/confiança na palavra dada) representava o universo da boa-fé obrigacional na Alemanha e, conforme explica Judith Martins-Costa, traduzia conotações em parte diversas daquelas que a marcaram no Direito Romano,

[...] muito embora ali estejam suas mais arcanas origens. Essas conotações diversas prendem-se à circunstância de terem sido enxertadas na ideia de fidelidade ao pactuado (uma das acepções da *fides* romana), as ideias de lealdade (*Treu* ou *Treue*) e crença (*Glauben* ou *Glaube*), reportadas, contudo, ao *ethos* cavaleiresco, expresso nas tradições dos juramentos de honra medievais, ligando-se, por consequência, ao “ideal de vida sublime” e ao “sonho do heroísmo” que se alojaram como elementos essenciais da cultura cavaleiresca. Traduzem, pois, um significado diverso daquele que infletirá na boa-fé possessória, derivada, no idioma alemão, de outra fórmula linguística – *Gutten glaupe*.¹¹¹

Antônio Menezes Cordeiro¹¹² esclarece, ainda, que no período compreendido entre o Direito Romano e a Idade Moderna, verificou-se forte influência do direito canônico, época em que somente era possível observar a vertente subjetiva do princípio, com significado oposto ao da má-fé e vinculada ao dolo.

A partir da mudança de paradigmas trazida pelo jusracionalismo, passou-se a observar um sistema jurídico baseado em padrões de racionalidade e surge um sistema baseado em regras e princípios gerais, admitindo-se critérios objetivos para balizar as relações.

Nesse cenário que, em 1900, entra em vigor o Código Civil alemão (BGB – *Bürgerliches Gesetzbuch*), que, em seus parágrafos 242¹¹³ e 157¹¹⁴, enunciou a necessidade de interpretação dos negócios jurídicos a partir da boa-fé¹¹⁵.

Todavia, somente no pós-guerra, e em razão dos inúmeros conflitos decorrentes das transformações sociais e econômicas oriundas da hiperinflação da década de 1920, que a jurisprudência alemã reconheceu a boa-fé como fonte autônoma de direitos e obrigações, e deu efetividade ao princípio, o utilizando como instrumento de revisão de cláusulas contratuais, então, desequilibradas¹¹⁶.

¹¹¹ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 53-54.

¹¹² CORDEIRO, Antônio Menezes. **Da boa fé no direito civil**. São Paulo: Almedina, 2017. p. 106-107.

¹¹³ O devedor está obrigado a executar a prestação como exige a boa-fé, levando os usos e costumes em consideração.

¹¹⁴ Os contratos devem ser interpretados como exige a boa-fé, levando-se os usos e costumes em consideração.

¹¹⁵ MOTA, Maurício Jorge. A pós-eficácia das obrigações revisitada. **Revista Quaestio Iuris**, Rio de Janeiro, v. 04, n. 01, p. 351-423, 2011.

¹¹⁶ NEGREIROS, Teresa. **Fundamentos para uma interpretação constitucional do princípio da boa-fé**. Rio de Janeiro: Renovar, 1998. p. 48-49.

A modernização do Direito Civil alemão levada a efeito com as reformas do BGB dos anos de 2001/2002, conquanto possa ter alterado o caráter sistemático do BGB, veio ainda a acentuar a relevância da boa-fé objetiva, especialmente por sua interface com o princípio da confiança. Assim, nomeadamente, ao positivizar o “direito da perturbação das prestações” (*Recht der Leistungsstörungen*) que inclui os regimes da mora, da impossibilidade, os chamados “danos à confiança”, o incumprimento definitivo, a culpa *in contrahendo*, a violação positiva do contrato (violação de meros deveres de proteção), além da violação de deveres acessórios, a base do negócio e o contrato com eficácia protetiva a terceiros. Esses institutos, agora codificados, nasceram da construção doutrinária e jurisprudencial viabilizada pela conjugação entre a presença das cláusulas gerais e a atuação de uma jurisprudência (em sentido amplo) culta e responsável.¹¹⁷

Inspirados no BGB, diversos países positivaram a boa-fé, reconhecendo, assim, sua indiscutível força normativa. Ricardo Lupion destaca alguns exemplos:

O artigo 1337 do Código Civil Italiano de 1942, segundo o qual os contratantes, “no desenvolvimento das tratativas e na formação do contrato, devem comportar-se segundo a boa-fé”, complementado pelos artigos 1366 e 1375, os quais determinam, respectivamente, que o contrato deva ser interpretado e executado segundo a boa-fé. O Código Civil Português de 1967 também impõe aos contratantes “proceder segundo as regras da boa-fé”.¹¹⁸

2.2 A BOA-FÉ NO ORDENAMENTO JURÍDICO BRASILEIRO

No ordenamento jurídico brasileiro, a primeira referência à boa-fé constou no artigo 131 do Código Comercial de 1850, que trouxe disposição acerca da boa-fé como princípio interpretativo dos contratos comerciais. A norma dispunha que:

[...] sendo necessário interpretar as cláusulas do contrato, a interpretação, além das regras sobreditadas, será regida sobre as seguintes bases: I – a inteligência simples e adequada, que for mais conforme à boa-fé e ao verdadeiro espírito e natureza do contrato, deverá sempre prevalecer à rigorosa e restrita significação das palavras [...].

Todavia, a amplitude desse dispositivo não foi reconhecida pela doutrina e pela jurisprudência, “[...] provavelmente devido ao fato de que em nossa tradição jurídica é

¹¹⁷ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 53-54.

¹¹⁸ GARCIA, Ricardo Lupion. **Boa-fé objetiva nos contratos empresariais**: contornos dogmáticos dos deveres de conduta. Porto Alegre: Livraria do Advogado, 2011. p. 41.

dispensável a invocação de uma regra jurídica para determinar a interpretação de lei e contratos”¹¹⁹.

Eduardo Tomasevicius Filho conclui que:

Já o Código Civil de 1916 não tinha cláusula geral sobre a boa-fé. Em matéria contratual, a doutrina sempre apontou o art. 1443, relativo a contrato de seguro, como único que estabelecia o dever de informar à contraparte sobre os riscos a serem cobertos, por força da boa-fé. Isso não significa, entretanto, que a boa-fé era um instituto ausente do direito brasileiro. O que houve foi a aproximação do direito brasileiro ao clássico inglês da boa-fé, de “tudo-ou-nada”: Liberdade para celebração dos contratos, sob o controle das regras sobre vícios do consentimento, e reconhecimento expresso da boa-fé na sua maior intensidade, ao impor a ubérrima fides contrato de seguro (art. 1443). Também havia outra disposição sobre a boa-fé como um modelo de conduta, ao cuidar da fraude contra credores, inspirada no brocardo *Non fraudantur creditores, cum quid non adquiritur a debitore, sed cum quid de bonis diminuitur*.¹²⁰

No Código Civil de 1916 não houve previsão expressa da boa-fé como cláusula geral, restringindo-se o diploma a fazer inúmeras referências à boa-fé em sua acepção psicológica, como estado de ignorância do agente, subjetiva, portanto. Judith Martins-Costa¹²¹ justifica a escolha de Clóvis Beviláqua na sua excessiva preocupação com a segurança, certeza e clareza das expressões normativas, que não permitiu a inserção de cláusulas gerais e, por essa razão, a boa-fé ficou restrita às hipóteses de ignorância escusável, especialmente em matéria de direito de família e em questões possessórias.

Em 1990, com o advento do Código de Defesa do Consumidor (CDC), a boa-fé objetiva foi expressamente referida no ordenamento jurídico brasileiro a partir dos artigos 4º, inciso III, e 51, inciso IV, do CDC. A legislação consumerista, derivada dos ditames constitucionais, orienta-se pelo desdobramento dos princípios fundamentais da dignidade da pessoa humana, da solidariedade social e da igualdade substancial. E, nesse contexto, a boa-fé passou a ser utilizada na interpretação das cláusulas contratuais e na integração das obrigações pactuadas, representando a importância do comportamento correto, leal e ético das relações contratuais.

A previsão da boa-fé no Código de Defesa do Consumidor mostra-se como um reflexo do princípio constitucional da solidariedade, consagrado no artigo 3º, I, da

¹¹⁹ TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no direito civil**. São Paulo: Almedina, 2020. p. 154.

¹²⁰ *Ibid.*, p. 155.

¹²¹ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 2000. p. 267.

Constituição da República, e se expande a partir do cenário obrigacional para todo o ordenamento jurídico.

Conforme Cláudia Lima Marques¹²², a adoção da boa-fé objetiva pelo CDC teve primordial importância na exegese das relações contratuais no Brasil como linha teleológica de interpretação e como cláusula geral, porquanto do seu conjunto de normas se correlaciona uma série de deveres anexos às relações contratuais, em especial, o dever de informação.

Teresa Negreiros¹²³, por sua vez, destaca que a importante contribuição do reconhecimento da boa-fé objetiva no ordenamento jurídico nacional, por meio do artigo 51, IV, do Código de Defesa do Consumidor, que prevê a nulidade de cláusulas contratuais incompatíveis com a boa-fé, foi a correlata necessidade de interpretação das relações negociais a partir da Constituição Federal. Isso porque, para que esse dispositivo seja aplicado,

[...] há que se buscar na normativa constitucional critérios de interpretação e densificação desta noção que funcionalizem à proteção da pessoa, de sua dignidade – onde e para onde, em última e definitiva instância, se radicam e convergem os princípios constitucionais.¹²⁴

Nesse sentido, a proteção contratual conferida ao consumidor, a partir do reconhecimento da boa-fé objetiva em seu diploma protetivo, representa efetivação do princípio constitucional da dignidade da pessoa humana.

Contudo, é a partir do Código Civil de 2002 que a boa-fé consolidou sua importância no Brasil. A expressão boa-fé permeia todo o texto da Lei e contempla uma grande quantidade de matérias, tais como posse, propriedade, seguro, tutela, pagamento, casamento, obrigações etc.

Nesse sentido, é possível reconhecer que o Código Civil evoluiu no seu conteúdo quanto à boa-fé e deixou de utilizá-la apenas em casos de ignorância escusável (aspecto subjetivo), passando a implicar sua incidência também como fonte de deveres autônomos sobre todos os contratos, eliminando a exclusividade de sua aplicação no âmbito das relações contratuais consumeristas.

¹²² MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**. 4. ed. São Paulo: Revista dos Tribunais, 2002. p. 186.

¹²³ NEGREIROS, Teresa. **Fundamentos para uma interpretação constitucional do princípio da boa-fé**. Rio de Janeiro: Renovar, 1998. p. 48-49.

¹²⁴ *Ibid.*

Destaca-se o reconhecimento da boa-fé objetiva como cláusula geral em matéria de direito contratual, técnica adotada pelos autores do texto para promover o avanço do direito por meio da jurisprudência¹²⁵.

Três dispositivos consagraram a boa-fé objetiva no Código Civil de 2002, cada um deles representando uma de suas funções, que mais adiante serão mais bem detalhadas. O artigo 113 determina que “[...] os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração”, comunicando sua função interpretativa. O artigo 187 estabelece que “[...] também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes”; eis a função controladora ou limitativa. E, por fim, o artigo 422 prevê que “[...] os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé”, sendo essa a função integrativa da boa-fé.

2.3 A BOA-FÉ OBJETIVA COMO CLÁUSULA GERAL

Não sendo o objeto deste estudo aprofundar a distinção entre cláusulas gerais e princípios jurídicos, cumpre, ao menos, pontuar alguns conceitos já consagrados na doutrina e que podem melhor orientar a compreensão do papel exercido pela boa-fé objetiva no cenário da proteção de dados e quais os seus reflexos no contexto em que se dá o consentimento.

Princípios normativos e cláusulas gerais são expressos em linguagem vaga e dotados de significativo grau de vagueza semântica, o que é próprio à referência a elementos axiológicos (bem comum, conduta razoável, boa-fé, moralidade etc.)¹²⁶.

Humberto Ávila, em sua conhecida obra *Teoria dos Princípios*, apresentou reconhecida distinção entre os princípios e as regras, e, quanto aos primeiros, que nos interessam neste momento, considera princípios normativos os que “[...] configuram proposições prescritivas de comportamentos”¹²⁷ a que estão ligadas consequências, e, como tal, possuem efetiva carga prescritiva. Não estando aqui a se

¹²⁵ TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no direito civil**. São Paulo: Almedina, 2020. p. 156.

¹²⁶ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 169.

¹²⁷ ÁVILA, Humberto Bergmann. **Teoria dos princípios**. Da definição à aplicação dos princípios jurídicos. 16. ed. São Paulo: Malheiros, 2015. p. 102.

referir a aforismas, axiomas, recomendações ou sínteses indicadoras da *ratio* de determinado instituto¹²⁸.

Os princípios normativos, segundo Humberto Ávila, e em relação aos quais interessa identificar a existência de distinção, possuem as seguintes características:

[...] (a) os princípios não descrevem objetos imediatamente determináveis, mas um “estado ideal de coisas” a ser promovido mediante a adoção de determinado comportamento; (b) o modo pelo qual o julgador os aplica, exigindo uma prévia avaliação da “correlação positiva entre os efeitos da conduta adotada e o estado das coisas que deve ser promovido”; e (c) a circunstância de contribuírem para a solução do problema prático sobre o qual incidem como “razão a serem conjugadas com outras para a solução de um problema”.¹²⁹

São essas as características dos princípios prescritivos de normas que muito se identificam com a ideia de cláusulas gerais.

Tanto nos princípios quanto nas cláusulas gerais é manifesto o caráter imediatamente finalista da norma quanto ao escasso ou inexistente elemento descritivo. Os princípios visam a prescrever determinados fins, sem descrever, diretamente, qual o comportamento devido para alcançar tais fins. Também nas cláusulas gerais não há o elemento descritivo. Ao invés de descrever condutas, ambos proporcionam critérios para o juiz tomar uma posição diante de situações concretas que, no entanto, a priori, são indeterminadas, só adquirindo um significado operativo no momento da sua aplicação a um caso específico.¹³⁰

Os princípios cominam a promoção de um estado ideal de coisas, igualmente como as cláusulas gerais, que indicam condutas ideais, mas sem descrevê-las. Contudo, os princípios prescritivos enviam diretamente a uma realidade valorativa, as cláusulas gerais remetem o intérprete a outros espaços do ordenamento.

Quando uma cláusula geral promove o reenvio a um valor, haverá superposição entre a cláusula geral e o princípio jurídico. É exatamente o caso do art. 422 do Código Civil, que expressa, concomitantemente, um princípio, um standard comportamental é uma cláusula geral: trata-se de um princípio porque os contraentes deverão adotar um comportamento probado (segundo o standard comportamental da probidade), porque este comportamento é necessário à promoção de um tráfico jurídico adequado, fundado na seriedade das declarações negociais, na confiança na mútua conduta e na consideração às legítimas expectativas dos contraentes. os contraentes são, portanto, direcionados a uma ação valiosa (leal, proba, útil,

¹²⁸ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 165.

¹²⁹ *Ibid.*, p. 166.

¹³⁰ *Ibid.*, p. 166.

correspondente à legítima confiança investida) em vista ao adimplemento satisfativo, fim que polariza toda e qualquer relação contratual.¹³¹

Judith Martins-Costa, em seu prestigiado livro sobre a boa-fé no direito privado¹³², faz um minucioso estudo sobre as *normas abertas*, ou *vagas*, e apresenta a classificação delas em (i) princípios normativos (ou gerais), (ii) conceitos indeterminados¹³³ e (iii) cláusulas gerais, para concluir que a boa-fé objetiva, nos moldes em que consta no ordenamento jurídico brasileiro, deve ser considerada como cláusula geral, ainda que a distinção conceitual para a definição de princípio jurídico não seja absolutamente evidente.

A autora¹³⁴, após examinar seis critérios, conclui não haver distinção entre princípios normativos e as cláusulas gerais, nem pela linguagem, nem pela estrutura, sequer pela finalidade ou modo de raciocínio que ensejam. E afirma que somente existirá distinção entre princípios inexpressos legislativamente e cláusulas gerais, porquanto essas últimas somente podem ser aceitas quando derivadas de uma fonte legal.

Cláusulas gerais serão sempre objeto de uma expressa formulação legal e, muitas vezes, referem um valor, pois assim, ter-se-á um enunciado normativo que configura, ao mesmo tempo, princípio e cláusula geral.

Karl Larenz¹³⁵, abordando a boa-fé como cláusula geral, afirmou que se tratava de princípio supremo do Direito das Obrigações, com possibilidade de aplicação universal; e, no mesmo sentido, defendeu António Menezes Cordeiro¹³⁶ que a boa-fé concretiza, ao longo do tempo, e independentemente do momento, sua ideia básica, a busca da lealdade e equivalência entre as partes.

Portanto, já é possível concluir que a boa-fé, nos termos como referida na Lei Geral de Proteção de Dados, pode ser enunciada como princípio normativo ou cláusula geral, sem maior equívoco.

¹³¹ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 168.

¹³² *Ibid.*, p. 131.

¹³³ Segundo a autora, os conceitos indeterminados distinguem-se entre aqueles que aludem a uma *realidade valorativa* e os que aludem a uma *realidade fática*. Em relação aos últimos, não se verifica dificuldade na distinção com as cláusulas gerais, pois reportam vagueza socialmente típica; exemplificando com as expressões “ainda a crédito” (artigo 1643, I, CC), “divisão cômoda do imóvel a ser partilhado” (artigo 1251, *caput*, CC), entre outras. *Ibid.*

¹³⁴ *Ibid.*, p. 156-196.

¹³⁵ LARENZ, Karl. **Derecho de obligaciones**. Tradução para o espanhol de Jaime Santos Briz. Madrid: Editorial Revista de Derecho Privado, 1958. tomo I. p. 146.

¹³⁶ CORDEIRO, António Menezes. **Da boa fé no direito civil**. São Paulo: Almedina, 2017. p. 1280.

Mas, para ajustar o texto deste estudo, importa definir a boa-fé como cláusula geral do tipo regulativa¹³⁷, ainda tomando-se por base a classificação da citada autora, uma vez que o *caput* do artigo 6º da LGPD é taxativo em afirmar que “as atividades de tratamento de dados deverão observar a boa-fé” e, portanto, regula todo o universo de situações que envolvam dados pessoais, direcionando e orientando as condutas nessas relações.

Destacam-se, por oportuno, dois reflexos principais da boa-fé, da forma como está alocada na Lei Geral de Proteção de Dados: normatividade, ou seja, seu conteúdo como fonte direta de eficácia jurídica e proteção da confiança dos sujeitos envolvidos nessas relações, em especial, o titular dos dados.

2.4 BOA-FÉ SUBJETIVA E BOA-FÉ OBJETIVA

A delimitação da acepção da boa-fé que demandará nossa atenção, antes anunciada, exige que se faça a distinção entre elas: a boa-fé objetiva, como dever de conduta, e a boa-fé subjetiva, como elemento psicológico. Clóvis do Couto e Silva expõe que

[...] a boa-fé possui múltiplas significações dentro do direito. Refere-se, por vezes, a um estado subjetivo decorrente do conhecimento de certas circunstâncias, em outras, diz respeito à aquisição de determinados direitos, como o de perceber frutos. Seria fastidioso enumerar as diferentes formas de operar desse princípio nos diversos setores do direito. Com relação ao das obrigações, manifesta-se como máxima objetiva que determina aumento de deveres, além daqueles que a convenção explicitamente constitui. Endereça-se a todos os partícipes do vínculo e pode, inclusive, criar deveres para o credor, o qual, tradicionalmente, era apenas considerado titular de direitos.¹³⁸

A boa-fé subjetiva tem ligação estreita com a crença do agir de acordo com o Direito; é ignorância que escusa a antijuridicidade do agente que acredita se comportar em estrita legalidade, não tendo consciência de que sua conduta é contrária ao ordenamento jurídico. Consiste numa situação psicológica, num estado de ânimo ou de espírito do agente que realiza determinado ato ou vivencia dada situação, sem ter ciência do vício que a macula.

¹³⁷ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 142.

¹³⁸ SILVA, Clóvis V. do Couto e. **A obrigação como processo**. Rio de Janeiro: FGV, 2006. p. 33.

A expressão boa-fé subjetiva indica um estado de fato, traduzindo a ideia naturalista da boa-fé, aquela que, por antinomia, é conotada à má-fé, razão pela qual essa acepção comumente é expressada como “agir de boa-fé”, o contrário a “agir de má-fé”. Diz-se subjetiva a boa-fé compreendida como estado psicológico, isto é: estado de consciência caracterizado pela ignorância de se estar a lesar direitos ou interesses alheios, ou a convicção de estar agindo em bom direito.¹³⁹

A boa-fé subjetiva é uma condição psicológica, na qual o agente acredita legitimamente estar agindo de acordo com o Direito e ignora estar lesando direito alheio; por essa razão, a incidência das regras atinentes à tutela da boa-fé subjetiva importam, evidentemente, avaliação sobre a subjetividade do sujeito; e, concluindo-se pela presença da boa-fé subjetiva, excluída será a ilicitude.

A boa-fé objetiva, ou boa-fé normativa, não se relaciona com a intencionalidade ou subjetividade do sujeito, mas aponta, conforme ensina Judith Martins-Costa¹⁴⁰, para (i) um instituto ou modelo jurídico, (ii) um *standard* ou modelo comportamental, e (iii) um princípio jurídico, apresentado, assim, a dificuldade de caracterização precisa da locução *boa-fé objetiva*.

Ainda assim, é possível afirmar que a boa-fé se traduz em regra de conduta que qualifica o comportamento leal, ético e confiável. Agir conforme a boa-fé, reforça-se, significa agir com probidade, correção e lealdade no âmbito das relações jurídicas negociais.

Pode-se afirmar que a boa-fé objetiva representa o dever de agir de acordo com os padrões socialmente reconhecidos de lisura e lealdade. São esses padrões que traduzem confiança necessária à vida de relação e ao intercâmbio de bens e serviços. Consequentemente é dever de cada parte agir de forma a não defraudar a confiança da contraparte, indispensável para a tutela da segurança jurídica, para a garantia da realização das expectativas legítimas das partes.¹⁴¹

Seu elemento central é a confiança entre os contratantes, devendo cada uma das partes comportar-se de modo a não iludir indevidamente a outra ou frustrar as legítimas expectativas e os interesses do outro contratante quanto à execução do contrato e tudo o que o cerca.

¹³⁹ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 279.

¹⁴⁰ *Ibid.*, p. 281.

¹⁴¹ GARCIA, Ricardo Lupion. **Boa-fé objetiva nos contratos empresariais**: contornos dogmáticos dos deveres de conduta. Porto Alegre: Livraria do Advogado, 2011. p. 50.

2.5 AS FUNÇÕES DA BOA-FÉ OBJETIVA E OS DEVERES ANEXOS

A boa-fé objetiva interessa mais por suas funções do que por sua definição¹⁴². Atuando funcionalmente, a boa-fé serve como pauta de interpretação, fonte de integração e critério para a correção de condutas contratuais. As funções da boa-fé objetiva revelam seu caráter tridimensional e salientam seu viés de proteção do equilíbrio contratual e busca pelo adequado adimplemento das relações jurídicas.

Judith Martins-Costa adverte sobre a importância da identificação precisa sobre as três distintas funções da boa-fé: hermenêutica, integradora e corretiva.

Conquanto na prática possam estar superpostas – pois, ao interpretar certo o contrato ou ao integrá-lo, determinando a existência de um dever, se estará, ao dar a solução, também possibilitando a correção do conteúdo de um contrato, ou de certa conduta da parte –, no plano analítico e no funcional, a criação de deveres, via integração do conteúdo contratual, não se confunde com a função corretiva daquele conteúdo. Esta última se dará, por exemplo, pela declaração de ineficácia (ou nulidade, conforme o caso) de cláusulas abusivas ou determinações que importem na alegação da própria torpeza; ou, ao se pedir o exercício do direito de resolução, conta do adimplemento substancial do contrato; ou, ainda, ao ser suspensa a eficácia de comportamentos deslealmente contraditórios.¹⁴³

A *função interpretativa* apresenta a boa-fé como um cânone hermenêutico, servindo como referencial interpretativo, fundamentando a análise da relação jurídica na ética e na adequação. Trata-se de norma de interpretação dos negócios jurídicos, nos quais “[...] as declarações de vontade serão avaliadas conforme a confiança que haja suscitado de acordo com a boa-fé”¹⁴⁴.

O artigo 113 é norma cogente e não poderá ser afastada pela vontade das partes, uma vez que o comportamento alinhado com a boa-fé é dever jurídico, o qual deve ser observado pelos contratantes durante todo o período do contrato.

[...] trata-se de regra objetiva que concorre para o comportamento devido, desvelando o verdadeiro sentido e alcance contratual, permitindo, então, que o bom fim das obrigações, a satisfação dos interesses juridicamente protegidos dos contratantes, seja alcançado. Trata-se de preceito ético, porém ligado igualmente à finalidade econômica do contrato.¹⁴⁵

¹⁴² MARTINS-COSTA, Judith. **A boa-fé no direito privado: critérios para a sua aplicação**. 2. ed. São Paulo: Saraivajur, 2018. p. 43.

¹⁴³ *Ibid.*, p. 564.

¹⁴⁴ OLIVEIRA, J. M. Leoni Lopes. **Novo Código Civil anotado**. Rio de Janeiro: Lumen Juris, 2004. p. 218.

¹⁴⁵ BUSSATTA, Eduardo Luiz. **Resolução dos contratos e teoria do adimplemento substancial**. 2. ed. São Paulo: Saraiva, 2008. p. 78-80.

As cláusulas contratuais deverão ser interpretadas de forma que se “[...] privilegie sempre o sentido mais conforme à lealdade e à honestidade entre as partes”¹⁴⁶, não sendo correta a sua leitura que admita interpretação maliciosa ou dirigida a iludir e/ou prejudicar qualquer uma das partes.

Na função hermenêutica, a boa-fé permite apreender os interesses das partes em vista dos esquemas socialmente normais e regulares, contrastando-os com a eventual singularidade do ato de autonomia privada. Viabiliza valorar a conduta das partes no curso do processo obrigacional, contrastando a conduta efetivamente tida com o *standard* da conduta segundo a boa-fé, é dizer: uma conduta leal, proba, cooperativa com o *alter* em vista dos fins visados pelo negócio e das expectativas legitimamente geradas por sua pactuação. E autoriza o intérprete a concluir – em razão do comportamento seguido – qual o sentido a conferir à manifestação de vontade, pois todo o contrato importa um dever de manutenção de uma linha de coerência.¹⁴⁷

Clóvis do Couto e Silva¹⁴⁸ explica que, nesse processo hermenêutico, cuida-se em conferir justa medida à vontade que se interpreta – pois que o contrato não se constitui de duas volições, ou de uma oferta e uma aceitação, isoladamente, mas da fusão desses dois elementos.

De fato, quando a boa-fé é utilizada como o cânone hermenêutico, o intérprete não parte de uma abstração a ser resolvida num plano ideal, mas da necessidade de dar uma resposta adequada a problemas inseridos em um contexto concreto e singular¹⁴⁹.

Também nas atividades de tratamento de dados, conforme se verá mais adiante, a função hermenêutica deve amparar a análise que se fará da manifestação de vontade, ou consentimento, para a autorização de utilização de dados pessoais, pois, assim como nos negócios jurídicos de massa, ou de consumo, é característica desses vínculos a assimetria informacional e, portanto, a boa-fé auxilia identificar o que era razoável esperar em vista da compreensibilidade do universo dos contratantes-aderentes (critério do tipo médio ou público-alvo específico, e não abstrato)¹⁵⁰ no momento da formação do vínculo.

¹⁴⁶ TEPEDINO, Gustavo; SCHREIBER, Anderson. A boa-fé objetiva no Código de Defesa do Consumidor e no Novo Código Civil. *Revista da EMERJ*, Rio de Janeiro, v. 6, n. 23, p. 29-44, 2003.

¹⁴⁷ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 511.

¹⁴⁸ SILVA, Clóvis V. do Couto e. **A obrigação como processo**. Rio de Janeiro: FGV, 2006. p. 35.

¹⁴⁹ MARTINS-COSTA, *op. cit.*, p. 490.

¹⁵⁰ *Ibid.*, p. 509.

A *função corretora, controladora ou limitativa* da boa-fé impede o abuso do direito, coibindo o exercício manifestamente desleal, incoerente, imoderado ou irregular de direitos subjetivos, formativos, faculdades e posições jurídicas¹⁵¹, ou seja, constitui obstáculo ao uso abusivo dos direitos subjetivos dos contratantes, determinando os limites do uso desses direitos e a extensão do exercício legítimo dos mesmos. Configura-se, assim, como critério de diferenciação entre o exercício regular e o exercício irregular ou abusivo de direitos diante da outra parte na relação contratual.

O abuso do direito é definido por Heloísa Carpena Vieira de Mello como sendo

[...] aquele pelo qual o sujeito excede os limites ao exercício do direito, sendo estes fixados por seu fundamento axiológico, ou seja, o abuso surge no interior do próprio direito, sempre que ocorra uma desconformidade com o sentido teleológico em que se funda o direito subjetivo. O fim – social ou econômico – de um certo direito subjetivo não é estranho à sua estrutura, mas elemento de sua própria natureza.¹⁵²

A boa-fé objetiva configura-se, assim, como *máxima de conduta ética-jurídica*, que impede o abuso do direito subjetivo, identificada pelo ordenamento jurídico como *ato ilícito*, nos termos do artigo 187 do Código Civil. Nesse sentido, a função da boa-fé de limitar e impedir o exercício de direitos que emergem da relação contratual está diretamente relacionada à teoria do abuso de direito.

Judith Martins-Costa adverte, contudo, que

[...] não basta o fato da contrariedade – isoladamente considerada – para tachar-se de determinada conduta contraditória como ilícita. Pode não haver consequências jurídicas à contradição que, afinal, integra a condição humana. É preciso averiguar se a conduta contraditória atinge aqueles vetores postos no artigo 187 da Lei Civil como “balizas da ilicitude” no modo do exercício. Haverá ilicitude quando a contrariedade importar em uma deslealdade e não houver justa causa para a contrariedade.¹⁵³

Por seu turno, a função estabelecida pelo artigo 422 do Código Civil é a *integrativa*, sendo a boa-fé criadora de deveres especiais de conduta, também

¹⁵¹ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 626.

¹⁵² MELLO, Heloísa Carpena Vieira de. O abuso de direito no Código Civil de 2002: relativização dos direitos na ótica civil-constitucional. In: TEPEDINO, Gustavo (coord.). **A parte geral do Novo Código Civil**: estudos na perspectiva civil-constitucional. 2. ed. Rio de Janeiro: Renovar, 2003. p. 377-396.

¹⁵³ MARTINS-COSTA, *op. cit.*, p. 674.

chamados de deveres anexos, instrumentais ou colaterais, a serem observados pelas partes durante todo o vínculo obrigacional.

António Meneses Cordeiro¹⁵⁴ sistematiza os deveres anexos decorrentes da boa-fé objetiva de forma tripartida: deveres de proteção, de esclarecimento e de lealdade. Entende-se por dever de proteção a obrigação de que cada uma das partes tem de impedir, mediante a sua lisura, que o outro seja, de algum modo, prejudicado com aquela relação negocial. Para atender ao dever de informação, necessário se faz que as partes atuem, uma perante a outra, com transparência, sem omitir informações que possam ensejar prejuízo ao outro. Já a lealdade está diretamente ligada às legítimas expectativas da outra parte com relação àquilo que ambas pactuaram.

Judith Martins-Costa¹⁵⁵ aponta que esses deveres se referem ao *exato processamento da relação obrigacional*, sintetizando-os como (i) *deveres de cuidado, previdência e segurança*, (ii) *deveres de aviso e esclarecimento*, (iii) *deveres de informação*, (iv) *dever de prestar contas*, (v) *deveres de colaboração e cooperação* e (vi) *deveres de omissão e de segredo*.

A boa-fé objetiva, portanto, agrega à relação uma *obrigação de conduta*¹⁵⁶, de forma a garantir um ético e correto adimplemento obrigacional.

Para Clóvis do Couto e Silva¹⁵⁷, a boa-fé revela-se, por sua função integrativa, como orientadora da conduta a ser adotada pelas partes, indicando um dever de como se portar, e é essa a principal faceta da cláusula geral da boa-fé no âmbito das relações que envolvem tratamento de dados.

O dever geral de boa-fé é atendido quando as partes desempenham suas condutas de modo honesto, leal e correto, evitando causar danos ao outro (dever de proteção) e garantindo o conhecimento de todas as circunstâncias relevantes para o vínculo (dever de informação) – comportamento que faz florescer laços de confiança entre os contratantes¹⁵⁸.

¹⁵⁴ CORDEIRO, António Menezes. **Da boa fé no direito civil**. São Paulo: Almedina, 2017. p. 604-608.

¹⁵⁵ MARTINS-COSTA, Judith. **A boa-fé no direito privado: critérios para a sua aplicação**. 2. ed. São Paulo: Saraivajur, 2018. p. 573.

¹⁵⁶ MARQUES, Cláudia Lima. **Contratos no código de defesa do consumidor: o novo regime das relações contratuais**. 6. ed. São Paulo: Revista dos Tribunais, 2011. p. 217.

¹⁵⁷ SILVA, Clóvis V. do Couto e. **A obrigação como processo**. Rio de Janeiro: FGV, 2006. p. 36.

¹⁵⁸ Conforme Paulo Lôbo, ao analisar o pensamento de António Menezes Cordeiro, a noção de boa-fé exprime um imperativo ético, ou seja, encerra a ideia de um comportamento ideal a ser atingido, não se confundindo com a noção de bons costumes, muito mais próxima do campo da moral que é extraída da realidade social. LÔBO, Paulo Luiz Netto. **Teoria geral das obrigações**. São Paulo: Saraiva, 2005. p. 81-83.

Sobre os deveres decorrentes da boa-fé objetiva, portanto, várias são as classificações e denominações que podem ser utilizadas ou adotadas, todas bastante similares e interconectadas. Em síntese, e para adotar uma delas, com o objetivo de destacar o dever de conduta que merece maior ênfase nas relações aqui estudadas, adota-se a seguinte subdivisão: deveres de proteção, deveres de cooperação e deveres de informação e transparência.

Os deveres de proteção impõem às partes a obrigação de prevenir danos, tanto em relação ao objeto da prestação como também em relação às esferas jurídicas das partes e eventualmente de terceiros, e se desdobram na exigência da manutenção de um comportamento diligente, de velar pelo adequado fluxo da relação jurídica obrigacional com cuidado, previdência e segurança.

O dever de cooperação, por sua vez, impõe às partes obrigação de mútuo auxílio na superação de eventuais obstáculos surgidos em qualquer fase do desenvolvimento da relação jurídica obrigacional, por vezes confundindo-se com a exigência de fidelidade e lealdade entre as partes contratantes, que, dentre outras condutas, pode ensejar o dever de omissão e segredos de informações obtidas no *iter* obrigacional para a preservação de interesses comuns ou específicos de um dos figurantes. O dever de cooperação associa-se à exigência de lealdade e à relação de confiança que deve existir entre as partes.

Destaca-se, por fim, o dever de informação, que parece o dever decorrente da boa-fé objetiva de maior repercussão nas relações as quais envolvem o tratamento de dados pessoais.

Informar é advertir, explicar, esclarecer, avisar e prestar contas, sempre que se fizer necessário, em especial quando dessas informações depende uma decisão da outra parte para o pleno desenvolvimento da relação.

Alguns doutrinadores entendem que a transparência advém do princípio da boa-fé objetiva, ou mesmo que se trata de um reflexo ou subprincípio¹⁵⁹, que, em consonância com o dever de informação, possui o intuito de qualificar a informação prestada¹⁶⁰.

¹⁵⁹ RIBEIRO, Joaquim de Sousa. O imperativo de transparência no Direito Europeu dos Contratos. *In*: FIUZA, César; SÁ, Maria de Fátima Freire de; NAVES, Bruno Torquato de Oliveira (coord.). **Direito civil**: atualidades. Belo Horizonte: Del Rey, 2003. p. 131-157. p. 146.

¹⁶⁰ CAVALIERI FILHO, Sergio. **Programa de direito do consumidor**. São Paulo: Atlas, 2008. p. 34-36.

A transparência – ao lado do dever de informação – é entendida como verdadeiro *corolário da boa-fé objetiva*¹⁶¹, possuindo um papel fundamental nas relações de tratamento de dados, pois impõe a efetiva qualificação da informação que antecede o consentimento, sob pena de esse não ser suficiente como base de legitimação à utilização dos dados.

2.6 A BOA-FÉ NA LEI GERAL DE PROTEÇÃO DE DADOS

No cenário hiperconectado em que se vive, no qual a troca, a circulação e o tratamento de dados são fundamentais, não só para o desenvolvimento econômico da sociedade, mas, também, para o desenvolvimento social, normas reguladoras em todo o mundo passaram a estabelecer regras para permitir que o fluxo informacional preserve a privacidade e a dignidade dos indivíduos.

Na esteira do implemento do Regulamento Geral de Proteção de Dados europeu, a Lei Geral de Proteção de Dados brasileira, Lei n.º 13.709/2018, inseriu o Brasil entre os países que contam com instrumentos¹⁶² para a proteção desse importante aspecto da dignidade da pessoa humana e do direito à privacidade¹⁶³. Representou grande avanço no sistema jurídico brasileiro, concretizando e uniformizando direitos dos titulares de dados e reconhecendo a autodeterminação informacional¹⁶⁴ como um de seus fundamentos; e culminou com a aprovação da Emenda Constitucional 115, de 2022, que alcançou *status* de direito fundamental ao

¹⁶¹ BRAGA NETO, Felipe Peixoto. **Manual de direito do consumidor**: à luz da jurisprudência do STJ. 8. ed. Salvador: Juspodivm, 2013. p. 54.

¹⁶² Mesmo antes da LGPD, os dados pessoais já eram merecedores de tutela constitucional à luz do sistema de proteção dos direitos fundamentais. Segundo Laura Mendes, “[...] é possível, a partir de uma interpretação sistemática da Constituição, fundamentar uma garantia geral de proteção de dados pessoais no sistema de direitos fundamentais: partindo do reconhecimento da proteção da informação pessoal pela ação de *habeas data* e do princípio fundamental da dignidade humana (art. 1º, III, CF), é possível ampliar a garantia da inviolabilidade da intimidade e da vida privada para a proteção de dados pessoais”. MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, a. 12, n. 39, p. 185-216, jul./dez. 2018. p. 199.

¹⁶³ SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 319-338. p. 320.

¹⁶⁴ Assim, percebe-se que a regra é a autodeterminação do titular sobre os dados pessoais, salvo direitos de terceiros ou interesse público predominante, previsto em legislação. Isso enseja a necessidade de autorização legal ou consentimento do titular de dados para que a coleta, o processamento, a utilização ou a circulação de dados pessoais sejam considerados legítimos. MENDES, *op. cit.*

direito à proteção de dados (ainda que esse já pudesse assim ser depreendido do direito à privacidade).

Por seu turno, a noção de boa-fé objetiva está fortemente ligada ao valor da ética e, nesse sentido, ampara os conceitos de lealdade, correção, transparência e boas práticas, que compõem a essência dos contratos em geral. É princípio geral que orienta a adoção de condutas corretas e adequadas no agir em sociedade e, por essa razão, tem papel de destaque na Lei Geral de Proteção de Dados, que, nos termos do *caput* do artigo 6º, afirma que “[...] as atividades de tratamento de dados deverão observar a boa-fé”.

Fabiano Menke e Guilherme Goulart¹⁶⁵ afirmam o importante papel da boa-fé na legislação brasileira, bem como nas legislações protetivas de dados europeias, destacando a essencialidade do princípio da boa-fé objetiva na segurança das relações que envolvem tratamento de dados.

A inclusão do princípio da boa-fé objetiva na legislação que protege a privacidade dos dados tem especial importância, porque a norma expressamente refere a indisponibilidade de conduta proba, leal e honesta nesse contexto. A existência do princípio da boa-fé no ordenamento jurídico, tanto pelas implicações, quando cabíveis, do Código Civil e do Código de Defesa do Consumidor nas relações digitais, mas, também, e especialmente, pelos consectários do princípio constitucional da dignidade da pessoa humana, com destaque para a proteção da privacidade, já seriam suficientes para que se exigissem condutas éticas e seguras nessas relações.

Contudo, a opção legislativa, ao consagrar a cláusula geral em estudo, no *caput* do artigo 6º da LGPD, corrobora o fato de que

[...] o Direito não pode se dar ao luxo de não ser positivo e o Direito positivo não pode se dar ao luxo de desvalorizar a segurança jurídica. Por definição, um Ordenamento jurídico deve oferecer segurança e almejar segurança. O Direito não serve para inquietar, mas para direcionar condutas e assegurar expectativas legítimas dos que vivem em sociedade. Deve acalmar, e não sobressaltar. Toda segurança jurídica em um Estado de Direito consiste em se poder ter ideia do a que se ater, a que seguir e a que obedecer. Por isso, é tarefa tanto do ordenamento quanto dos juristas oferecer critérios prévios –

¹⁶⁵ MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.); BIONI, Bruno (coord. Executivo). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 339-359. p. 347.

tanto para pautar a conduta dos homens quanto para explicitar e determinar os significados das normas que estabelecem essas condutas.¹⁶⁶

Ainda que a expressão boa-fé possa ser considerada semanticamente “vaga” ou “aberta”, não haverá maiores dificuldades de concretizá-la num cenário contextual específico. Isso significa dizer, conforme ensina Judith Martins-Costa¹⁶⁷, que a “boa-fé” não tem um conteúdo “imane” ou “substancialista”, mas contextual, estreitamente ligado às circunstâncias, aos “fatores vitais” determinantes do contexto de sua aplicação.

A LGPD, ao estabelecer “[...] que as atividades de tratamento de dados deverão observar a boa-fé”, busca corrigir um cenário de desequilíbrio contratual, ou assimetria informacional, inerente às relações digitais. Nesse sentido, sobressai sua função integrativa, que traz para as relações de tratamento de dados os deveres de coerência, informação e cooperação, em sintonia com a proteção da confiança e o dever de transparência.

Veja-se que no artigo 6º da LGPD são destacadas outras diretrizes, ou princípios, como refere a Lei, que também poderiam ser considerados como deveres decorrentes da boa-fé. Os critérios da finalidade, adequação e necessidade no tratamento de dados pessoais são exemplos de comportamentos corretos decorrentes do dever de coerência. As garantias de livre acesso, qualidade e transparência se relacionam com a observância do dever de informação. Os critérios de segurança, prevenção, não discriminação e responsabilização estão ligados à necessidade de cooperação dos agentes de tratamento de dados (controlador e operador).

Desse modo, reconhecida a importância e indispensabilidade do tratamento de dados para a evolução e aperfeiçoamento da atividade econômica, não se admite comportamento contraditório e abusivo nessas relações. É a cláusula geral da boa-fé que garante às partes a sensação de confiança para que forneçam seus dados em troca de produtos, acesso a informações e conteúdos, serviços e uma infinidade de benefícios que são condicionados a essa concessão.

¹⁶⁶ MARTINS-COSTA, Judith. Como harmonizar os modelos jurídicos abertos com a segurança jurídica dos contratos? (notas para uma palestra). **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 5, p. 67-76, jul./set. 2015. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/90/86>. Acesso em: 16 mar. 2022.

¹⁶⁷ *Id.* Os campos normativos da boa-fé objetiva: as três perspectivas do direito privado brasileiro. In: AZEVEDO, Antônio Junqueira; TORRES, Heleno Taveira; CARBONE, Paolo (coord.). **Princípios do Novo Código Civil Brasileiro e outros temas**. São Paulo: Quartier Latin, 2008. p. 386-420. p. 400.

Também da cláusula geral da boa-fé decorre a proibição de fazer mau uso, ou uso indevido, dos dados coletados. Tão importante quanto o consentimento válido do titular dos dados que autorize o seu tratamento, nos termos do artigo 7º, I, da LGPD, é o respeito que a boa-fé exige quanto ao seu uso. Nesse sentido, é disposto nos artigos 46 e 47 da Lei, que orientam a adoção de procedimentos de segurança no armazenamento, eliminação e descarte dos dados, para que terceiros não tenham acesso a essas informações.

Como anteriormente dito, a função hermenêutica auxilia na compreensão da intenção das partes em vista dos esquemas socialmente normais e regulares e viabiliza a valoração da conduta das partes no curso do processo obrigacional, contrastando a conduta efetivamente havida com o *standard* da conduta segundo a boa-fé, ou seja, uma conduta leal, proba, cooperativa com o *alter* em vista dos fins visados pelo negócio e das expectativas legitimamente geradas por sua pactuação. Essa função hermenêutica da boa-fé também deve ser observada nas relações de tratamento de dados, porque consequência lógica da inserção dela como cláusula geral na legislação que rege a matéria.

A avaliação de conduta do agente receptor dos dados que, amparado no desequilíbrio informacional intrínseco a essas relações, informa de forma ambígua, confusa e lacunosa não deve ser admitida e não poderá amparar o consentimento que antecede e autoriza o tratamento de dados.

A faceta limitativa da boa-fé também pode ser depreendida do *caput* do artigo 6º da LGPD, porque nos contratos entre desiguais, quando se identifica a assimetria informativa, é a boa-fé que age de forma a assegurar condições de relativa igualdade real entre os figurantes.

Quando um dos contratantes possui menos informações, ou nenhum domínio sobre elas, a boa-fé se apresenta como mecanismo autorregulador do equilíbrio contratual.

O reconhecimento de haver, na relação interindividual, situações de disparidade de poder fático leva a admitir restrições na liberdade contratual, sendo a falta (ou a impossibilidade fática) de exercício de autodeterminação por uma das partes o pressuposto da disciplina limitativa.¹⁶⁸

¹⁶⁸ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 629.

A inserção da cláusula geral da boa-fé na Lei Geral de Proteção de Dados encontra fundamento no próprio princípio da dignidade da pessoa humana e na construção de uma sociedade justa e solidária, como objetivo constitucional.

A opção do modelo legislativo brasileiro, ao fixar a necessidade de conduta de acordo com a boa-fé, nas atividades de tratamento de dados, mostra uma de suas facetas de caráter preventivo, que busca antecipar os riscos de violação à privacidade para evitar danos à pessoa humana¹⁶⁹.

¹⁶⁹ TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 281-318.

3 ASSIMETRIA INFORMACIONAL E O CONSENTIMENTO NA LGPD: BUSCA DE SOLUÇÕES A PARTIR DA CLÁUSULA GERAL DA BOA-FÉ OBJETIVA

O consentimento, como máxima expressão da autodeterminação informativa, deve se constituir em uma escolha livre, voluntária, o que somente é possível se aquele que consente tiver um complexo de informações suficientes para embasar sua decisão. Contudo, o ambiente digital dificulta significativamente a configuração dessa manifestação voluntária de vontade, especialmente por conta do cenário de grande assimetria informacional que gravita em torno do tratamento de dados.

Por seu turno, a boa-fé objetiva, como cláusula geral, é presença obrigatória em todas as relações que envolvem o tratamento de dados pessoais, o que significa dizer que um padrão ético e leal de conduta se exige dos seus personagens, especialmente daqueles que possuem o domínio das informações sobre as tecnologias que usam e tratam os dados, bem como a responsabilidade de zelar pela privacidade dos usuários que autorizam a utilização de seus dados nas redes a partir do consentimento.

O dever de informação e transparência tem especial destaque na disciplina de tratamento de dados e, por ser suporte do consentimento como instrumento de exercício do direito à autodeterminação informativa, será analisado na sequência. Esses deveres decorrem da lei, mas também da imposição de conduta ética orientada pela boa-fé objetiva que, especialmente nas relações marcadas pelo desequilíbrio informacional, são determinantes para a adequação dos vínculos.

Após analisado o conteúdo do dever de informação, pretende-se analisar o cenário de assimetria informacional no qual acontece a manifestação de vontade que autoriza o tratamento de dados pessoais, indagando-se se no ambiente digital é realmente possível a adjetivação plena do consentimento, como livre, informado, inequívoco e para uma finalidade determinada, ou se esse “qualificado” consentimento é simplesmente uma ficção.

A partir daí, pretende-se identificar os deveres de conduta dos agentes de tratamento e as potencialidades da boa-fé objetiva nas relações que envolvem dados pessoais como balizadora das condutas desses agentes, em busca de alternativas para a mitigação da assimetria informacional e proteção da autodeterminação informativa.

E, por fim, identificadas as condutas legais e as decorrentes da cláusula geral da boa-fé a serem observadas pelos controladores para minimizar riscos à proteção de dados, analisar a conexão entre o *privacy by design* e a boa-fé como uma estrutura necessária para a proteção da confiança dos titulares sobre a segurança de suas informações no momento do consentimento.

3.1 A IMPORTÂNCIA DO DEVER DE INFORMAÇÃO COMO SUPORTE AO CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

O *caput* do artigo 6º da LGPD, cumulado com seu inciso VI¹⁷⁰, que garante aos titulares de dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, enuncia a existência de um direito de informação, por parte do interessado, no momento em que se procede a solicitação de seus dados, bem como se as informações prestadas são adequadas, corretas e suficientes para a tomada de decisão sobre a concessão da autorização para o uso dos dados pessoais.

O dever de informar por parte dos agentes de tratamento de dados é tópico central do sistema de proteção de dados, notadamente no que diz respeito ao consentimento do titular das informações, pois, como dito anteriormente, essa obrigação deve ser cumprida de maneira eficaz, ou seja, o agente de tratamento de dados não se libera desse dever fornecendo qualquer informação, é preciso que a linguagem seja clara e de fácil compreensão.

O titular não pode exercer o direito fundamental à proteção de dados pessoais, assim entendido como o direito de controle sobre as suas informações, ou autodeterminação informativa, pois se desconhece quais são as finalidades que justificam o requerimento e tratamento dos seus dados. É esse direito de informação que atribui à pessoa o conhecimento e controle sobre o que se fará com os seus dados pessoais e lhe permite optar por dar ou não o seu consentimento.

No se puede ejercer el derecho fundamental a la protección de los datos personales, entendido como el derecho al control sobre la propia información personal, si se desconoce cuáles son las finalidades que justifican el tratamiento de la información personal, quién es el responsable ante el cual

¹⁷⁰ LGPD - Artigo 6º. [...] 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.

se pueden ejercitar los derechos y cuáles son las finalidades que justifican el tratamiento de la información personal, quién es el responsable ante el cual se pueden ejercitar los derechos y cuáles son los posibles cesionarios. De hecho, el consentimiento del interesado es definido como toda manifestación de voluntad no solo libre, inequívoca y específica, sino también informada. El cumplimiento del principio de información no solo permite el consentimiento, sino también facilita el ejercicio del derecho de acceso, rectificación, cancelación y oposición, incluyendo la posibilidad de ejercitar estos derechos, así como la identidad y dirección del responsable.¹⁷¹

A exigência de que ao indivíduo sejam fornecidas informações transparentes e precisas sobre os riscos e implicações da utilização de seus dados busca minimizar a assimetria técnica ínsita a essas relações. Bruno Bioni¹⁷² fala no dever-direito de informação: dever de informar suficientemente sobre a utilização dos dados e direito do cidadão de estar capacitado a controlar essas informações e o uso delas.

A prestação de uma informação só tem razão de ser se ela ocasionar transparência no fluxo dos dados pessoais. Esse é o resultado ótimo esperado decorrente do adimplemento satisfatório do dever de informar e, em última análise, do que se espera ao adjetivar como informado o consentimento.¹⁷³

O princípio da transparência, enunciado pelo inciso VI do artigo 6º da LGPD, proclama a existência de um direito de informação por parte do titular de dados e esse direito à informação atribui à pessoa o conhecimento que lhe permite o controle sobre seus dados pessoais sujeitos ao tratamento; determina que o indivíduo deva ser informado claramente e de maneira adequada sobre a coleta, o uso, o armazenamento e o tratamento dos dados pessoais.

O elemento finalístico desse princípio é alcançar uma relação sem qualquer tipo de opacidade, obscuridade; mas, ao revés, clara, cristalina, nítida, translúcida e, por que não, sincera, como aponta Cláudia Lima Marques¹⁷⁴

O direito/dever de informar é uma garantia correlata e necessária a esse princípio¹⁷⁵, pois é justamente esse diálogo que propicia ao titular dos dados o

¹⁷¹ MONTERO, Javier Puyol. Transparencia de la información y derecho de acceso de los interesados em la nueva normativa de protección de datos. In: LOMBARTE, Artemi Rallo (dir.). **Tratado de protección de datos**. Valencia: Tirant lo Blanch, 2019. p. 275-312. p. 285.

¹⁷² BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 184.

¹⁷³ *Ibid.*, p. 184.

¹⁷⁴ MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 8. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2016. p. 745.

¹⁷⁵ NUNES, Luiz Rizatto. **Curso de direito do consumidor**. São Paulo: Saraiva, 2011. p. 174.

necessário conhecimento para que possa exercer em sua plenitude os direitos que a lei lhe assegura.

Portanto, o dever de informar operacionaliza o princípio da transparência, uma vez que é a tal interação que eliminará qualquer tipo de deslealdade na relação posta, a ponto de racionalizar as decisões do titular dos dados, pois “[...] somente a vontade racional: a vontade realmente livre (autônoma) e informada, legítima, isto é, tem o poder de ditar a formação, e, por consequência, os efeitos da manifestação de vontade”¹⁷⁶.

Daniel Solove, em estudo sobre o dever de informação, explica que o princípio da transparência exige que a informação prestada ao titular dos dados resolva os problemas de ciência e compreensão, que dizem respeito à percepção do indivíduo a respeito do objeto da declaração do seu consentimento, que podem decorrer tanto do não acesso ao conteúdo do termo de adesão quanto da sua não compreensão¹⁷⁷.

Importa referir, também, que o artigo 7º, incisos VIII e XI, do Marco Civil da Internet, traz regras expressas segundo os quais se consubstanciam em direitos do usuário da internet, respectivamente: ser informado de forma clara e completa sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para as finalidades que estejam especificadas nos contratos de prestação de serviços ou em termos de aplicações de internet; e de consentir de forma expressa sobre coleta, uso, armazenamento e tratamento de seus dados pessoais.

Apesar de o foco do Marco Civil da Internet não ser a proteção de dados, essas disposições foram um passo importante ao delimitar condições mínimas que provedores de conteúdo deveriam passar a adotar, especialmente ao garantir maior clareza aos usuários e delimitar a coleta de dados apenas àqueles essenciais à finalidade para a qual serão utilizados.¹⁷⁸

Contudo, no sistema brasileiro, o dever de informar não decorre unicamente do princípio da transparência (artigo 6º, VI, LGPD), mas, também, é resultante da

¹⁷⁶ LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 204.

¹⁷⁷ SOLOVE, Daniel J. **Introduction: privacy self-management and the consent dilemma**. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/hlr126&div=87&id=&page=>. Acesso em: 18 abr. 2022.

¹⁷⁸ TRANQUILLINI NETO, Aristides. Compliance com a Lei Geral de Proteção de Dados como forma de evitar a Responsabilização civil. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (org.). **Proteção de dados pessoais na sociedade de informação: entre dados e danos**. Indaiatuba: Foco, 2021. p. 241-257. p. 244.

cláusula geral da boa-fé objetiva (artigo 6º, *caput*, LGPD), que orienta toda a disciplina do tratamento de dados, como antes já demonstrado.

O direito à informação, abrigado expressamente pelo art. 5º, XIV, da Constituição Federal, é uma das formas de expressão concreta do Princípio da Transparência, e também corolário do Princípio da Boa-fé Objetiva e do Princípio da Confiança, todos abraçados pelo CDC.¹⁷⁹

A boa-fé objetiva, a partir de sua função integrativa, importa na criação dos deveres informativos¹⁸⁰ nas relações de tratamento de dados, o que reforça a necessidade de que as explicações sejam completas, corretas e sem qualquer intenção de abusividade sobre a forma de coleta, utilização e destino dos dados pessoais, pois é absolutamente indispensável para amparar o consentimento válido, ou seja, verdadeiramente livre, informado e inequívoco.

O dever de informar, que antecedente ao consentimento para o tratamento de dados pessoais, corresponde a um dever anexo de proteção. Os bens jurídicos protegidos são a higidez da manifestação de vontade e a confiança, que possibilita não apenas acalentar expectativas legítimas, mas, igualmente, avaliar riscos¹⁸¹.

Conforme explica Judith Martins-Costa¹⁸², na concretização dos deveres informativos, antes de mais, há que ter extrema atenção aos critérios das fases da relação em que esse dever se aloca, dos campos em que atua, do tipo de relação jurídica em causa e do interesse envolvido (prestar ou proteger). E aqui se identifica, portanto, a verdadeira importância da informação prévia ao consentimento como base de legitimação para o tratamento de dados, porque somente ela, quando adequadamente fornecida, poderá validar a manifestação de vontade que autorizará o tratamento de dados.

A LGPD não elencou os itens mínimos que devem ser informados pelos agentes de tratamento de dados, como o fez o RGPD, no capítulo III, artigos 13, 14 e 15, que assim especificou o mínimo a ser informado aos titulares dos dados antes do seu consentimento: 1. a identidade e os contatos do responsável pelo tratamento e, se for o caso, do seu representante; 2. os contatos do encarregado da proteção de

¹⁷⁹ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 582.

¹⁸⁰ Conforme Judith Martins-Costa, os deveres informativos podem derivar da lei, do contrato ou do princípio da boa-fé. *Ibid.*, p. 578.

¹⁸¹ *Ibid.*, p. 582.

¹⁸² *Ibid.*, p. 586.

dados; 3. as finalidades do tratamento a que os dados pessoais se destinam, bem como fundamento jurídico para o tratamento; 4. se o tratamento dos dados se basear no legítimo interesse, isso deve ser informado e detalhado o legítimo interesse no caso; 5. os destinatários ou categorias de destinatários dos dados pessoais, se houver; 6. se for caso, a transferência internacional dos dados pessoais, informando se o país tem um nível adequado de proteção de dados; 7. o prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo; 8. a existência do direito de solicitar ao responsável pelo tratamento e no que disser respeito ao titular dos dados, ou do direito de esse se opor ao tratamento, bem como do direito à portabilidade dos dados; 9. se o tratamento dos dados se basear no legítimo interesse, a existência do direito de revogar consentimento a qualquer tempo, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; 10. o direito de apresentar reclamação a uma autoridade de controle; 11. se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; 12. a existência de decisões automatizadas, incluindo a definição de perfis, as informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular de dados.

Judith Martins-Costa¹⁸³ classificou o dever de informar a partir de elementos fático-subjetivos, relacionados às partes envolvidas, como também a partir de elementos normativos, que correspondem à natureza contratual ou não desse dever de informar; e, por fim, os elementos fáticos objetivos, como, por exemplo, a natureza do negócio. Cumpre destacar duas das classificações elencadas pela autora, que auxiliam no esclarecimento do importante papel do dever de informação decorrente da cláusula geral da boa-fé nas relações de tratamento de dados: classificação quanto à intensidade e classificação quanto à finalidade.

Quanto à intensidade, o dever de informação pode ser classificado em dever de informação em sentido estrito, dever de conselho e dever de esclarecimento¹⁸⁴. O dever de informação em sentido estrito é aquele que tem por objeto a transmissão objetiva de uma informação e comunicação de fatos. Uma das partes tem o dever de

¹⁸³ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 587.

¹⁸⁴ *Ibid.*, p. 589.

transmiti-la à parte contrária, que a processará e a utilizará em sua conveniência. O dever de conselho, ou de recomendação, importa informar e emitir um juízo de valor indicativo de um modo de agir, que pode ou não ser acolhido pela outra parte na tomada de decisão¹⁸⁵.

O dever de esclarecimento é o dever de informação em que há também o processamento da mesma por parte do seu devedor, para facilitar o seu entendimento pelo credor da mesma. Tem por objetivo não apenas transmiti-la, mas cooperar com o credor de modo que o transmissor proporcione ao receptor a compreensão do significado da mensagem transmitida, valendo-se de clareza na transmissão do conteúdo transmitido. Não só informa, mas traduz em linguagem simples, o que isso quer dizer. Clóvis do Couto e Silva¹⁸⁶, ao analisar esse dever, afirma que esse se dirige ao outro participante da relação, para tornar clara certa circunstância de que a parte contrária tenha conhecimento imperfeito, insuficiente, errôneo, ou, ainda, ignore totalmente. É justamente esse dever de informação, entendido como dever de esclarecimento, o recomendado pela cláusula geral da boa-fé nas relações de tratamento de dados.

Quanto à finalidade do dever de informar, esse pode destinar-se ao conteúdo do contrato ou para o controle do comportamento das partes. Assim, há o dever de informar sobre o objeto do contrato; dever de informar sobre as intenções no contrato; dever de aviso, cuidado e alerta; e dever de notificação.

O dever de informar as próprias intenções no contrato tem por objetivo combater os problemas de ruptura injustificada das negociações, decorrentes da liberdade das partes em assumir ou não as obrigações que resultaram no contrato¹⁸⁷. Essa classificação não parece importar para as relações de tratamento de dados.

O dever de informar sobre o objeto do contrato tem por objetivo transmitir informações necessárias à sua boa formação e deixar o seu conteúdo mais transparente entre as partes. Compreende o esclarecimento das obrigações que serão assumidas pelas partes, as informações sobre as características em termos de quantidade, qualidade, preço, objeto das prestações e todas aquelas que sejam decisivas para a decisão de contratar (ou consentir). Esse dever de informar tem por

¹⁸⁵ SILVA, Eva Sónia Moreira. **Da responsabilidade pré-contratual por violação dos deveres de informação**. Coimbra: Almedina, 2003. p. 68.

¹⁸⁶ SILVA, Clóvis V. do Couto e. **A obrigação como processo**. Rio de Janeiro: FGV, 2006. p. 93.

¹⁸⁷ TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no direito civil**. São Paulo: Almedina, 2020. p. 248.

finalidade a tutela da liberdade de estipular o seu conteúdo, sendo de fundamental importância para a redução do estado de informação assimétrica decorrente das relações de tratamento de dados.

Assim como informar sobre o conteúdo do tratamento de dados, o dever de informar, que se constitui em aviso, cuidado e alerta, também se amolda às relações regidas pela LGPD. É um dever de informação que se constitui em dever de proteção e importa na obrigação de informação completa sobre os perigos e os riscos da emissão do consentimento. O dever de aviso chama a atenção do usuário acerca dos eventuais perigos decorrentes da má utilização dos seus dados, por exemplo.

Portanto, fornecer informações aos titulares dos dados antes de obter seu consentimento é essencial para capacitá-los a tomar decisões embasadas e oportunizar que entendam com o que estão concordando e, também, possam exercer o seu direito de retirar o seu consentimento, se assim o decidirem. Esse dever de informação, embora consignado na lei, é consectário lógico do dever geral de conduta exigido pela cláusula geral da boa-fé.

En el momento de recabar los datos debe enunciarse la finalidad del tratamiento y ponderar si los datos recogidos son excesivos respecto de dicha finalidad. Por ejemplo, se solicitan datos para que los alumnos participen en salidas culturales o pueden beneficiarse de descuentos en librerías. Un consentimiento para una finalidad muy genérica no sería válido. Si se considerara que los datos son excesivos, a pesar de exigir consentimiento, no sería válido para el tratamiento de los datos. Tampoco sería válido para el tratamiento un consentimiento en blanco, sin especificar la finalidad concreta del tratamiento.¹⁸⁸

Assim, a informação cumpre papel decisivo em matéria de proteção de dados. É com base nela que o titular dos dados manifesta sua vontade ao consentir para que as suas informações sejam utilizadas e/ou tratadas. Quanto mais qualificada a informação, menores as possibilidades de erro e de celebração de vínculos dos quais os titulares venham a se arrepender posteriormente. Diz-se qualificada a informação porque ela precisa ser clara, acessível e em linguagem adequada ao público que consentirá; portanto, aquele que informa deve observar a boa-fé ao fornecer as informações ao titular; só assim criar-se-ão condições ótimas entre as partes e estará

¹⁸⁸ SOLANA, Mònica Vilasau. Menores. Centros docentes y datos: decisiones conflictivas. In: MALLÉN, Beatriz Tomáz; MAHAMUT, Rosario Garcia; CHULVI, Cristina Pauner. **Las cláusulas específicas del Reglamento General de Protección de Datos en el Ordenameto Jurídico Español**. Valencia: Tirant lo Blanch, 2021. p. 179-212. p. 183.

assegurada a integridade, exatidão e a liberdade do consentimento emitido, livrando-o de vícios.

Indiscutível a relevância da informação para que se tenha um consentimento qualificado; contudo é preciso analisar o cenário no qual essa informação deve ser prestada e avaliar como a informação será transferida ao titular dos dados por aqueles que detêm seu domínio e que usarão e tratarão os dados pessoais, ou seja, os controladores.

Na sequência do trabalho, buscar-se-á refletir sobre a assimetria no domínio das informações que devem ser prestadas ao titular dos dados e que garantiriam um consentimento livre, informado e inequívoco, bem como alternativas de preservação do principal fundamento da legislação protetiva de dados: a autodeterminação informativa.

3.2 ASSIMETRIA INFORMACIONAL NAS RELAÇÕES DE TRATAMENTO DE DADOS E O MITO DO CONSENTIMENTO

O consentimento, ainda que não seja a única base de legitimação para o tratamento de dados, é o instrumento que empodera o titular a exercer o domínio sobre as suas informações, ou seja, a necessidade de consentimento impõe que os dados de uma pessoa somente serão processados quando, como e para os fins que ela autoriza, a partir das informações recebidas dos agentes de tratamento de dados.

O consentimento e a autodeterminação informativa estão intimamente ligados: se o direito de proteção de dados serve para proteger liberdades individuais, é natural que cada titular decida o que se fará com os seus dados e informações e que a legislação ampare a sua decisão.

Y el consentimiento cumple, a su vez, una importante función de adaptación contextual. El valor que damos a la privacidad puede oscilar mucho según las circunstancias y los entornos en que actuamos, como también lo hacen nuestras preferencias y deseos sobre el uso que otros puedan hacer de nuestros datos. De ahí que la ley no imponga de forma taxativa y para cualquier contexto todas las condiciones del tratamiento, sino que admita cierta dosis de flexibilidad y permita modular el régimen legal de acuerdo a la voluntad del titular de los datos: debemos ser nosotros, al fin y al cabo,

*quienes decidamos sobre nuestra información. Hasta aquí, en teoría, todo en orden; la realidad, sin embargo, no es tan simple.*¹⁸⁹

Para autores como Bart W. Schermer, Bart Custers e Simone Van der Hof¹⁹⁰, da Universidade de Leiden, é necessário que o consentimento seja dado por um sujeito com entendimento substancial acerca das consequências daquela manifestação de vontade, além de que essa manifestação seja intencional, livre de coerção, e que autorize um processo específico.

Ocorre que:

Embora o exercício do direito de controle do indivíduo sobre as suas informações consista em uma dimensão importante da disciplina de proteção de dados pessoais, a sua forma de implementação é bastante complexa, num contexto caracterizado pela sociedade de massas e pela constante inovação tecnológica, em que nem sempre é possível ao indivíduo dimensionar as consequências futuras de uma disposição em relação aos seus dados. Especialmente nas relações em que há uma assimetria de poder e de informação, como é o caso da relação trabalhista e da relação de consumo, questiona-se se de fato o consentimento é dado de forma livre e informada ou se a autonomia não passaria de uma mera ficção. Dessa forma, para que o tratamento de dados pessoais baseado no consentimento seja legítimo, é preciso que o controlador se certifique de que o consentimento foi dado de forma livre e informada, resguardando não apenas a liberdade de escolha meramente formal do indivíduo, mas efetivamente a sua liberdade material.¹⁹¹

Relações assimétricas, marcadas pelo desequilíbrio informacional, não são uma novidade para o direito. O direito do consumidor, por exemplo, campo que muito se identifica e, inúmeras vezes, se conecta à disciplina de proteção dos dados pessoais, surgiu justamente para corrigir a desigualdade do consumidor diante dos prestadores e fornecedores de produtos e serviços¹⁹².

¹⁸⁹ LALANA, Angel Daniel; SORO, José Felix Muñoz. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. *In*: VALERO TORRIJOS, Julian. **La protección de datos personales en internet ante la innovación tecnológica**. Riesgos, amenazas y respuestas desde la perspectiva jurídica. Navarra: Aranzadi, 2013. p. 153-196. p. 155.

¹⁹⁰ SCHERMER, B. W.; CUSTERS, Bart; HOF, S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). **Ethics and Information Technology**. DOI: 10.1007/s10676-014-9343-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418. Acesso em: 21 fev. 2022.

¹⁹¹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 65.

¹⁹² MIRAGEM, Bruno. **Direito do consumidor**: fundamentos do direito do consumidor: direito material e processual do consumidor; proteção administrativa do consumidor, direito penal do consumidor. São Paulo: Revista dos Tribunais, 2008. p. 23.

Segundo Bruno Bioni¹⁹³, o ramo consumerista, ao elencar o direito à segurança, à informação, à escolha de bens alternativos e com preços justos e o direito de ser ouvido na formulação de políticas públicas, procura corrigir falhas de um mercado capazes de lesar essa parte mais frágil; cumprindo o direito do consumidor, “[...] uma missão protetiva em favor do elo mais frágil da cadeia econômica que tende a se submeter ao poder de controle dos titulares dos bens de produção”¹⁹⁴.

Em cena, portanto, o paradigma protetivo, que reconhece a posição de *vulnerabilidade* de certos grupos, dedicando-lhes normas especiais para tutelá-los na exata medida de suas fraquezas. Ainda, etimologia da palavra vulnerabilidade – em latim: *vulnus* (machucado ou ferida) – significa a potencialidade de o sujeito, ora identificado como vulnerável, ser mais suscetível de sofrer danos. Decorre daí, portanto, a noção de *instrumentalidade* do direito na missão de normas protetivas para dispensar um tratamento desigual aos sujeitos desiguais.¹⁹⁵ (Grifo do autor).

Judith Martins-Costa explica a existência de duas espécies de assimetria: assimetria fática e a assimetria juridicamente presumida. Essa última é a encontrada nos regimes especiais, em que – para assegurar condições de relativa igualdade entre os figurantes – a lei interfere diretamente e com maior amplitude no conteúdo dos vínculos¹⁹⁶; é o caso da relação de tratamento de dados.

O titular de dados é o sujeito vulnerável e a quem se destina todo o contexto regulatório protetivo da LGPD, e é ele quem deve, mesmo num contexto de indiscutível assimetria informacional, consentir sobre a utilização e tratamento de suas informações, mas, evidentemente, se beneficia da concessão desses dados, num jogo de ganhos e perdas¹⁹⁷.

Alan Westin, em 1970, já dizia que:

O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. Assim, cada indivíduo está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de disposição e comunicação com os

¹⁹³ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 158.

¹⁹⁴ COMPARATO, Fábio Konder. A proteção do consumidor: importante capítulo do Direito Econômico. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (org.). **Coleção doutrinas essenciais**: direito do consumidor – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1. p. 167-186. p. 177.

¹⁹⁵ BIONI, *op. cit.*, p. 159.

¹⁹⁶ MARTINS-COSTA, Judith. A boa-fé no direito privado: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 627.

¹⁹⁷ BIONI, *op. cit.*, p. 145.

outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive.¹⁹⁸ (Tradução nossa).

O direito de autodeterminação pressupõe que as escolhas do indivíduo, de acordo com a sua conveniência, por vezes, justificarão ou a flexibilização do seu âmbito de privacidade, ou a flexibilização aparente (pois o que é privado para um não necessariamente o é para outro). A liberdade de escolha existe e é necessária, porque toda a complexidade humana, reconhecida em uma sociedade plural, faz com que diferentes interesses preponderem nas decisões de cada indivíduo¹⁹⁹.

*Es natural que cada cual decida qué se hace con sus datos, y que la legislación ampare su margen decisorio. El valor que damos a la privacidad puede oscilar mucho según las circunstancias y los entornos en que actuamos, como también lo hacen nuestras preferencias y deseos sobre el uso que otros pueden hacer de nuestros datos.*²⁰⁰

Contudo, a discrepância entre o domínio da informação e as consequências quanto ao uso e ao compartilhamento de dados pessoais, assim como pesquisas sobre decisão comportamental, levantam questões sobre a capacidade dos usuários para otimizar as escolhas em torno da privacidade. Por isso, mostra-se importante a análise da capacidade de escolha individual sobre a concessão de dados pessoais diante do controle informacional daqueles que obtêm esses dados e da regulação que orienta o mercado em busca do equilíbrio entre a tutela da privacidade e a conversão de dados pessoais em experiências.

A própria lógica do *trade-off* dá economia dos dados pessoais é a traiçoeira, portanto frente a tal *arquitectura de escolhas de decisões*, notadamente por essa *idiosincrasia* entre *gratificações imediatas e prejuízos imediatos/distantes*. A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é a posta em xeque por toda essa complexidade em

¹⁹⁸ WESTIN, Alan F. Science, privacy and freedom: issues and proposals for the 1970's. Part I – The current impact of surveillance on privacy. **Columbia Law Review**, n. 6, v. 66, p. 1003-1050, jun. 1966. Disponível em: https://www.jstor.org/stable/1120997?seq=1&cid=pdfreference#references_tab_contents. Acesso em: 29 mar. 2022.

¹⁹⁹ Negar-se a possibilidade de autonomia ou perspectivar-se a autonomia privada por um viés negativo equivaleria a violar uma das dimensões mais valiosas da própria personalidade humana, qual seja, a possibilidade de fazer escolhas, tomar decisões, responsabilizando-se por elas (autodeterminação); sua negação implicaria, ainda, o afastamento da garantia constitucional à liberdade de iniciativa econômica. MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. São Paulo, Marcial Pons, 2019. p. 249.

²⁰⁰ LALANA, Angel Daniel; SORO, José Felix Muñoz. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. In: VALERO TORRIJOS, Julian. **La protección de datos personales en internet ante la innovación tecnológica**. Riesgos, amenazas y respuestas desde la perspectiva jurídica. Navarra: Aranzadi, 2013. p. 153-196. p. 156.

volta do fluxo das informações pessoais. Ele está em uma situação de *vulnerabilidade específica* em meio a uma *relação assimétrica* que salta aos olhos, havendo uma série de evidências empíricas a esse respeito.²⁰¹ (Grifo do autor).

Daniel Solove²⁰² aponta que o controle do titular sobre a sua privacidade enfrenta diversos obstáculos tanto cognitivos quanto estruturais. Os primeiros dizem respeito aos desafios que envolvem a forma através da qual as pessoas tomam decisões, e podem ser sintetizados em problemas de informação e de tomada de decisão distorcida. Os problemas estruturais, por sua vez, dizem respeito à multiplicidade de entes (problema de escala) coletando e usando os dados pessoais, o que dificulta tanto o controle dos dados quanto a previsibilidade do que pode resultar da junção (problema da combinação) de todas as informações que foram fragmentadamente cedidas a cada ente. Por fim, há ainda o problema de avaliação do prejuízo.

Os problemas com informação dizem respeito ao fato de que a maioria das pessoas não leem as políticas de privacidade²⁰³. De fato, muitas sequer tomam conhecimento de que há uma política de privacidade (o ato de correr a barra de rolagem é praticamente automático). A razão para tanto é comumente ligada ao tamanho dos termos e à complexidade do conteúdo, de modo que, mesmo as que leem muitas vezes, não compreendem os termos e aqui se identifica com muita clareza a assimetria informacional que domina a temática do tratamento de dados pessoais.

Há um claro embate nesse sentido, entre o dever de prestar todas as informações e a necessidade de concisão da informação prestada para que seja lida e compreendida, para essa informação ser suficiente para amparar um válido consentimento.

Nesse jogo de ganhos e perdas, o ser humano tende a procurar uma “zona de conforto” para não se culpar em torno do prejuízo por ele suportado. Trata-se das chamadas *dissonâncias cognitivas* em que o sujeito procura um alívio para assimetricamente compensar um desconforto. É nesse contexto que se insere o denominado “paradoxo da privacidade”. Em que pese as pessoas valorarem a proteção de seus dados pessoais, elas empreendem ações

²⁰¹ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 145.

²⁰² SOLOVE, Daniel J. **Introduction**: privacy self-management and the consent dilemma. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/hlr126&div=87&id=&page=>. Acesso em: 18 abr. 2022.

²⁰³ *Ibid.*

dissonantes a tal preço. As condutas contradizem o que elas estimam, surgindo uma relação de incoerência entre o que elas praticam e o que elas enxergam como ideal.²⁰⁴ (Grifo do autor).

Bruno Bioni²⁰⁵ apresenta quatro estudos que demonstram que os indivíduos raramente têm plena consciência sobre os riscos e ameaças aos seus dados pessoais, os quais serão brevemente sintetizados a seguir.

O estudo denominado *Mental Models*, das Universidades de Stanford e Carnegie Mellon, investigou os modelos mentais dos usuários a respeito do funcionamento da publicidade comportamental no ambiente *on-line*²⁰⁶ e concluiu que uma parcela ínfima dos usuários teria conhecimento técnico para autodeterminar os seus dados pessoais nesse cenário de coleta.

As conclusões dessa pesquisa empírica trazem uma série de argumentos que convergem para a conclusão de que os usuários não estão capacitados para tomar decisões informadas no tocante ao controle de seus dados pessoais, como: i) falta de conhecimento no que diz respeito ao funcionamento das tecnologias de coleta dos dados pessoais e da sua inserção no contexto da publicidade comportamental, que determina o fluxo de suas informações em meio aos diversos atores que operam esse mercado; ii) idiosincrasia do *trade-off* da economia informacional, uma vez que o controle aos dados pessoais é visto, respectivamente, como um benefício imediato e uma perda mediata, o que o desvaloriza nesse processo de tomada de decisão; iii) em último lugar, porque os próprios usuários discordam da lógica econômica pela qual eles teriam que despende uma quantia para assegurar o seu direito à privacidade, enxergando tal dinâmica como uma extorsão.

Em poucas palavras, tal estudo empírico sublinha a posição de vulnerabilidade dos cidadãos em exercer o controle de seus dados pessoais, o que perpassa desde uma assimetria informacional até a própria estruturação dos modelos de negócio que se divorciam das expectativas de privacidade dos usuários.²⁰⁷

O segundo estudo empírico apresentado por Bruno Bioni, que é complementar ao primeiro, no sentido de confirmar a assimetria informacional e a vulnerabilidade dos usuários no controle dos seus dados pessoais, foi realizado pela Universidade de Berkeley, da Califórnia²⁰⁸, que analisou tecnologias utilizadas como elemento neutralizador da capacidade dos usuários em controlar as suas informações pessoais.

²⁰⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 145.

²⁰⁵ *Ibid.*, p. 145-165. Faz um apanhado dos estudos sobre o assunto.

²⁰⁶ CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs na Behaviors: Internet User's Understanding of Behavioral Advertising *apud* BIONI, *op. cit.*, p. 146.

²⁰⁷ BIONI, *op. cit.*, p. 148.

²⁰⁸ HOOFNAGLE, Chris Jay; URBAN, Jennifer M.; LI, Su. Privacy and modern advertising: most US internet users want 'do not track' to stop collection of data about their online activities. In:

Tais tecnologias empregam liquidez a um monitoramento contínuo e permanente dos usuários, acuando-os em meio a uma “corrida armamentista tecnológica” quem valida as suas escolhas para que as suas informações pessoais não sejam coletadas.²⁰⁹

Da Faculdade de Comunicação Annenberg, da Universidade da Pensilvânia²¹⁰, é a terceira pesquisa apresentada pelo autor, que contrapõe a conclusão das anteriores de que os consumidores estariam confortáveis e conscientes da troca de seus dados pessoais por serviços e produtos (*trade-off*), afirmando que a grande maioria das pessoas é conivente com a lógica da economia dos dados pessoais por estarem com ela resignadas, ou seja, elas teriam simplesmente acatado algo que é indesejável, mas, ao mesmo tempo, inevitável²¹¹.

Trata-se do paradoxo da privacidade que, no caso da proteção de dados pessoais, residiria na incoerência de os seus titulares anuírem com um trânsito contínuo de suas informações pessoais, ainda que eles estimassem a sua proteção.

[...]

O estudo conclui que os consumidores estão resignados com essa dinâmica. No fundo, eles desejam ter um maior controle sobre o uso de seus dados pessoais, reconhecendo, ao mesmo tempo, que têm pouca gerência sobre tal situação.

[...]

Em suma, o problema é estrutural. Parafraseando o título da pesquisa sobre análise, trata-se de uma falácia imposta pelo *trade-off* da economia de dados pessoais. Mistifica-se a capacidade do cidadão de autoproteção de seus dados pessoais, notadamente por sua pseudo autonomia em controlar as suas informações.

Em conclusão, esse terceiro estudo empírico é complementar aos anteriores, uma vez que ele situa, de forma estrutural, o problema da autodeterminação informacional frente à própria dinâmica da economia de dados pessoais.²¹²

A pesquisa da Universidade de Bochum (Alemanha)²¹³ é a quarta relatada por Bruno Bioni e analisou as notificações, chamadas de aviso de *cookies*, “[...]”

AMSTERDAM PRIVACY CONFERENCE, 2012. HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathan; WAMBACH, Dietrich James; AYENSON, Mika. Behavioral advertising: the offer you cannot refuse. *Harvard Law & Policy Review*, v. 6, p. 273, Aug. 2012); UC Berkeley Public Law Research Paper. 2137601, p. 273-296 *apud* BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 151.

²⁰⁹ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 151.

²¹⁰ TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. *The tradeoff fallacy: how marketers are misrepresenting and opening them up to exploitation* *apud* BIONI, *op. cit.*, p. 152.

²¹¹ BIONI, *op. cit.*, p. 154.

²¹² *Ibid.*, p. 155.

²¹³ UTZ, Christine; DEGELING, Martin; FAHL, Sascha; SCHAUB, Florian; HOLZ, Thorsten. (Un)informed consent: studying GDPR consent notices in the field. In: 2019 ACM SIGSAC Conference on Computer and Communications Security (CCs'19), November 11-15, 2019, London, United Kingdom. ACM, New York, NY, USA *apud* BIONI, *op. cit.*, p. 156.

promovem, de fato, transparência acerca das práticas de tratamento de dados pessoais pelas plataformas e, em última análise, auxiliam na obtenção de um consentimento válido por parte dos usuários”²¹⁴.

Esse último estudo concluiu que:

Em síntese, tão importante quanto criar uma tecnologia voltada a reduzir a assimetria de informação e de poder é verificar se a sua arquitetura é responsiva a tais objetivos. As variáveis consideradas por este último estudo empírico evidenciam o quão traiçoeiro pode ser o seu design a ponto de manipular a decisão tomada pelo cidadão com relação aos seus dados.²¹⁵

No cenário informático, os indivíduos não são apenas consumidores de informação, mas produtores de um volume imenso de dados pessoais que impulsionam a atividade econômica a partir da formação dos chamados perfis comportamentais, que antecipam, favorecem e induzem preferências, escolhas e decisões sobre consumo.

As pessoas realizam diariamente transações e disponibilizam seus dados pessoais nas redes, a partir de um consentimento que, na imensa maioria das vezes, não é antecedido da assimilação da informação sobre como esses dados serão usados e tratados. E isso decorre da própria lógica do espaço digital, que, a partir de uma arquitetura para aquisição do consentimento, admite uma “falsa escolha” como manifestação de vontade, apta a amparar o tratamento de dados pessoais, ficando o verdadeiro objetivo desse consentimento, que é a proteção da privacidade, à margem dessa relação.

Percebe-se, pois, um *traço vulnerante peculiar* sob diversas perspectivas: informacional, técnica e econômica. Isso é o saldo de uma assimetria, igualmente própria do mercado informacional, que agrava a condição de vulnerável do cidadão. Há uma sobreposição de fraquezas, na medida em que aquele sujeito vulnerável é inserido em um novo contexto: o do mercado informacional.²¹⁶

Nesse contexto, ainda que o consentimento deva ser precedido de informações claras, precisas e facilmente acessíveis, e é fundamental que o seja, sob pena de não ser suporte suficiente para o tratamento de dados, não há dúvidas sobre a marcante

²¹⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 156.

²¹⁵ *Ibid.*, p. 157.

²¹⁶ *Ibid.*, p. 161.

assimetria informacional presente nas relações de tratamento de dados, seja pela própria complexidade dos sistemas de informação, seja pelas limitações cognitivas dos indivíduos que lançam seus dados nas redes.

Contudo, diante da irretroatividade do cenário de hiperconectividade, que inúmeros benefícios trouxe para a vida em sociedade, é necessário equacionar o direito à autodeterminação informativa, expressa através do consentimento, e o domínio da informação por parte dos controladores de dados.

Em outras palavras, embora esse processo tenha sido marcado por expressiva assimetria informacional, o fato é que os dados pessoais e a privacidade tornaram-se o motor do que se convencionou denominar da *data driven economy*, deveras marcada pelo suposto compartilhamento e pela capacidade de auto-geração de riqueza a partir de ferramentas como o emprego da inteligência artificial e uso de algoritmos, ou seja, um modelo de desenvolvimento econômico construído pelo poder informacional derivado, baseado na possibilidade de geração exponencial de riqueza e proliferação de situações de poder por parte daqueles que possuem o controle sobre dados qualitativamente relevantes para o redimensionamento da privacidade. A despeito dos ganhos proporcionados pela economia dirigida por dados na reformulação de políticas públicas e do modelo de desenvolvimento, a reflexão em torno da redução da esfera de proteção da privacidade e dos dados pessoais exige maior recontextualização.²¹⁷

Nesse contexto de evidente assimetria de informação, mas também no qual o titular dos dados deve ter seu direito à autodeterminação informacional assegurado e protegido pelo complexo regulatório desenvolvido pelo Estado, é que se destaca a relevância da cláusula geral da boa-fé, como impositiva de condutas probas, leais e honestas, do direito de acesso à informação e da execução de boas práticas, para equacionar os benefícios econômicos da circulação de dados pessoais e os riscos de danos à privacidade dos seus titulares, em especial quando a base legal que autoriza o seu uso é o consentimento.

3.3 DEVERES DE CONDUTA DOS AGENTES DE TRATAMENTO DE DADOS: EM BUSCA DA MITIGAÇÃO DA ASSIMETRIA INFORMACIONAL

A partir da compreensão de que a disciplina da proteção de dados tem como um de seus principais objetivos a proteção da autodeterminação informativa e que

²¹⁷ SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço: a *accountability* como fundamento da *lex privacy***. 219 f. Tese (Doutorado em Direito) – Curso de Direito, Universidade de Brasília, Brasília, 2019. p. 12.

consentimento é o instrumento de execução desse direito, bem como que, apesar da significativa e já demonstrada assimetria informacional presente no espaço digital, a informação clara, adequada e acessível é imprescindível para amparar o consentimento com todas as suas qualificadoras cumpre buscar meios, instrumentos e diretrizes para superar, ou, no mínimo, mitigar, a constrangedora incompatibilidade entre o direito dos titulares decidirem sobre os rumos de suas informações e o potencial abuso desses dados por aqueles que os adquirem no exercício de suas atividades.

De fato, um sistema de proteção individual de dados pessoais parece não ser suficiente para a proteção da privacidade. São crescentes os impedimentos para que um indivíduo normal controle suas informações em um contexto globalizado, no qual as técnicas de intercâmbio, formação de perfis automáticos e mineração de dados são cada vez mais sofisticadas.

Já na própria decisão do Tribunal alemão, que reconhecidamente apresentou a autodeterminação informativa como um viés dos direitos da personalidade, havia referência à necessidade de garantias para que o consentimento, como expressão desse direito, não se desse de forma viciada ou em ambiente incapaz de lhe alcançar a característica de livre expressão.

Apesar da concepção primariamente procedimental do direito à autodeterminação informativa, em sua fundamentação da sentença referente ao recenseamento populacional, o Tribunal Constitucional forneceu também elementos substanciais, como os riscos concretos à liberdade do indivíduo e limites substanciais do processamento de informações, que recaem em uma relação de tensão com o a noção de poder de decisão: atenção entre o controle de dados e riscos da informação.

A questão a respeito de como o quadro jurídico para a proteção individual pode ser realizado, no tocante ao tratamento de dados em informações, continua a ser cunhada pela ambivalência evidenciada pela sentença do Tribunal relativa ao recenseamento: por um lado, há a abordagem de proteção procedimental, isto é, que se orienta pela decisão do interessado e revela um caráter individual; por outro, há a concepção que se fixa nos riscos decorrentes do uso das informações, aplicando conceitos substanciais exigindo limites em determinados casos. Trata-se de tensão entre o conceito puramente formal de privacidade, em que apenas a decisão e a vontade do interessado têm um papel a desempenhar, e outro conceito, mais objetivo, no qual a situação objetiva de risco individual também ganha importância.²¹⁸

²¹⁸ MALLMANN, Otto. Zielfunktionen des Datenschutzes. Schutz der privatsphäre. Korrekte Information. Frankfurt am Main: Luchterland, 1995 *apud* MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 18 jun. 2021.

De fato, a compreensão de que o Estado – ao colocar sobre o indivíduo a responsabilidade pela defesa de seus dados pessoais, de usar seu direito à autodeterminação informacional frente a toda a complexidade do tratamento de dados pessoais na atualidade – em certa medida se exime de sua função de tutelar a personalidade por normas específicas, é um ponto de vista possível. No entanto, deve-se levar em conta que não há como permitir que o indivíduo exerça sua autodeterminação se lhe for retirado o poder de decidir sobre seus dados.

Por outro lado, os processadores de dados dependem de um fundamento de legitimação confiável para o tratamento de dados, e tal fundamento de legitimação muitas vezes só pode ser oferecido pelo consentimento. Por isso, parece importante definir como os agentes que tratam dados pessoais devem conduzir esses processos e como a cláusula geral da boa-fé poderia permear todo esse cenário, uma vez que sua presença e exigência certamente geram um contexto de transparência, segurança e confiança para os titulares em relação aos seus dados.

El consentimiento y la información, como mecanismos de protección de la privacidad, resultan en gran medida nociones fraudulentas y, en la práctica, sirven más para facilitar flujos continuos de información que para asegurar la protección de los derechos individuales. Dicho de un modo más suave: sin excluir que las normas de consentimiento puedan operar como es debido (control y adaptación contextual), al menos en áreas muy significativas de actividad su función real es la traslación de responsabilidad: es la persona titular de los datos quien carga con la responsabilidad del tratamiento que autoriza. Y no es difícil ingeniárselas para que autorice casi cualquier cosa. Siempre que cuente formalmente con esa autorización, una empresa puede aprovechar la información personal casi sin límites.²¹⁹

Anteriormente, foram relatados estudos que demonstraram que, além do desequilíbrio informacional fruto do domínio da tecnologia, também aspectos psicológicos condicionam os sujeitos a consentirem com o processamento de seus dados pessoais, daí também é possível extrair a importância da cláusula geral da boa-fé objetiva como orientadora das condutas que envolvem o tratamento de dados e, associada às boas práticas, identificar mecanismos para equilibrar e gerar confiança no fluxo informacional de dados.

²¹⁹ LALANA, Angel Daniel; SORO, José Felix Muñoz. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. In: VALERO TORRIJOS, Julian. **La protección de datos personales en internet ante la innovación tecnológica**. Riesgos, amenazas y respuestas desde la perspectiva jurídica. Navarra: Aranzadi, 2013. p. 153-196. p. 160.

A concepção individualista de proteção, expressa pelo consentimento, talvez não seja suficiente no universo computacional onde as práticas de obtenção e análise maciça de dados banalizam a ideia de processamento consentido²²⁰. Assim, parece importante reconhecer que a proteção da autodeterminação informativa deve ser considerada de forma mais coletiva, exigindo que os agentes de tratamento de dados comportem-se de forma correta, leal e honesta, e garantindo um contexto de confiabilidade e segurança para justificar a aquisição do consentimento que autoriza o tratamento de dados pessoais.

Então, se, de um lado, tem-se os titulares dos dados, a quem devem ser asseguradas informações suficientes para garantir um consentimento livre, informado e inequívoco, como máxima expressão da autodeterminação informativa, de outro, tem-se uma imensa capacidade de processamento e tratamento de dados proporcionada pelos mais diversos sistemas de informação sob o domínio dos agentes de tratamento de dados²²¹, ou seja, controladores e processadores de dados pessoais, aos quais compete o dever de informação, transparência e boa-fé no exercício dessas atividades, para que a assimetria informacional possa, ao menos, ser mitigada.

3.3.1 Quem são os agentes de tratamento de dados?

Antes da busca de sistematização de formas de mitigar a assimetria informacional identificada e detalhada, na tentativa de preservar a autodeterminação informativa cumpre esclarecer quem são os agentes de tratamento a quem esses deveres e orientações se destinam.

Os conceitos de controlador e processador de dados são tão importantes quanto a definição do que são dados pessoais e de suas formas de proteção. A função de controlador e sua interação com o processador de dados e seus deveres de conduta são fundamentais para a compreensão do regime de responsabilidades, bem

²²⁰ LALANA, Angel Daniel; SORO, José Felix Muñoz. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. In: VALERO TORRIJOS, Julian. **La protección de datos personales en internet ante la innovación tecnológica**. Riesgos, amenazas y respuestas desde la perspectiva jurídica. Navarra: Aranzadi, 2013. p. 153-196. p. 154.

²²¹ A figura do “encarregado”, definido como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), conforme o inciso VIII do artigo 5º da LGPD, tem suas atribuições elencadas no artigo 41 da lei e que deverão ser reguladas pela ANPD.

como para que se saiba quais são os padrões comportais e boas práticas que devem ser exigidos para a aquisição do consentimento.

Nos termos da LGPD, *controlador* é toda pessoa física ou jurídica, pública ou privada, a quem compete as decisões referentes ao tratamento de dados pessoais (artigo 5º, VI), e o *processador* é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (artigo 5º, VII).

Dito de outra forma, são eles, controlador e processador, os responsáveis por, intra-relação de tratamento de dados, assegurar aos titulares o direito de acesso à informação, que é a principal matriz de garantias dos titulares de dados pessoais dentro desse contexto. O conhecimento sobre a finalidade, a duração e os responsáveis pelas atividades de processamento e tratamento de dados tornou-se a base de toda a interação realizada no ciberespaço²²².

É do controlador a responsabilidade pelo cumprimento das regras de proteção de dados e a ele compete assegurar os direitos dos titulares. O controlador é, portanto, o ponto de alocação operacional da responsabilidade sob todas as perspectivas: exercício de direitos e responsabilidade civil. A delimitação da atuação do controlador é essencialmente funcional e objetiva traçar um regime de responsabilidade em função da sua influência operacional²²³.

A condição de controlador decorre de uma situação de fato, originada na opção de processar dados pessoais de acordo com a sua decisão e para os seus propósitos. Por isso, uma indicação meramente formal da figura do controlador para cumprir obrigações legais não terá o condão de afastar as verdadeiras premissas fáticas da atividade de tratamento, isto é, em qualquer circunstância será considerado controlador aquele que estiver na condição de tomar as decisões e definir em concreto a finalidade do processamento de dados pessoais.

Mesmo não havendo indicação legal ou contratual de quem seja o controlador, a análise da circunstância em concreto o identificará. Uma das formas de analisar se determinado agente atua como controlador – e, portanto, influencia os meios do

²²² WORKING PARTY 29. **Opinion 3/2010 on the principle of accountability**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 02 maio 2022.

²²³ SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço: a accountability como fundamento da *lex privacy***. 219 f. Tese (Doutorado em Direito) – Curso de Direito, Universidade de Brasília, Brasília, 2019. p. 156.

processamento – decorre da sua capacidade de definir a finalidade mediante a indicação de aspectos técnicos e organizacionais da delegação (natureza dos dados, forma de processamento, período de retenção e terceiros com quem compartilhar). O elemento central para a caracterização do controlador do tratamento de dados é seu poder de gerenciamento e de tomada de decisão no tratamento de dados²²⁴.

Por sua vez, o processador age em nome do controlador, o que significa dizer que atua segundo as hipóteses legais de tratamento a ele aplicadas e por sua delegação, ou seja, se atuar fora das diretrizes estipuladas também poderá ser considerado um controlador (controle conjunto). A condição básica para essa atividade de processamento é que ele atue em nome e segundo as diretrizes do controlador.

Destaca-se que a LGPD considera apenas o controlador e o operador como agentes de tratamento de dados, responsáveis por eventuais danos que vierem a causar aos titulares dos dados (artigo 42), ou seja, o encarregado não é tido como responsável²²⁵ e, portanto, seus deveres não serão aqui analisados.

Definidos quem são os agentes de tratamento de dados e diagnosticada a impossibilidade de se aceitar somente o consentimento como ato garantidor do direito à autodeterminação informativa, é preciso identificar outras ferramentas para mitigar a assimetria informacional nas relações de tratamento de dados.

Nesse sentido, Bruno Bioni afirma que:

O consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócios da economia digital, do que como um meio eficiente para desempenhar a proteção dos dados pessoais. Ele tem sido encarado como uma verdadeira ficção legal deformadora e voraz do teorizado regime legal de proteção de dados pessoais e da sua aplicação na prática. Não seria mais do que uma mistificação, na medida em que não é confrontado com o anotado contexto socioeconômico que estrangula a prometida Liberdade da autodeterminação informacional.

Por tal motivo, é de suma importância frisar essa incompatibilidade do desenho normativo de proteção de dados pessoais e, por conseguinte, pensar como isso pode ser absorvido para fins de reflexão e reajustes do ponto de vista de uma (nova) estratégia regulatória.

Mais do que garantir, artificialmente, diversos qualificadores para o consentimento, devem-se buscar, sobretudo, outras ferramentas regulatórias para equalizar a referenciada assimetria do mercado informacional, redesenhando a sua dinâmica de poder. Esse é o maior desafio para se propiciar ao cidadão um melhor controle de seus dados – uma verdadeira

²²⁴ LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 222.

²²⁵ *Ibid.*, p. 223.

autonomia para, com o perdão de ser prolixo, a autodeterminar as suas informações pessoais.
Deve-se, contudo e concomitantemente, pensar em disposições normativas complementares que interfiram no próprio fluxo informacional, não deixando, apenas, sobre os ombros dos titulares dos dados pessoais, o fardo normativo da proteção de dados pessoais.²²⁶

3.3.2 Obrigações legais dos agentes de tratamento de dados e deveres decorrentes da cláusula geral da boa-fé objetiva no tratamento de dados pessoais

Identificado o papel central do controlador no domínio das informações que antecedem o consentimento, como base legal, para o tratamento de dados pessoais e tendo ele o poder de gerenciamento e de tomada de decisão sobre as estruturas que precedem a coleta de dados, bem como o uso e o destino que se dará para os mesmos, parece importante destacar algumas obrigações legais que, em conjunto com os deveres anexos decorrentes da cláusula geral da boa-fé objetiva, auxiliam na mitigação da assimetria informacional já reconhecida como existente nessas relações jurídicas.

O artigo 50 da LGPD prevê a possibilidade de os controladores e operadores adotarem

[...] regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança ou os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

E, nos termos do parágrafo primeiro do mesmo artigo, impõe-se que,

[...] ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Entende-se por Código de Boas Práticas os documentos normativos internos das empresas ou associações cujo objeto é adequar as práticas da empresa ou da

²²⁶ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 163-164.

associação à lei de proteção de dados, esclarecendo as peculiaridades do tratamento dos dados daqueles que aderirem ao tratamento mediante regras ou padrões específicos que permitam harmonizar os tratamentos de dados realizados, bem como facilitar o exercício dos direitos assegurados aos sujeitos²²⁷.

A revogada Dir. 95/46/CE disciplinou os denominados códigos de boas práticas em seu artigo 27, no qual estabelecia que as associações e outras organizações representativas de determinado setor poderiam estabelecer normas ontológicas para estabelecer um padrão ético e leal para o tratamento de dados, sujeitas à apreciação da Autoridade de Proteção de Dados²²⁸.

Nos artigos 46 e 47 da LGPD estão previstos o dever de adotar medidas de segurança e o dever de sigilo, nos seguintes termos:

Artigo 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.

§ 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.

Artigo 47 – Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Esses deveres estão presentes em diversos modelos regulatórios de proteção de dados, como no artigo 17 da Dir. 95/46/CE e no artigo 32 do RGPD. Nos termos do RGPD, o dever de adotar medidas de segurança importa em:

Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante

²²⁷ LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 228.

²²⁸ UNIÃO EUROPEIA. Diretiva 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. **Jornal Oficial da União Europeia**, Estrasburgo, 24 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 20 maio 2022.

aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

- a. a pseudonimização e a cifragem dos dados pessoais;
- b. a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- c. a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma adequada no caso de um incidente físico ou técnico;
- d. um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.²²⁹

A segurança é um conceito dinâmico e relacional, portanto, deve acompanhar os avanços tecnológicos²³⁰; por isso que, em todos os documentos nos quais o princípio da segurança está previsto, não se menciona especificamente quais as medidas necessárias a serem implementadas, mas se utiliza uma recomendação genérica, porque essas medidas são definidas pelo estado da arte no campo da tecnologia e da informática, levando em consideração a natureza dos dados e características específicas do tratamento²³¹.

O dever de segurança existe antes mesmo de realizado o tratamento e deve permanecer durante todo o período em que o tratamento se realiza, bem como após a sua execução. Nesse sentido é a disposição do § 2º do artigo 46 e artigo 47 da LGPD, acima transcritos.

O dever de notificação está previsto no artigo 48 da LGPD e determina que “[...] o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares”. Esse dever pressupõe a existência de uma entidade de controle e fiscalização do cumprimento das regras relacionadas à proteção de dados pessoais. No Brasil, trata-se da Autoridade Nacional de Proteção de Dados (ANPD).

Esse dever impõe aos responsáveis do tratamento de dados informarem à ANPD a ocorrência de eventos que comprometam a segurança e coloquem em risco os dados pessoais que estão sob sua tutela.

²²⁹ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

²³⁰ FINOCCHIARO, Giusella. *Privacy e protezione dei dati personali: disciplina e strumenti operativi*. Bolonha: Zanichelli, 2012. p. 251 *apud* LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020. p. 233.

²³¹ LIMA, *op. cit.*, p. 233.

O artigo 35 do RGPD tem dispositivo similar, mas com conteúdo mais extenso, e prevê que, quando um determinado tipo de tratamento implicar elevado risco para os direitos e liberdades das pessoas, seu responsável deve, antes de iniciar o tratamento, apresentar uma avaliação de impacto das operações sobre a proteção de dados pessoais.

O dever de notificação de ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares dos dados, assim como o dever de notificar novas tecnologias potencialmente danosas, vão ao encontro dos princípios de segurança, prevenção e *accountability*, previstos no artigo 6º, incisos VII, VIII e X da LGPD.

Os deveres legais impostos pela Lei Geral de Proteção de Dados aos agentes de tratamento, também deveres decorrentes da boa-fé objetiva, em comunhão com o princípio da transparência, são suficientes para exigência de condutas protetivas dos dados pessoais.

Já se disse, mas importa lembrar, nas palavras do Professor Ricardo Lupion,

[...] que a boa-fé objetiva representa o dever de agir de acordo com os padrões socialmente reconhecidos de lisura e lealdade. São esses padrões que traduzem confiança necessária à vida de relação e ao intercâmbio de bens e serviços. Consequentemente é dever de cada parte agir de forma a não defraudar a confiança da contraparte, indispensável para a tutela da segurança jurídica, para a garantia da realização das expectativas legítimas das partes.²³²

A inclusão da cláusula geral da boa-fé objetiva na legislação que protege a privacidade dos dados traz para dentro dessas relações todas as funções dela decorrentes. Sendo assim, os deveres de conduta, oriundos de sua faceta integrativa, também precisam ser observados pelas partes, em especial pelos controladores dos dados, que devem pautar seus procedimentos em fundamentos de lealdade, honestidade e ética.

A boa-fé objetiva está ligada à ideia de modelo de conduta social, segundo o qual cada parte contratante deve ajustar sua conduta ao parâmetro (modelo) legitimamente esperado para aquele caso, agindo com correção, lealdade, probidade e mútua confiança.²³³

²³² GARCIA, Ricardo Lupion. **Boa-fé objetiva nos contratos empresariais**: contornos dogmáticos dos deveres de conduta. Porto Alegre: Livraria do Advogado, 2011. p. 50.

²³³ BLUM, Rita Peixoto Ferreira. Boa-fé objetiva. **Revista de Marketing Industrial**, São Paulo: Instituto de Marketing Industrial, a. 9, n. 22, p. 70-75, 2003. p. 72.

Os deveres instrumentais decorrentes da boa-fé não raro se interligam entre si e, também, com os deveres legais que orientam a disciplina de tratamento de dados, como os deveres de segurança, boas práticas, informação, notificação etc.

O dever de informação e transparência, acima bastante explicado, segundo Judith Martins-Costa, por vezes se subsume ao dever de lealdade. A ligação é efetivamente estreita, pois o dever de lealdade engloba o de veracidade, mas vai além, pois lealdade é mais do que veracidade: é contribuir, positivamente, com o interesse alheio, daí a importância daqueles que são responsáveis pelo tratamento de dados pessoais de incorporarem na sua estrutura padrões de conduta ancorados na boa-fé, porque a eles compete, também, proteger a privacidade dos seus usuários²³⁴, além de que os impedem de criar dificuldades e armadilhas nesse processo. Essa é a ideia de boa-fé, como lealdade.

Quem é ético, não mente: fala a verdade, informa. Como a facilidade de acesso a informações, há transparência. Onde esta houver, reduzem-se as margens de manobra para o comportamento oportunista. Os efeitos do aumento do nível de informação no caso concreto fazem com que se tenha a impressão de que esse apelou à ética, que seria a situação em que alguém, de boa vontade, revelaria voluntariamente determinadas informações. O princípio da boa-fé atua, portanto, como um calibrador do nível de informação ao caso concreto: quando for necessário aumentar o nível de informação em determinada relação jurídica, apela-se à boa-fé para que produzam maiores informações.²³⁵

A referência ao dever de lealdade e cooperação, corolário da cláusula geral da boa-fé objetiva, no tratamento de dados, corresponde a um conjunto de qualidades positivas que se espera dos seus agentes. Não se trata apenas de lealdade, mas, também, mais amplamente, probidade, veracidade, honestidade, fidelidade, comprometimento, responsabilidade e cooperação na proteção da privacidade dos titulares dos dados. Resgata-se, assim, a figura do *bonus pater familias* romano, que dever ser adequada aos dias atuais²³⁶, como o padrão de comportamento das

²³⁴ MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. 2. ed. São Paulo: Saraivajur, 2018. p. 594.

²³⁵ TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no direito civil**. São Paulo: Almedina, 2020. p. 236.

²³⁶ “[...] a conduta de boa-fé é um comportamento objetivo, separado da vontade individual, que se inspira no modelo do *bonus vir* ou do *bonus mercator* e que pode impor a modificação, a adaptação, a correção da vontade das partes. *Treu und Glauben, bonne foi, correttezza*, são noções legais, objetivas, que impõem comportamentos aos sujeitos”. BROGGINI, Geraldo. *L’abus de droit et le principe de la bonne foi - aspects historiques et comparatifs*. In: WIDMER, P.; COTTIER, B., *Abus de droit et bonne foi*, Editions Universitaires, Fribourg, 1994, p. 21 *apud* MATTIETTO, Leonardo.

relações sociais, como um todo e que serve para ilustrar as práticas socialmente aceitas naquele determinado momento. O dever de lealdade representa um

[...] princípio ético-jurídico fundamentalíssimo e existe porque a ordem jurídica não pode deixar de tutelar a confiança legítima baseada na conduta de outrem. Assim tem de ser, pois, [...] poder confiar é uma condição básica de toda a convivência pacífica e da cooperação entre os homens. Mais ainda: esse poder confiar é logo condição básica da própria possibilidade de comunicação dirigida ao entendimento, ao consenso e à cooperação [...]. Podemos assim dizer que toda a conduta, todo o agir ou interagir comunicativo, além de carrear uma pretensão de verdade ou de autenticidade (de fidelidade à própria identidade pessoal), desperta nos outros expectativas quanto à futura conduta do agente.²³⁷

Os deveres de proteção impõem às partes a obrigação de prevenir danos, tanto em relação ao objeto da prestação como também em relação às esferas jurídicas das partes e eventualmente de terceiros, e se desdobram na exigência da manutenção de um comportamento diligente, de velar pelo adequado fluxo da relação jurídica obrigacional com cuidado, previdência e segurança.

Num cenário onde é marcante o desequilíbrio informacional, decorrente da assimetria técnica e do domínio dos ambientes pelos controladores, o dever de proteção deve ser cuidadosamente observado pelos agentes de tratamento de dados, que devem diligenciar para que, no uso das tecnologias, não ocorram danos à privacidade e à autodeterminação dos indivíduos. Esse dever de proteção, decorrente da boa-fé, está intimamente ligado ao dever de adoção de medidas de segurança no uso e tratamento de dados pessoais.

Independentemente da classificação adotada para subdividir os deveres anexos ou instrumentais decorrentes da boa-fé objetiva, todos eles, cooperação, lealdade, informação, transparência, proteção etc., estão associados à confiança depositada pelo titular dos dados na ética e boa conduta do agente que recebe o consentimento para tratar seus dados pessoais.

A presença da boa-fé no tratamento de dados pessoais respalda a confiança do titular dos dados que o controlador e o operador imprimirão todos os esforços necessários para proteger esses dados e tratá-los da forma pactuada.

Sobre o princípio da boa-fé no Código Civil brasileiro de 2002: interpretação, correção e integração dos contratos. **Cadernos de Direito Actual**, n. 16, p. 133-145, 2021. Disponível em: <http://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/727/356>. Acesso em: 10 mar. 2022.

²³⁷ MACHADO, João Baptista. Tutela da confiança e *Venire contra Factum Proprium*. **Obra dispersa**, Braga: Scientia Iuridica, 1991. v. I. p. 345-423.

Como é perceptível, muitas das repercussões da boa-fé na proteção de dados são também objeto da incidência dos outros princípios, mais específicos, ainda que isso não diminua a importância da previsão dessa cláusula geral e mais ampla. A interligação da boa-fé com o princípio da finalidade, por exemplo, é sensível. A proteção da confiança na disciplina da proteção de dados implica manter o tratamento dos dados dentro dos limites pactuados, de modo a não exorbitar as finalidades legítimas que deram origem à relação entre as partes e justificaram o consentimento²³⁸.

O princípio da finalidade está previsto no inciso I do artigo 6º da LGPD e sustenta um tratamento feito para propósitos legítimos, específicos, explícitos e informados ao titular, e, sobretudo, serve de limitação ao tratamento posterior incompatível com esses propósitos pela incidência de outro princípio, o da adequação, constante do inciso II do mesmo artigo e que exige a compatibilidade do tratamento com as finalidades informadas ao titular.

Por sua vez, o inciso III define o princípio da necessidade como aquele que impõe uma limitação ao tratamento de dados ao mínimo necessário à realização das finalidades às quais se vinculou o responsável pelo tratamento quando da solicitação do consentimento, orientação também coerente com o dever de lealdade. Os princípios do livre acesso (inciso IV) e transparência (inciso VI), já abordados, são requisitos essenciais materiais para que os indivíduos exerçam seu direito de autodeterminação, pois o controle só é possível diante de informações que deverão ser corretamente prestadas por quem fará o tratamento.

Os princípios da segurança (inciso VII), prevenção (inciso VIII) e responsabilização e prestação de contas (inciso X), também já referidos anteriormente, servem à preservação dos dados pessoais, seja pela indicação da necessidade de adoção de medidas que protejam os dados e garantam o cumprimento das normas, seja pela imposição de deveres de prestação de contas através das quais o agente deverá demonstrar a aptidão das medidas para essas finalidades, condutas igualmente orientadas pela boa-fé como cláusula geral.

²³⁸ Em sentido que pode ser aqui empregado: “[...] a boa-fé objetiva é mais que apelo à ética, é noção técnico-operativa que se especifica [...], como o dever do juiz de tornar concreto o mandamento de respeito à recíproca confiança incumbente às partes contratantes, por forma a não permitir que o contrato atinja finalidade oposta ou divergente daquela para o qual foi criado”. MARTINS-COSTA, Judith. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 1996. p. 437.

Portanto, o rol de princípios do artigo 6º, todos em conjunto com a boa-fé, geram uma gama de deveres para os agentes de tratamento de dados. Deveres esses direcionados à finalidade que orienta todo o contexto da circulação de dados pessoais: efetividade na proteção da privacidade.

A boa-fé objetiva, enquanto o princípio com força normativa, mandamento de conduta que impõe comportamento leal e honesto, impõe ao operador de bancos de dados pessoais a observância de um conjunto de deveres indissociáveis à validade do consentimento oferecido, sob pena de configurar-se conduta abusiva, ilícita e passível de responsabilização. Entre eles, destacam-se os clássicos deveres de proteção, informação e cooperação, a congregar a exigência de fidelidade e lealdade. Na aplicação do primado da boa fé no cenário digital, é possível traduzir o dever de proteção, exigindo-se oferecimento e manutenção de ambiente virtual dotado de segurança para usuários, bem como diligências de cuidado e previdência, dever de informação, oferecimento de esclarecimentos e advertências, canais para atendimento e saneamento de dúvidas, além da prestação de contas quando do uso e tratamento de dados. Já pela cooperação, denotação máxima da boa-fé, conjugação de transparência, disponibilização de ferramentas para auxílio e solução de problemas, retificação de dados ou revogação imediata incondicionada do consentimento.²³⁹

Todos esses deveres e condutas exigidas dos agentes de tratamento de dados, ao fim e ao cabo, refletem o principal fundamento da legislação de proteção de dados, a autodeterminação informativa, a adequação e a qualidade da *interação* do usuário com as tecnologias que captam seus dados, bem como a geração de confiança desses mesmos usuários no bom uso que se fará dos seus dados.

Contudo, à existência de todos esses deveres ao encargo dos agentes de tratamento de dados e à necessidade de se ter o consentimento qualificado, quando essa for a base legal para o tratamento, soma-se a necessidade de adequação do ambiente onde se dará esse consentimento. Ou seja, uma arquitetura amparada na atenção aos deveres dos agentes de tratamento e com foco na proteção dos direitos dos titulares dos dados.

²³⁹ DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados: ensaio à luz da teoria do fato jurídico. *In*: EHRHARDT JÚNIOR, Marco; CATALAN, Marcos; MALHEIROS, Pablo. **Direito civil e tecnologia**. Belo Horizonte: Fórum, 2020. p. 69-88. p. 76.

3.3.3A boa-fé e o *privacy by design*: arquitetura para a proteção do consentimento

Segundo Helen Nissenbaum, o foco dos institutos que visam à proteção de dados era o controle do indivíduo sobre as suas informações pessoais ou a preservação de eventos íntimos e privados. Porém, ela define privacidade como “integridade contextual”, afirmando que a privacidade não é um direito ao sigilo, nem direito ao controle, mas, sim, o fluxo apropriado de informações pessoais, conforme normas informacionais orientadas pelo contexto social²⁴⁰.

A professora norte-americana propõe que o trânsito das informações pessoais tenha um valor social, guiado por considerações políticas e morais, que é o que determina ser ele apropriado ou não. Nessa equação, o indivíduo não se torna o soberano pelo tratamento de seus dados pessoais, até porque, muitas das vezes, esse é hipossuficiente na relação. Sugere a professora que a fórmula seja a soma do contexto mais a integridade resultando em normas informacionais²⁴¹.

Estabelece-se, assim, a locução *privacidade como integridade contextual*. Dessa conjunção (contexto + integridade) é que se arquiteta uma alternativa normativa em que a proteção dos dados pessoais não se baseia única e exclusivamente nos desígnios do próprio titular dos dados pessoais. Pelo contrário, as chamadas normas informacionais impõem restrições ao fluxo informacional que independem do controle (consentimento) exercido pelo indivíduo.²⁴² (Grifo do autor).

Os ensinamentos de Helen Nissenbaum se coadunam com a necessidade de implementação de meios capazes de proteger a vontade do titular dos dados, uma vez reconhecida sua vulnerabilidade no cyberspaço.

A partir do reconhecimento de que um modelo individualista de proteção de dados, com base exclusivamente na adjetivação do consentimento, não é suficiente para garantir o exercício pleno da autodeterminação informativa, cumpre identificar reforços para que se garanta o fluxo seguro e transparente de dados no ambiente digital.

²⁴⁰ NISSENBAUM, Helen. *Privacy in Context: technology, policy, and the integrity of social life*. Stanford: Stanford University Press, 2010; NISSENBAUM, Helen. *Privacy as contextual integrity*. *Washington Law Review*, v. 79, p. 119, 2004 *apud* BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 204.

²⁴¹ *Ibid.*, p. 204.

²⁴² BIONI, *op. cit.*, p. 204.

Uma solução viável é defender que a ética e a boa-fé devem conduzir todos os cenários de proteção da privacidade como medida fundamental e estruturante para uma evolução dos instrumentos de proteção da autodeterminação informativa.

De fato, a atenção e o cuidado com o consentimento do titular são indispensáveis no cenário tecnológico, no qual a coleta em massa de dados e a possibilidade de abuso do uso dos mesmos nem sempre atendem ao princípio da transparência e ao dever de informação.

Na Lei Geral de Proteção de Dados, a cláusula geral da boa-fé objetiva impõe conduta relacional ética, leal e honesta, e soma-se aos instrumentos preventivos de proteção da privacidade e dos dados pessoais desde o *design* e por padrão, conforme explicam Gustavo Tepedino e Chiara Teffé:

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.²⁴³

A LGPD estabelece, em seu artigo 46, que

[...] 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.

E, a seguir, no § 2º complementa que “[...] as medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do

²⁴³ TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 281-318. p. 300.

serviço até a sua execução”, incluindo na lei de proteção de dados brasileira o conceito de *privacy by design*.

Esse dispositivo, lido em conjunto com o *caput* do artigo 6º, que dispõe que as atividades de tratamento de dados deverão observar a boa-fé, e com seu inciso VIII, o qual refere o princípio da prevenção, conduz à conclusão de quão importante é a criação de confiança no procedimento de coleta e de tratamento de dados, não só pela necessidade de informação e transparência que antecede o consentimento, mas, também, pelo próprio cuidado com a arquitetura do sistema. Objetiva-se com a chamada *privacy by design* dar ao usuário mais ferramentas de confiança na rede e tranquilidade de que seu consentimento será utilizado de forma correta.

Segundo Bruno Bioni:

Trata-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 de dados pessoais, e que percorram universalmente todo o ambiente online²⁴⁴.

Ou seja, diante de instrumentos regulatórios que adjetivaram o consentimento para uma maior proteção da autodeterminação informativa, e identificado que essa larga qualificação não alcançará sozinha o seu propósito, outras formas de proteção merecem atenção.

Um dos caminhos para viabilizar maior transparência do fluxo informacional e redução das assimetrias nas relações de tratamento de dados é a metodologia conhecida como *privacy by design*, que abrange a ideia “[..] de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviço, devendo eles ser abarcados com tecnologias que facilitem o controle e a proteção das informações pessoais”²⁴⁵.

Jonas Valente, no mesmo sentido, afirma que:

A solução passaria pela consideração dessa preocupação como uma diretriz orientadora da elaboração de soluções tecnológicas, perspectiva que ganhou a denominação de *Privacy By Design* para autores em diversos campos, da ciência da computação ao direito. O conceito consiste na compreensão da

²⁴⁴ BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 170.

²⁴⁵ *Ibid.*, p. 176.

necessidade de “*information systems by designed in such a way that privacy and data protection rules are automatically*” (KOOPS *et al.*, 2013, p. 678)²⁴⁶.

O conceito do *privacy by design*, ou simplesmente PbD, fundamenta-se no reconhecimento de que a privacidade não pode ser satisfatoriamente tutelada apenas pelas estruturas regulatórias tradicionais, sendo necessário que a privacidade esteja enraizada na metodologia de operações das organizações²⁴⁷. Ann Cavoukian, em seu reconhecido artigo *Privacy by Design: the 7 Foundational Principles*, aponta os sete pilares norteadores da concepção do *privacy by design*:

1. adoção de medidas proativas e preventivas, não reativas, a fim de remediar as situações;
2. privacidade como *default*, ou seja, como padrão;
3. privacidade inserida no *design* e na arquitetura do sistema de tecnologia da informação e nas práticas de negócio;
4. funcionalidade completa, de modo que o resultado seja benéfico, não nulo;
5. segurança de ponta a ponta;
6. visibilidade e transparência; e
7. respeito pela privacidade do usuário.²⁴⁸

O primeiro dos princípios pretende a concreção prévia da tutela da privacidade, em busca de minimizar violações, bem como uma autoexecutoriedade da proteção dos dados, pois os próprios mecanismos tecnológicos efetuarão a salvaguarda das informações, porque foram arquitetados a partir de padrões éticos e orientados pela boa-fé.

O denominado *privacy by default*, segundo princípio, determina que a configuração padrão de produtos e serviços deve preservar a privacidade do usuário. Os dispositivos e as plataformas digitais devem ser ofertados ao público com todos os recursos de proteção de dados ativos, a fim de que sejam coletadas apenas informações essenciais ao funcionamento do produto ou à prestação do serviço, representando uma minimização dos dados.

²⁴⁶ VALENTE, Jonas. **Promovendo a privacidade e a proteção de dados pela tecnologia: *privacy by design* e *privacy enhancing-technologies***. Privacidade em perspectiva. Rio de Janeiro: Lumen Juris, 2018. p. 117.

²⁴⁷ BODANESE, Andréa; VIEIRA, Thyessa Junqueira Gervásio. A segurança dos dados: o conteúdo do dever e os efeitos dos incidentes de segurança. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). **Lei Geral de Proteção de Dados: aspectos relevantes**. Indaiatuba: Foco, 2021. p. 267-283.

²⁴⁸ CAVOUKIAN, Ann. **Privacy by design: the 7 foundational principles – implementation and mapping of fair information practices**. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 15 maio 2022.

Trata-se da ideia de que o produto ou serviço seja lançado e recebido pelo usuário com todas as salvaguardas que foram concebidas durante o seu desenvolvimento. Ou seja, todas as medidas para proteger a privacidade que foram idealizadas desde o início do desenvolvimento do projeto, atendendo o princípio do *privacy by design*.²⁴⁹

Dito de outra forma:

A configuração de privacidade mais restritiva possível é estabelecida desde o momento zero. Apenas os dados pessoais essenciais para prestar o serviço ou entregar o produto devem ser coletados. Ainda assim, o usuário deverá ser informado de quais informações estão sendo coletadas e para qual propósito. Caberá ao usuário, caso deseje, desativar uma ou todas essas salvaguardas. A empresa não deve fornecer o produto ou serviço com essas proteções desativadas, dependendo de uma ação do usuário para serem ativadas.²⁵⁰

Essa conduta é fundamental porque a imensa maioria dos usuários não tem conhecimentos suficientes para reconfigurar os sistemas e as políticas de privacidade, quando isso é possível.

O terceiro pilar importa na incorporação da privacidade ao *design* e visa tornar a promoção e proteção da privacidade um componente constitutivo da base funcional do dispositivo tecnológico ou do modelo de negócios²⁵¹.

O princípio da funcionalidade completa, quarto tópico, objetiva conjugar todos os interesses legítimos existente no caso concreto; permitindo, por exemplo, a troca de mensagens e informações entre emissor e receptor com a manutenção da confidencialidade do conteúdo informativo em relação a terceiros²⁵².

O princípio da segurança de ponta a ponta é a quinta proposição do método *privacy by design* e consiste em proteger o dado desde a coleta até sua eliminação; exigem-se medidas de proteção durante todo o processo de tratamento de dados, pois a proteção deve estar presente em todas as etapas, logicamente.

²⁴⁹ OLIVEIRA, Samanta. **LGPD: as diferenças entre o *privacy by design* e o *privacy by default***. Disponível em: <https://www.consumidormoderno.com.br/2019/05/27/lgpd-diferencas-privacy-design-privacy-default/>. Acesso em: 16 maio. 2022.

²⁵⁰ LEMOS, Ronaldo e BRANCO, Sérgio. *Privacy by design: conceito, fundamentos e aplicabilidade na LGPD*. In: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo Gen, 2020. p. 447-457. p. 451.

²⁵¹ MODENESI, Pedro. *Privacy by design e código digital: a tecnologia a favor de direitos e valores fundamentais*. In: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (org.). **Proteção de dados pessoais na sociedade de informação: entre dados e danos**. Indaiatuba: Foco, 2021. p. 61-75.

²⁵² *Ibid.*

O sexto princípio é o que exige visibilidade e transparência na arquitetura dos códigos digitais e refere-se à mesma orientação que está inserta no artigo 6º, VI, da LGPD, ou seja, que sejam prestadas informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados e seus respectivos agentes. Aqui se evita a opacidade, tão frequente nesse cenário, que inviabiliza a verificação da conformidade da atuação dos controladores e operadores com a boa-fé, as boas práticas e as normas de proteção aplicáveis.

A sétima e última diretiva que determina o respeito à privacidade do usuário tem como principal objetivo incentivar a disseminação de tecnologias cujos *designs* sejam amigáveis, fáceis de usar, proporcionando facilidade de manuseio. Os artefatos e sistemas tecnológicos devem ser criados e desenvolvidos levando-se em conta as necessidades e os interesses dos titulares²⁵³.

Todas essas diretrizes são destinadas aos responsáveis pelo tratamento de dados e visam garantir a privacidade e o controle das informações pelo seu titular por meio de medidas técnicas e organizacionais aplicáveis tanto no momento de definição dos métodos de tratamento quanto na sua própria execução²⁵⁴. Propõe-se que a arquitetura do sistema desde a sua concepção seja formulada de forma a proteger a privacidade dos titulares de dados e que seus criadores observem a boa-fé e a ética na formulação dos cenários digitais, observando a máxima proteção da privacidade dos usuários.

As tecnologias que adotam o *privacy by design* em sua concepção ou execução são conhecidas como PETs (*privacy enhancing technologies*), o que significa que são estruturas que priorizam a proteção da privacidade a partir de um conceito ético e leal de conduta daqueles que têm o controle dos dados pessoais disponibilizados na rede.

Pode-se dizer que o objetivo essencial do *privacy by design*, que emana do dever de respeito ao usuário e titular de dados e, também, da cláusula geral da boa-fé objetiva, é a proteção da autodeterminação informativa. O *privacy by design* atua como uma diretriz de todos os processos de tratamento de dados desde a concepção e vai muito além da mera ampliação dos requisitos de segurança dos dados do titular,

²⁵³ MODENESI, Pedro. *Privacy by design* e código digital: a tecnologia a favor de direitos e valores fundamentais. In: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (org.). **Proteção de dados pessoais na sociedade de informação**: entre dados e danos. Indaiatuba: Foco, 2021. p. 61-75. p. 61-75.

²⁵⁴ *Ibid.*

mas sua implementação deve refletir a prevenção de riscos (princípio da prevenção) e despertar no titular dos dados confiança e tranquilidade para consentir o seu uso e tratamento.

De fato, tem um discutível que, nas exigências de probidade, lisura e correção de conduta que a boa-fé traduz, cabe a de não criar ou acalantar indevidamente expectativas em outrem, bem como prevenir a formação ou manutenção de representações falsas, temerárias ou infundadas (ou o respectivo risco).²⁵⁵

Uma arquitetura de rede responsável, correta e leal aos seus propósitos, que transmita confiança aos titulares de dados de que os controladores não se comportarão de forma contraditória e desleal ao longo da relação, será uma arquitetura que se alinha ao modelo de *privacy by design* e à cláusula geral da boa-fé objetiva, em busca de efetividade e garantias de proteção da autodeterminação informativa.

O PbD é uma forma de orientar a proteção de dados e privacidade por dentro, ou seja, por meio da disposição de camadas na arquitetura da rede que garantam o possível controle e autonomia do titular dos dados²⁵⁶. Além da integração de sistemas, o PbD exige a implementação de requisitos funcionais que garantam o controle e autodeterminação informativa aos titulares dos dados. Embora seja uma diretriz principiológica, muito se sustenta que o PbD seria uma forma de, por meio da autorregulação, amenizar as contramedidas da regulação estatal, visto que, se o consentimento tem as suas limitações para atingir determinadas hipóteses de tratamento de dados pessoais²⁵⁷, também o teria o PbD, dada a pouca experiência e habilidade dos titulares dos dados com determinados dispositivos.

Importante destacar que a ideia em torno do *privacy by design* não deve representar simplesmente um rótulo atribuído a produtos e serviços para que as operações de tratamento de dados pessoais aconteçam “revestidas” de adequação; mas compreender procedimentos que efetivamente estimulem a minimização na coleta de dados pessoais e outras medidas técnicas e operacionais que ampliem

²⁵⁵ FRADA, Manuel António de Castro Portugal Carneiro da. **Teoria da confiança e responsabilidade civil**. Coimbra: Almedina. 2018. p. 467.

²⁵⁶ SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço: a *accountability* como fundamento da *lex privacy***. 219 f. Tese (Doutorado em Direito) – Curso de Direito, Universidade de Brasília, Brasília, 2019. p. 182.

²⁵⁷ BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 234.

sobremaneira as formas de tutela da privacidade²⁵⁸ e garantam confiabilidade na coleta e tratamento de dados.

Nesse sentido, é possível defender que a solução tecnológica fundamentada no *privacy by design* carrega consigo a indispensável observância da cláusula geral da boa-fé objetiva, porque é justamente uma arquitetura de rede com bons propósitos, proteção à autodeterminação informativa e respeito à privacidade que trará para o ambiente digital a confiança de que o consentimento, respaldado nesse cenário, será válido.

A regra da boa-fé credibiliza a formação e perduração das expectativas. Promove ou assegura espaços de confiança, pois determina precaver o sujeito do que não deve ou não é curial esperar. Deste modo, circunda as várias situações de confiança, atuais ou potenciais, como ordem normativa envolvente das formas de coordenação de conduta entre os sujeitos baseadas na confiança e propiciadora do seu êxito.²⁵⁹

Antes foi dito sobre as dificuldades de o consentimento representar, verdadeiramente, uma manifestação livre, informada e inequívoca que autorize o tratamento de dados pessoais, especialmente em razão da marcante assimetria informacional presente no cenário digital. O que se confirma, por exemplo, com a constatação de que políticas de privacidade, termos de uso e outros arranjos contratuais são concebidos de forma extensa, pouco prática e sob a perspectiva de que o destinatário é um usuário, via de regra, incapaz de proteger sozinho sua esfera de privacidade.

Assim, sendo o consentimento a base legal disponível ao controlador para amparar o tratamento de dados pessoais, e sabendo que a participação do indivíduo no fluxo de suas informações pessoais somente pode ser validada se todos os requisitos, exigidos pela LGPD, estiverem presentes nessa manifestação de vontade, o *privacy by design*, implementado a partir das diretrizes impostas pela cláusula geral da boa-fé objetiva, deve ser reconhecido como um instrumento fundamental na busca de proteção da autodeterminação informativa e mitigação da reconhecida assimetria informacional nas relações de tratamento de dados.

²⁵⁸ SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço: a *accountability* como fundamento da *lex privacy***. 219 f. Tese (Doutorado em Direito) – Curso de Direito, Universidade de Brasília, Brasília, 2019. p. 184.

²⁵⁹ FRADA, Manuel António de Castro Portugal Carneiro da. **Teoria da confiança e responsabilidade civil**. Coimbra: Almedina. 2018. p. 467.

Se o consentimento é a ponte que liga o titular dos dados ao controlador que deseja coletá-los e tratá-los, uma arquitetura de rede que observe o *privacy by design* e os deveres oriundos da boa-fé objetiva é o trajeto para que esse consentimento possa representar uma manifestação de vontade livre, informada e inequívoca e, de fato, apresente-se como expressão do direito à autodeterminação informativa.

CONCLUSÃO

O desenvolvimento das relações humanas tornou inafastável o fornecimento de informações e dados pessoais no ambiente físico e digital, nesse cenário, a Lei Geral de Proteção de Dados, ao disciplinar o uso e integridade dos dados de cada pessoa, protege e garante a dignidade da pessoa humana, em especial a sua privacidade.

Ao trazer a autodeterminação informativa como um de seus fundamentos, a LGPD busca assegurar o exercício da liberdade existencial diante do papel relevante da informação para as escolhas individuais e o estabelecimento de vínculos na sociedade.

Diante da certeza de que as relações que envolvem o tratamento de dados são marcadas por uma inevitável assimetria informacional, e nas quais existe grande potencial de dano à privacidade e à dignidade da pessoa humana, mas também sabendo que é atividade indissociável da sociedade de informação, a lei trouxe várias ferramentas específicas a favor do controle do titular sobre os seus dados. O consentimento é a mais importante delas e deve representar uma manifestação livre informada e inequívoca de vontade, quando for a base legal utilizada para o tratamento de dados.

O cuidado e a centralidade dispensados à figura do consentimento, objeto deste estudo, revelam a preocupação do legislador, que também se constitui em resposta social, com a participação do indivíduo no fluxo de suas informações pessoais, incentivando e oportunizando um comportamento ativo de parte do titular, mas também exigindo condutas específicas e condizentes com a cláusula geral da boa-fé dos agentes que realizam o tratamento de dados.

A boa-fé objetiva é conceito que há muito orienta as relações jurídicas e encontra-se consolidada pela doutrina e pela jurisprudência como princípio ético-jurídico, impositivo de padrões éticos e leais de conduta, e a LGPD, ao referir a boa-fé objetiva como princípio orientador das relações por ela regidas, consolidou-a como cláusula geral de observância obrigatória em todas as relações que envolvem tratamento de dados pessoais. Esse princípio traz consigo, para além da ideia de lealdade entre as partes, a promoção de uma efetiva cooperação para o adequado adimplemento da obrigação, buscando a promoção e tutela da confiança na troca de informações.

A cláusula geral da boa-fé objetiva, como impositiva de padrões de conduta, exige ética, lealdade, cooperação em todas as relações jurídicas nas quais o direito se aplica²⁶⁰, e, ao ganhar papel de destaque na legislação protetiva de dados pessoais, se revela como ferramenta de grande importância na mitigação da assimetria informacional presente nessas relações, bem como, na proteção do direito à autodeterminação informativa, e atua tanto para a interpretação dos termos gerais nos quais consta o requerimento do consentimento quanto para o enquadramento das condutas do ente que realiza o tratamento de dados, assim como, orienta toda a arquitetura de rede que está por trás da coleta do consentimento.

A informação como suporte ao consentimento, que legitima o tratamento de dados pessoais, embora indispensável, sozinha não se mostra suficiente para resguardar a autodeterminação informativa, tanto pela discrepância informacional constatada, quanto pelas dificuldades cognitivas de seus titulares.

Nesse sentido, a boa-fé, como impositiva de condutas éticas, conjuntamente com os deveres legais de informar, de segurança e de boas práticas podem equacionar e mitigar a assimetria informacional presente no tratamento de dados e evitar que o consentimento se torne uma mera ficção.

Se de fato um sistema de proteção individual de dados pessoais não é suficiente para a proteção da privacidade dos dados, porque inúmeros são os obstáculos para isso, a existência dos diversos deveres, arrolados neste trabalho, ao encargo dos controladores e operadores dos dados, somada a um adequado ambiente de rede onde se dará o consentimento, parece um caminho a ser perseguido.

Nesse contexto, de tecnologias que interferem ativamente no dia a dia dos indivíduos, direcionando conteúdo personalizado e tomando decisões automatizadas sobre seus dados, considera-se que as soluções tecnológicas fundamentadas no *privacy by design*, que carrega consigo a indispensável observância da cláusula geral da boa-fé objetiva, por configurarem-se em uma arquitetura de rede com bons

²⁶⁰ “Se todos os homens cumprissem espontaneamente seus deveres jurídicos, seria inútil a sanção que as normas de Direito contêm. Mas, se é certo que a maioria observa, ‘por virtude, por disciplina, por hábito ou por temor’, as regras jurídicas, não é pequeno o número de desobedientes. Para obrigá-los a comportamento conforme o Direito, são proporcionados aos titulares de direitos os meios necessários para defendê-los. [...] A autodefesa e o direito de invocar a proteção jurídica do Estado são as duas modalidades principais de proteção. Outra modalidade de proteção é o nascimento automático de uma nova situação jurídica para eliminar a violação ou o perigo de lesão do direito”. GOMES, Orlando. **Introdução ao direito civil**. 21. ed. atual. por Edvaldo Brito e Reginalda Paranhos de Brito. Rio de Janeiro: Forense, 2016. p. 393.

propósitos, alinhada com a proteção à autodeterminação informativa e respeito à privacidade, são o caminho para um ambiente digital que alcance a confiança necessária dos titulares de dados no momento de consentir para o uso de seus dados pessoais. Confiança, essa, que propiciará o consentimento com todas as qualificadoras exigidas pela LGPD.

A observância da cláusula geral da boa-fé objetiva no *design* das redes, que coletam e tratam dados pessoais, auxilia na equação dos benefícios e efeitos positivos da inteligência artificial com os riscos das tecnologias ao direito de controle dos dados pessoais pelos seus titulares.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. Teoria e direito público. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. Título original: Theorie der Grundrechte.

ALIMONTI, Veridiana. Autodeterminação informacional na LGPD: antecedentes, influências e desafios. *In*: VILLAS BÔAS CUEVA, Ricardo; DONEDA, Danilo; MENDES, Laura Schertel (org.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters, 2020. p. 177-192.

ÁVILA, Humberto Bergmann. **Teoria dos princípios**. Da definição à aplicação dos princípios jurídicos. 16. ed. São Paulo: Malheiros, 2015.

ÁVILA, Humberto. **Teoria dos princípios**: da definição à aplicação dos princípios jurídicos. 18. ed. São Paulo: Malheiros, 2018.

AZEVEDO, Antonio Junqueira de. **Negócio jurídico**: existência, validade e eficácia. 4. ed. atual. São Paulo: Saraiva, 2002.

BAROCAS, Solon; NISSENBAUM, Helen. Big Data's End Run around Anonymity and Consent. *In*: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (ed.). **Privacy, Big Data, and the Public Good**: Frameworks for Engagement. Cambridge: Cambridge University Press, 2014. p. 44-75.

BIONI, Bruno e DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, a. 9, n. 3, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662>. Acesso em: 01 jun. 2021.

BIONI, Bruno Ricardo. O consentimento como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 145-161.

BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo "Lulu". **Revista de Direito do Consumidor**, São Paulo, a. 23, v. 94, p. 283-326, 2014.

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

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPai/USP, 2015.

Disponível em:

https://www.researchgate.net/publication/328266374_Xequemate_o_tripecte_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 31 mar. 2022.

BISNETO, C. D. Dano moral pela violação à legislação de proteção de dados: um estudo de direito comparado entre a LGPD e o RGPD. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (org.). **Proteção de dados pessoais na sociedade de informação**: entre dados e danos. 1. ed. Indaiatuba: Foco, 2020. p. 218-240.

BLUM, Rita Peixoto Ferreira. Boa-fé objetiva. **Revista de Marketing Industrial**, São Paulo: Instituto de Marketing Industrial, a. 9, n. 22, p. 70-75, 2003.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BODANESE, Andréa; VIEIRA, Thyessa Junqueira Gervásio. A segurança dos dados: o conteúdo do dever e os efeitos dos incidentes de segurança. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). **Lei Geral de Proteção de Dados**: aspectos relevantes. Indaiatuba: Foco, 2021. p. 267-283.

BONNA, Alexandre Pereira. Dados pessoais, identidade virtual e a projeção da personalidade: “profiling”, estigmatização e responsabilidade civil. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020. p. 19-38.

BRAGA NETO, Felipe Peixoto. **Manual de direito do consumidor**: à luz da jurisprudência do STJ. 8. ed. Salvador: Juspodivm, 2013.

BREEN, Stephen; OUAZZANE, Karim Ouazzane e PATEL, Preeti. GDPR: is your consent valid? **Business Information Review**, London: London Metropolitan University, v. 37, p. 19-24, 2020. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/0266382120903254>. Acesso em: 05 jun. 2021.

BRUNTON, Finn e NISSENBAUM, Helen. **The Fantasy of Opting Out**. Disponível em: <https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/>. Acesso em: 02 jun. 2021.

BUCAR, Daniel; VIOLA, Mário. Tratamento de dados pessoais por “legítimo interesse do controlador”: primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 465-484.

BUNDESVERFASSUNGSGERICHT. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em 02 jun. 2022.

BUSSATTA, Eduardo Luiz. **Resolução dos contratos e teoria do adimplemento substancial**. 2. ed. São Paulo: Saraiva, 2008.

CAVALIERI FILHO, Sergio. **Programa de direito do consumidor**. São Paulo: Atlas, 2008.

CAVOUKIAN, Ann. **Privacy by design**: the 7 foundational principles – implementation and mapping of fair information practices. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>. Acesso em: 15 maio 2022.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52., p. 1373-1438, 2000. Disponível em: <https://scholarship.law.georgetown.edu/facpub/810>. Acesso em: 01 jun. 2021.

COMPARATO, Fábio Konder. A proteção do consumidor: importante capítulo do Direito Econômico. *In*: MARQUES, Cláudia Lima; MIRAGEM, Bruno (org.). **Coleção doutrinas essenciais**: direito do consumidor – fundamentos do direito do consumidor. São Paulo: Revista dos Tribunais, 2011. v. 1. p. 167-186.

CONSELHO DA EUROPA. **Carta dos Direitos Fundamentais da União Europeia**. Nice, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 19 nov. 2021.

CORDEIRO, António Menezes. **Da boa fé no direito civil**. São Paulo: Almedina, 2017.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais**: comentada. 3. ed. São Paulo: Revista dos Tribunais, 2019.

DANTAS, Juliana de Oliveira Jota; COSTA, Eduardo Henrique. A natureza jurídica do consentimento previsto na Lei Geral de Proteção de Dados: ensaio à luz da teoria do fato jurídico. *In*: EHRHARDT JÚNIOR, Marco; CATALAN, Marcos; MALHEIROS, Pablo. **Direito civil e tecnologia**. Belo Horizonte: Fórum, 2020. p. 69-88.

DONEDA, Danilo. A proteção de dados como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.); BIONI, Bruno (coord. Executivo). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 3-20.

DRESCH, Rafael de Freitas Vale; FALEIROS JÚNIOR, José Luiz de Moura. Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei n. 13.709/2018). *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). **Responsabilidade civil**: novos riscos. Indaiatuba: Foco, 2019. p.65-89.

DRESCH, Rafael. **A especial responsabilidade civil na Lei Geral de Proteção de Dados**. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de->

[responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados](#). Acesso em: 13 jun. 2021.

EUROPEAN COMMISSION. **Article 29 Working Party Guidelines on consent under Regulation 2016/679**. 2017. p. 14. Disponível em: <https://ec.europa.eu/newsroom/article29/items/623051/en>. Acesso em: 06 abr. 2022.

FACCHINI NETO, Eugênio e DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito**, n. IX, p. 119-140, 2º sem. 2019.

FINCATO, Denise Pires. **A pesquisa jurídica sem mistérios**: do projeto de pesquisa à banca. Porto Alegre: Notadez, 2008.

FRADA, Manuel A. Carneiro da. **Teoria da confiança e responsabilidade civil**. Coimbra: Almedina, 2004.

FRADA, Manuel António de Castro Portugal Carneiro da. **Teoria da confiança e responsabilidade civil**. Coimbra: Almedina. 2018.

FREELY Given Consent. Recital 43. General Data Protection Regulation (GDPR). **Intersoft Consulting**, Disponível em: <https://gdpr-info.eu/recitals/no-43/>. Acesso em: 02 jun. 2021.

FREITAS, Juarez. **A Interpretação sistemática do direito**. 5. ed. São Paulo: Malheiros, 2010.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**: parte geral. São Paulo: Saraiva, 2002.

GARCIA, Ricardo Lupion. **Boa-fé objetiva nos contratos empresariais**: contornos dogmáticos dos deveres de conduta. Porto Alegre: Livraria do Advogado, 2011.
GOMES, Orlando. **Introdução ao direito civil**. 20. ed. Rio de Janeiro: Forense, 2010.

GOMES, Orlando. **Introdução ao direito civil**. 21. ed. atual. por Edvaldo Brito e Reginalda Paranhos de Brito. Rio de Janeiro: Forense, 2016.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do tratamento de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 219-241.

LALANA, Angel Daniel; SORO, José Felix Muñoz. El mito del consentimiento y el fracaso del modelo individualista de protección de datos. *In*: VALERO TORRIJOS, Julian. **La protección de datos personales en internet ante la innovación tecnológica**. Riesgos, amenazas y respuestas desde la perspectiva jurídica. Navarra: Aranzadi, 2013. p. 153-196.

LARENZ, Karl. **Derecho de obligaciones**. Tradução para o espanhol de Jaime Santos Briz. Madrid: Editorial Revista de Derecho Privado, 1958. tomo I.

LEMOS, Ronaldo e BRANCO, Sérgio. Pivacy by design: conceito, fundamentos e aplicabilidade na LGPD. *In*: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo Gen, 2020. p. 447-457.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

LIMA, Marco Antonio; BARRETO JÚNIOR, Irineu Francisco. Marco civil de internet: limites da previsão legal de consentimento expresso e inequívoco como proteção jurídica dos dados pessoais na internet. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 1, n. 2, p. 241-260, jan./jun. 2016.

LÔBO, Paulo Luiz Netto. **Direito civil** – parte geral. 6. ed. São Paulo: Saraiva, 2017.

LÔBO, Paulo Luiz Netto. **Teoria geral das obrigações**. São Paulo: Saraiva, 2005.

MACHADO, João Baptista. Tutela da confiança e *Venire contra Factum Proprium*. **Obra dispersa**, Braga: Scientia Iuridica, 1991. v. I.

MAÑAS, José Luis Piñar. El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. **Asamblea**: revista parlamentaria de la Asamblea de Madrid, n. 13, p. 21-46, 2005.

MANTOVANI, Alexandre Casanova. **O consentimento na disciplina da proteção dos dados pessoais**: uma análise dos seus fundamentos e elementos. 2019. 171 f. Dissertação (Mestrado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2019.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 8. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2016.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**. 4. ed. São Paulo: Revista dos Tribunais, 2002.

MARQUES, Cláudia Lima. **Contratos no código de defesa do consumidor**: o novo regime das relações contratuais. 6. ed. São Paulo: Revista dos Tribunais, 2011.

MARTINS, Guilherme Magalhães e FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de Dados. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020. p. 263-297.

MARTINS, Leonardo. **Tribunal Constitucional Federal alemão**: decisões anotadas sobre direitos fundamentais. Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung, 2016.

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

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. São Paulo, Marcial Pons, 2019.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 2000.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. São Paulo: Revista dos Tribunais, 1996.

MARTINS-COSTA, Judith. Como harmonizar os modelos jurídicos abertos com a segurança jurídica dos contratos? (notas para uma palestra). **Revista Brasileira de Direito Civil**, Rio de Janeiro, v. 5, p. 67-76, jul./set. 2015. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/90/86>. Acesso em: 16 mar. 2022.

MARTINS-COSTA, Judith. Os campos normativos da boa-fé objetiva: as três perspectivas do direito privado brasileiro. *In*: AZEVEDO, Antônio Junqueira; TORRES, Heleno Taveira; CARBONE, Paolo (coord.). **Princípios do Novo Código Civil Brasileiro e outros temas**. São Paulo: Quartier Latin, 2008. p. 386-420.

MATTIETTO, Leonardo. Sobre o princípio da boa-fé no Código Civil brasileiro de 2002: interpretação, correção e integração dos contratos. **Cadernos de Direito Actual**, n. 16, p. 133-145, 2021. Disponível em: <http://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/727/356>. Acesso em: 10 mar. 2022.

MELLO, Bernardes de. **Teoria do fato jurídico**: plano da existência. 22. ed. São Paulo: Saraiva, 2019.

MELLO, Heloísa Carpena Vieira de. O abuso de direito no Código Civil de 2002: relativização dos direitos na ótica civil-constitucional. *In*: TEPEDINO, Gustavo (coord.). **A parte geral do Novo Código Civil**: estudos na perspectiva civil-constitucional. 2. ed. Rio de Janeiro: Renovar, 2003. p. 377-396.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 18 jun. 2021.

MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, a. 12, n. 39, p. 185-216, jul./dez. 2018.

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

MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.); BIONI, Bruno (coord. executivo). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo: Revista dos Tribunais, v. 120, p. 468-486, nov./dez. 2018.

MENKE, Fabiano. A interpretação das cláusulas gerais: a subsunção e a concreção dos conceitos. **Revista da Ajuris**, Porto Alegre: AJURIS, v. 33, n. 103, p. 69-94, set. 2006.

MENKE, Fabiano. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2014. p. 205-230.

MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle (org.). **Lei Geral de Proteção de Dados: aspectos relevantes**. Indaiatuba: Foco, 2021. p. 13-22.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.); BIONI, Bruno (coord. Executivo). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 339-359.

MIRAGEM, Bruno. **Direito do consumidor**: fundamentos do direito do consumidor: direito material e processual do consumidor; proteção administrativa do consumidor, direito penal do consumidor. São Paulo: Revista dos Tribunais, 2008.

MODENESI, Pedro. *Privacy by design* e código digital: a tecnologia a favor de direitos e valores fundamentais. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (org.). **Proteção de dados pessoais na sociedade de informação**: entre dados e danos. Indaiatuba: Foco, 2021. p. 61-75.

MONTERO, Javier Puyol. Transparencia de la información y derecho de acceso de los interesados em la nueva normativa de protección de datos. *In*: LOMBARTE, Artemi Rallo (dir.). **Tratado de protección de datos**. Valencia: Tirant lo Blanch, 2019. p. 275-312.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. **Cadernos Adenauer**, Rio de Janeiro, v. 3, a. XX, p. 113-135, 2019. Disponível em: https://www.academia.edu/41132175/Autodetermina%C3%A7%C3%A3o_informativa_e_responsabiliza%C3%A7%C3%A3o_proativa_novos_instrumentos_de_tutela_da_pessoa_humana_na_LGDP. Acesso em: 10 mar. 2022.

MOTA, Maurício Jorge. A pós-eficácia das obrigações revisitada. **Revista Quaestio Iuris**, Rio de Janeiro, v. 04, n. 01, p. 351-423, 2011.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). *In*:

MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.).

Responsabilidade civil e novas tecnologias. Indaiatuba: Foco, 2020. p. 109-124.

MURILLO DE LA CUEVA, Pablo Lucas; PIÑAR MAÑAS, José Luis. **El derecho a la autodeterminación informativa.** Fundación Colóquio Jurídico Europeo. Madrid: J. San José S.A, 2009.

NEGREIROS, Teresa. **Fundamentos para uma interpretação constitucional do princípio da boa-fé.** Rio de Janeiro: Renovar, 1998.

NUNES, Luiz Rizatto. **Curso de direito do consumidor.** São Paulo: Saraiva, 2011.

OLIVEIRA, J. M. Leoni Lopes. **Novo Código Civil anotado.** Rio de Janeiro: Lumen Juris, 2004.

OLIVEIRA, Samanta. **LGPD: as diferenças entre o *privacy by design* e o *privacy by default*.** Disponível em: <https://www.consumidormoderno.com.br/2019/05/27/lgpd-diferencas-privacy-design-privacy-default/>. Acesso em: 16 maio. 2022.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018-LGPD.** São Paulo: Saraiva Educação, 2020.

RIBEIRO, Joaquim de Sousa. O imperativo de transparência no Direito Europeu dos Contratos. *In: FIUZA, César; SÁ, Maria de Fátima Freire de; NAVES, Bruno Torquato de Oliveira (coord.). Direito civil: atualidades.* Belo Horizonte: Del Rey, 2003. p. 131-157.

RÍSPOLI, Afonso Fratti Penna; QUADRADO, Hebert Fabricio Tortorelli. Fluxo informacional e autodeterminação informativa: o dilema do consentimento informado. *In: LIMA, Cíntia Rosa Pereira (coord.). ANPD e LGPD: desafios e perspectivas.* São Paulo: Almedina, 2021. p. 331-347.

RODOTÀ, Stefano. **A vida na sociedade da vigilância.** A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Daniel Piñeiro. **O direito fundamental à proteção de dados: vigilância, privacidade e regulação.** Rio de Janeiro: Lumen Juris, 2021.

RUARO, Regina Linden e 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). *In: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.). Tratado de proteção de dados pessoais.* São Paulo: Grupo Gen, 2020. p. 177-191.

RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jun. 2015.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. The Right to Personal Data Protection: a Reading of the European System and the Necessary Protection of

Sensible Data as a Paradigm for the Brazilian Legal Order. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 11, p. 163, 2010. p. 163-180.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito (UFPR)**, Curitiba, v. 53, p. 45-66, 2012.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden e FERNANDES, Márcia Santana. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. *In*: MENDES, Laura Schertel; DONEDA, Danilo, SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (coord.). **Tratado de proteção de dados pessoais**. São Paulo: Grupo Gen, 2020. p. 485-506.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2009.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 21-59.

SCHERMER, B. W.; CUSTERS, Bart; HOF, S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). **Ethics and Information Technology**. DOI: 10.1007/s10676-014-9343-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418. Acesso em: 21 fev. 2022.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 319-338.

SILVA, Clóvis V. do Couto e. **A obrigação como processo**. Rio de Janeiro: FGV, 2006.

SILVA, Eva Sónia Moreira. **Da responsabilidade pré-contratual por violação dos deveres de informação**. Coimbra: Almedina, 2003.

SOLANA, Mònica Vilasau. Menores. Centros docentes y datos: decisiones conflictivas. *In*: MALLÉN, Beatriz Tomáz; MAHAMUT, Rosario Garcia; CHULVI, Cristina Pauner. **Las cláusulas específicas del Reglamento General de Protección de Datos en el Ordenameto Jurídico Español**. Valencia: Tirant lo Blanch, 2021. p. 179-212.

SOLOVE, Daniel J. **Introduction**: privacy self-management and the consent dilemma. Disponível em:

<https://heinonline.org/HOL/LandingPage?handle=hein.journals/hlr126&div=87&id=&page=>. Acesso em: 18 abr. 2022.

SOLOVE, Daniel J. **Understanding privacy**. Cambridge: Harvard University Press, 2009.

SOMBRA, Thiago Luís Santos. **Direito à privacidade e proteção de dados no ciberespaço: a accountability como fundamento da *lex privacy***. 219 f. Tese (Doutorado em Direito) – Curso de Direito, Universidade de Brasília, Brasília, 2019.

TEPEDINO, Gustavo; SCHREIBER, Anderson. A boa-fé objetiva no Código de Defesa do Consumidor e no Novo Código Civil. **Revista da EMERJ**, Rio de Janeiro, v. 6, n. 23, p. 29-44, 2003.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 281-318.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil**. Responsabilidade civil. Rio de Janeiro: Forense, 2020. v. 4.

THEODORO JÚNIOR, Humberto; FIGUEIREDO, Helena Lanna. **Negócio jurídico**. Rio de Janeiro: Forense, 2021.

TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no direito civil**. São Paulo: Almedina, 2020.

TRANQUILLINI NETO, Aristides. Compliance com a Lei Geral de Proteção de Dados como forma de evitar a Responsabilização civil. *In*: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo (org.). **Proteção de dados pessoais na sociedade de informação: entre dados e danos**. Indaiatuba: Foco, 2021. p. 241-257.

TYBURSKA, Justyna. Criterion of legitimacy of consent for processing personal data in e-commerce. Disponível em: <https://czasopisma.uksw.edu.pl/index.php/cwc/article/view/6033>. Acesso em: 06 abr. 2022.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 2000/C 364/01. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 19 nov. 2020.

UNIÃO EUROPEIA. Diretiva 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. **Jornal Oficial da União Europeia**, Estrasburgo, 24 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046>. Acesso em: 20 maio 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 04 abr. 2022.

VALENTE, Jonas. **Promovendo a privacidade e a proteção de dados pela tecnologia: *privacy by design e privacy enhancing-technologies***. Privacidade em perspectiva. Rio de Janeiro: Lumen Juris, 2018.

WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 24 maio 2021.

WESTIN, Alan F. Science, privacy and freedom: issues and proposals for the 1970's. Part I – The current impact of surveillance on privacy. **Columbia Law Review**, n. 6, v. 66, jun. 1966. Disponível em: https://www.jstor.org/stable/1120997?seq=1&cid=pdfreference#references_tab_contents. Acesso em: 29 mar. 2022.

WORKING PARTY 29. **Opinion 3/2010 on the principle of accountability**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf. Acesso em: 02 maio 2022.



Pontifícia Universidade Católica do Rio Grande do Sul
Pró-Reitoria de Graduação
Av. Ipiranga, 6681 - Prédio 1 - 3º. andar
Porto Alegre - RS - Brasil
Fone: (51) 3320-3500 - Fax: (51) 3339-1564
E-mail: prograd@pucrs.br
Site: www.pucrs.br