doi: 10.21783/rei.v6i2.521

SUBMETIDO: 05 SET. 2020
ACEITO: 05 SET. 2020

PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO:
TENDÊNCIAS CONTEMPORÂNEAS DE MATERIALIZAÇÃO

DATA PROTECTION BEYOND CONSENT:
CONTEMPORARY DEVELOPMENTS TOWARDS MATERIALIZATION

LAURA SCHERTEL MENDES [1]
GABRIEL C. SOARES DA FONSECA [2]

RESUMO: O presente artigo tem como objetivo debater o enfoque no consentimento do titular dos dados como instrumento regulatório nuclear da proteção de dados pessoais. Para tanto, são brevemente abordados três aspectos que demonstram as insuficiências do paradigma do consentimento: (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos; (ii) a lógica binária "*take it or leave it*", que reflete a ausência de uma vontade livre em razão da assimetria de poderes entre ele e o agente responsável pelo tratamento, bem como a sua dependência a muitos serviços da sociedade da informação; e (iii) as modernas técnicas de tratamento e de análise dos dados pessoais, que possibilitam a agregação de informações e que dificilmente podem ser gerenciadas pelo titular de dados no momento da coleta dos dados. Para superar essas insuficiências, tendências contemporâneas de materialização da proteção de dados apresentam-se como soluções interessantes, tornando-a mais responsiva tanto aos riscos gerados pelo tratamento, como aos obstáculos concretos a uma decisão livre e autônoma. Neste texto, exploraram-se três caminhos nesse sentido: (i) estratégias a partir da tecnologia e do desenho dos

[1] Professora Adjunta de Direito Civil da Universidade de Brasília (UnB), e do Instituto Brasiliense de Direito Público (IDP). Doutora *summa cum laude* em Direito Privado pela Universidade Humboldt de Berlim, tendo publicado, na Alemanha, sua tese sobre proteção de dados no setor privado. Mestre em Direito, Estado e Constituição pela Universidade de Brasília (UnB). Bacharel em Direito pela Universidade de Brasília (UnB). Diretora da Associação Luso-Alemã de Juristas (DLJV-Berlim) e do Instituto Brasileiro de Política e Direito do Consumidor (Brasilcon). E-mail: lauraschertel@hotmail.com ORCID: https://orcid.org/0000-0001-8675-4994.

[2] Mestrando em Direito Econômico, Financeiro e Tributário na Universidade de São Paulo (USP). Bacharel em Direito pela Universidade de Brasília (UnB). Assessor de Ministro no Supremo Tribunal Federal (STF). E-mail: gabrielcsfonseca@gmail.com ORCID: https://orcid.org/0000-0002-5096-927X.

sistemas informacionais (*privacy by design*) a fim de auxiliar o titular no controle de seus dados; (ii) implementação da regulação pautada na prestação de contas pelos agentes de tratamento (*accountability*), dimensionando os riscos prévios ao tratamento de dados pessoais; e (iii) o controle contextual do consentimento.

Palavras-Chave: Proteção de Dados Pessoais; Consentimento; Privacidade; Regulação.

ABSTRACT: This paper highlights the need to reshape the focus on "notice and consent" as the main regulatory instrument in data protection. Therefore, we briefly outline three aspects that show its insufficiencies: (i) cognitive limitations, (ii) bargaining powers, and (iii) contemporary data processing and analysis techniques such as Big Data. Instead of claiming the "end" of notice and consent, we conclude that it is essential to reshape it in light of other available regulatory instruments and bearing in mind the multiple stakeholders involved. Hence, by analyzing contemporary data protection legislations and recent academic developments, we briefly set out three approaches that can be useful in that way: (i) data protection by design and default; (ii) risk analysis and accountability; (iii) limitations on consent that are responsive to the central values at stake and its particular context.

Keywords: Data Protection; Notice and Consent; Privacy; Regulation.

INTRODUÇÃO

"Li e aceito os termos". Ao navegar pela Internet, é bastante comum se deparar com essa frase ao fim de um longo texto, com letras pequenas e linguagem técnica. Não por acaso, estudos têm indicado que muitos usuários não leem esses termos e, quando leem, acabam por não os entender ou levam um tempo significativo para tanto (*v.g.* MCDONALD; CRANOR, 2008). Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja a de não desfrutar importantes produtos e serviços *online* (CATE; MAYER-SCHÖNBERGER, 2013, p. 67). Entretanto, em assim fazendo, acaba enfrentando elevados custos sociais na medida em que esses produtos e serviços penetram, cada vez mais, a vida social e as dinâmicas político-econômicas dos cidadãos com o Estado, com empresas privadas e com a comunidade na qual estão inseridos (MENDES, 2014, p. 22).

Ao longo das últimas cinco décadas, muitas das discussões relacionadas à regulação da privacidade e da proteção de dados pessoais destinaram bastante foco em torno do consentimento[3] expressado pelo titular dos dados. Nesse sentido, não é exagero afirmar que o consentimento tem figurado como instrumento [4] regulatório central e núcleo de legitimidade prática desse regime protetivo. Ele é lido, ainda, como expressão da autonomia individual e do controle do titular dos dados em torno de seus direitos de personalidade (BIONI, 2019, p. 177), contudo, sem inviabilizar o livre fluxo desses dados, elemento relevante para uma série de atividades econômicas e até mesmo para a elaboração de políticas públicas (CATE; MAYER-SCHÖNBERGER, 2013, p. 67).

Não obstante, parcela significativa da literatura (*v.g.* SOLOVE, 2013; 2020; BAROCAS; NISSENBAUM, 2014; BIONI, 2019) tem ressaltado as insuficiências do consentimento na tarefa de tutelar a privacidade e de proteger os dados pessoais dos cidadãos frente aos desafios contemporâneos trazidos, por exemplo, pela ascensão do *Big Data* [5], pela difusão da publicidade comportamental [6], pela proliferação de tecnologias relacionadas ao rastreamento e ao monitoramento dos usuários na Internet entre outros. Além disso, em frente a essas insuficiências, iniciativas normativas mais recentes, como a Lei Geral de Proteção de Dados (Lei n° 13.709/2018, doravante LGPD) e o Regulamento Geral de Proteção de Dados (RGPD), têm apresentado abordagens distintas e medidas complementares com o intuito de garantir maior efetividade e segurança ao consentimento do titular dos dados.[7]

3 Importante frisar que o termo "consentimento", na proteção de dados pessoais, não é isento de divergências conceituais (ZANATTA, 2015, P. 458-459). Entretanto, ao menos segundo o artigo 5°, XII, da Lei 13.709/2018 (BRASIL, 2018), o consentimento representa uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

4 Segundo Márcio Aranha e Othon Lopes (2019, p. 179-186), instrumentos regulatórios são meios para influenciar o comportamento social e alcançar os objetivos almejados. Por sua vez, as estratégias regulatórias integram funcionalmente esses instrumentos na busca por alcançar tal pretensão.

5 Conforme elucidam Viktor Mayer-Schönberger e Kenneth Cukier (2014, p. 6), o termo "*Big Data*" é de difícil definição precisa e taxativa. No entanto, em linhas gerais, segundo os autores, *Big Data* se refere às técnicas de captação, armazenamento e processamento de dados em larga escala para extrair novos insights ou criar novas formas de valor, alterando sensivelmente mercados, organizações, as relações entre o Governo e seus cidadãos.

6 A publicidade comportamental, também conhecida como *behavioral advertising*, está relacionada com a personalização da publicidade a partir do monitoramento das atividades online do consumidor (MENDES, 2014).

7 Por óbvio, não se defende aqui que essas legislações trouxeram inovações plenas ou medidas absolutamente eficazes, porém evoluíram em aspectos importantes que serão

Em meio a esse cenário, o objetivo do presente artigo é justamente explorar e sistematizar essas tendências contemporâneas. Desde logo, todavia, é importante ressaltar que não se pretende defender a inutilidade do consentimento nos dias atuais, mas a necessidade de revisitar o seu protagonismo no regime da proteção de dados pessoais. Em face da complexidade e das rápidas mudanças inerentes a esse âmbito (ALBERS, 2014), conclui-se ser imprescindível pensar o consentimento do titular dos dados ao lado do conjunto de instrumentos regulatórios disponíveis e do plexo de atores envolvidos.

O artigo está dividido em três partes, além desta introdução e das considerações finais. Na primeira parte do texto, a partir de revisão bibliográfica, apresentam-se os elementos gerais que constituem o paradigma do consentimento na proteção de dados, explorando sua formação e desenvolvimento. Em seguida, na segunda parte, igualmente a partir de revisão bibliográfica, expõem-se três insuficiências vivenciadas por esse paradigma. Primeiro, sua inobservância quanto às limitações cognitivas do titular dos dados capazes de afetar o seu processo decisório de consentir, ou não, com práticas e termos envolvendo dados pessoais. Segundo, a desconsideração das desigualdades de poder existentes entre o agente responsável pelo tratamento[8] de dados pessoais e o titular desses dados. Terceiro, sua menor capacidade em oferecer respostas mais efetivas aos desafios decorrentes, por exemplo, do advento do *Big Data*.

Por sua vez, na terceira parte, combinando revisão bibliográfica com análise documental de legislações como a LGPD (BRASIL, 2018), o RGPD (UNIÃO EUROPEIA, 2016) e o Marco Civil da Internet (BRASIL, 2014), são brevemente exploradas três abordagens que podem ser frutíferas no sentido de superar as referidas insuficiências. Em primeiro lugar, a inserção de princípios da proteção de dados na própria tecnologia. Em segundo lugar, a instauração de uma regulação pautada pelas ideias de risco e de *accountability*. Em terceiro lugar, o estabelecimento de limites materiais em torno do consentimento, responsivos ao contexto particular do tratamento de dados em questão.

Em síntese, o artigo perpassa brevemente pelas respectivas questões: *(i)* em que consiste o paradigma do consentimento? *(ii)* quais são suas insuficiências para lidar com o cenário atual que permeia a proteção de dados pessoais? e *(iii)* quais instrumentos e estratégias regulatórias podem ser úteis para atenuar essas

destacados ao longo do texto. Para críticas quanto ao consentimento no RGPD e na LGPD, vide (CAROLAN, 2016; BIONI, 2019).

[8] Segundo o art. 5°, X, da Lei n° 13.709/2018 (BRASIL, 2018), tratamento de dados é toda "operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

insuficiências vividas pelo foco excessivo no consentimento como núcleo da proteção de dados?

2 PRIVACIDADE E PROTEÇÃO DE DADOS: DESENVOLVIMENTO REGULATÓRIO E O PARADIGMA DO CONSENTIMENTO

Pode-se dizer que o sentido do direito à privacidade foi se transformando ao longo do tempo. O início desse debate acadêmico foi marcado fortemente pelo conceito de privacidade como barreira de acesso à vida privada do indivíduo, formando uma garantia de inviolabilidade e de imunidade quanto a certos aspectos da sua vida pessoal e da sua intimidade: uma liberdade individual negativa traduzida como o direito de ser deixado em paz/só (*the right to be left alone*) (WARRE;, BRANDEIS, 1890; BIONI, 2019, p. 125). Essa visão é marcada por uma divisão entre o que é público e o que é privado, conferindo-se proteção jurídica somente ao que é íntimo ou privado e não a fatos considerados de "conhecimento público" (*v.g*. nome, telefone, local de trabalho etc.).

Subjacente a essa perspectiva, portanto, é a existência de duas esferas dicotômicas ("público/privado") constituindo a própria razão de ser da privacidade (WHITLEY, 2009, p. 155). De um lado, tem-se a "casa": a esfera privada como espaço íntimo - e por vezes até sigiloso - no qual o indivíduo se refugia do escrutínio público e da própria intervenção estatal. De outro lado, tem-se a "Ágora": a esfera pública como espaço no qual são desenvolvidas as virtudes cidadãs do indivíduo, que se posiciona na sociedade e se expõe (PAIXÃO, 2003). Nesse cenário, o direito à privacidade atua como elemento delimitador dessas duas esferas dicotômicas, permitindo o controle da individualidade.

Não obstante, ao longo das últimas cinco décadas, as discussões jurídicas em torno do direito à privacidade perpassaram por transformações significativas, sobretudo em vista das mudanças tecnológicas que emergiram nesse período e alteraram substancialmente os riscos e as bases fáticas ao seu redor. Assim, a privacidade passou a ser vista não só como uma liberdade negativa que garante o "isolamento do indivíduo", mas também como liberdade positiva: um poder "de *exigir*, por exemplo, conhecimento, controle e disposição de dados relativos à individualidade (...) capazes de afetar autonomia e liberdades" (QUEIROZ, PONCE, 2020, p. 78-79). Nas palavras de Stefano Rodotá (2018, p. 15), ocorreu um verdadeiro "processo inexorável de reinvenção da privacidade" na medida em que novas tecnologias da informação e da comunicação (TICs) penetraram a vida social e as dinâmicas político-econômicas (público e privadas), alterando sensivelmente os fluxos de informação (VERONESE, FONSECA, 2018, p. 43).

Nesse cenário, muitas das discussões regulatórias começaram a se referir ao direito à proteção de dados pessoais (DONEDA, 2019, p. 27), concebido para além de uma mera decorrência da privacidade: um direito fundamental autônomo cujo âmbito de proteção está vinculado à tutela da dignidade e da personalidade dos cidadãos no seio da sociedade da informação (MENDES, 2011, p. 48-51).

De um lado, esse desdobramento histórico se deu em razão da necessidade de expansão e de "atualização" das formas jurídicas de tutela da personalidade dos cidadãos frente às mudanças tecnológicas ocorridas. De outro, estabeleceu-se também enquanto vetor de integração econômica dos países envolvidos e das dinâmicas empresariais multinacionais. Um cenário de fluxo massivo de dados pessoais no espaço virtual e de sofisticação do tratamento informatizado desses dados, tornando-os elemento relevantíssimo no sistema econômico mundial (MENDES; BIONI, 2019).

Exemplo histórico dessa agenda de integração foi justamente a aprovação, em 1980, das *Diretrizes Gerais da OCDE* (Organização para a Cooperação e Desenvolvimento Econômico) *sobre Privacidade e o Fluxo Transfronteiriço de Dados Pessoais*, revisadas em 2013. Com inspiração nas *Fair Information Practices* (FIPs) (GELLMAN, 2019, p. 11), o referido documento assentou as definições gerais, os princípios básicos e a cooperação internacional sobre o tema no bojo dos países membros da OCDE[9].

Para além desse exemplo, no entanto, Colin Bennett (1992, p. 111-112) destaca a existência de um fenômeno de *convergência regulatória* (*policy convergence*)[10] quanto aos dados pessoais, desde a década de 1970: um processo informal, porém relativamente coordenado, pelo qual legislações nacionais e instrumentos normativos internacionais foram se delineando em torno de princípios básicos e de diretrizes gerais para solucionar problemas comuns envolvendo o tratamento e o fluxo de dados pessoais em um mundo digitalmente conectado. Assim, não é exagero afirmar que paulatinamente foram construídos princípios básicos e diretrizes gerais sobre a proteção de dados os quais influenciaram diferentes jurisdições ao redor do mundo (CATE; MAYER-SCHÖNBERGER, 2013, p. 68-69).

Sobretudo a partir da dita "terceira geração"[11] de leis regulando o tema (MAYER-SCHÖNBERGER, 2011), essa convergência se deu em torno de bases teóricas e de fundamentos jurídicos calcados no consentimento: o paradigma do

[9] Segundo o próprio documento, trata-se de uma representação do consenso alcançado entre os países membros da OCDE sobre os princípios básicos a respeito do tema, que devem nortear as novas legislações domésticas, assim como as já existentes. Do original: "They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it." Disponível em: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> Acesso em 01 de março de 2020.

[10] A análise comparada de Colin Bennett sobre essa convergência regulatória perfaz os seguintes países: Estados Unidos, Alemanha, Grã-Bretanha e Suécia (BENNETT, 1992, p. 116-152).

[11] Com maior profundidade analítica, dissertando sobre as "quatro gerações" regulatórias das leis de proteção de dados, vide (MENDES, 2014, Capítulo 1).

consentimento (CATE; MAYER-SCHÖNBERGER, 2013). Nesse contexto, o consentimento passou a ser utilizado para legitimar, justificar e alicerçar a proteção de dados pessoais. Sem se olvidar da variedade de importantes avanços relativizando a ênfase no consentimento como garantia de autonomia e de proteção do titular dos dados, não é forçoso afirmar que o seu protagonismo permaneceu como "traço marcante da abordagem regulatória" (BIONI, 2019, p. 177).[12]

Nesse paradigma, o indivíduo se encontra no centro do processo decisório acerca do que é feito com seus dados pessoais.[13] Entretanto, nos casos em que o tratamento não está explicitamente autorizado por alguma base normativa, na prática, o positivo ideal de empoderamento do titular resulta na obtenção de seu consentimento individual frente aos termos do tratamento, após previamente informado a respeito da finalidade da coleta (*notice and consent*). O instrumento do consentimento tornou-se, assim, vetor dominante na busca pela materialização dessa almejada autonomia do titular dos dados, sobretudo no âmbito da Internet (CATE; MAYER-SCHÖNBERGER, 2013, p. 67-68).

Na prática, então, o consentimento figurou por muito tempo como núcleo de legitimidade jurídica do regime protetivo dos dados pessoais, viabilizando vários tratamentos de dados por entidades públicas e privadas: o indivíduo foi *informado* das práticas? *Consentiu* com o tratamento de dados realizado? Caso positivo, essas práticas e esses tratamentos se tornam legítimos, por terem passado pelo crivo individual do titular (SOLOVE, 2013, p. 1880-1882; DONEDA, 2019, p. 198).

3. INSUFICIÊNCIAS DO PARADIGMA DO CONSENTIMENTO

Não obstante sua importância para o florescimento e consolidação da disciplina normativa voltada à proteção de dados, os pressupostos que delineiam o paradigma do consentimento, atualmente, demonstram-se insuficientes para garantir um regime protetivo *efetivo* e *material*, em especial, para garantir um *verdadeiro controle* sobre o fluxo de dados pessoais pelo seu titular. Nesta seção, serão destacados três pontos que elucidam as insuficiências do consentimento como foco regulatório: (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do

[12] "[T]he basic approach to protecting privacy has remained largely unchanged since the 1970s. Under the current approach, the law provides people with a set of rights to enable them to make decisions about how to manage their data. I will refer to this approach to privacy regulation as 'privacy self-management. '" (SOLOVE, 2013, p. 1880).

[13] "This liberal autonomy principle seeks to place the individual at the center of decision-making about personal information use. Privacy-control seeks to achieve information self-determination through individual stewardship of personal data, and by keeping information isolated from access. [...] The weight of the consensus about the centrality of privacy-control is staggering. " (SCHWARTZ, 2000, p. 820).

titular como, por exemplo, em circunstâncias denominadas de "*take it or leave it*"; e (iii) as modernas técnicas de tratamento e análise de dados a partir de *Big Data* que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido.[14]

3.1 Limitações Cognitivas

A *primeira* insuficiência enfrentada pelo paradigma do consentimento advém de sua abordagem quanto ao próprio titular dos dados e seu processo cognitivo-decisório.

É que, sob tal ótica, esse indivíduo é guiado pela maximização de seus interesses em face dos custos e benefícios envolvidos em consentir, ou não, com os termos que lhe são apresentados. Assim, caso esteja munido de amplo conhecimento acerca do que é feito com seus dados pessoais, poderá sopesar os custos envolvidos para sua personalidade e contrapô-los em face dos benefícios trazidos, por exemplo, pela utilização de um serviço *online*. Por conseguinte, tomará uma decisão sobre o que consentir e o que não consentir na Internet, em seu melhor interesse, após ler os termos de privacidade disponibilizados, por exemplo.

Partindo dessas premissas, o seguinte procedimento se tornou comum: *(i)* informar o titular dos dados pessoais acerca de quais dados estão sendo coletados e como eles serão usados (*notice*); em seguida, *(ii)* permitir com que ele detenha o poder de decidir se aceita, ou não, os referidos usos de seus dados pessoais (*consent*) (SOLOVE, 2013, p. 1883). Com base nas informações disponibilizadas, portanto, pressupõe-se que o indivíduo está apto a tomar decisões racionais, embasadas e efetivamente autônomas.

Ocorre que importantes evidências empíricas trazidas pelas ciências comportamentais têm demonstrado que tais pressupostos nem sempre são adequados[15], especialmente em face de *limitações cognitivas*[16], como vieses e heurísticas[17], que podem dificultar a avaliação dos elementos necessários "para

[14] "Equally challenging is the fact that in the age of 'Big Data', much of the value of personal information is not apparent at the time of collection, when notice and consent are normally given" (CATE; MAYER-SCHÖNBERGER, 2013, p. 67).

[15] "There is a great deal of evidence that few consumers read privacy policies or similar documents, for instance, and that even fewer understand them" (CALO, 2012, p. 1050). "In fact, the psychology and behavioural science research shows that website users are subject to a variety of specific situational influences that intuitively impel the giving of consent." (CAROLAN, 2016, p. 462).

[16] Limites oriundos da racionalidade limitada (*bounded rationality*) dos seres humanos e que são capazes de impactar seu processo decisório, a partir da restrição de sua capacidade em apurar e interpretar informações (FUX; FONSECA, 2020).

[17] Para um dos trabalhos seminais sobre a temática, vide Sunstein e Thaler (2008).

racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais" (BIONI, 2019, p. 224). Por óbvio, não se trata de simplesmente "infantilizar" o titular dos dados, tratando-o como incapaz de decidir por si mesmo ou simplesmente ignorar sua capacidade racional. Porém, o foco excessivo na obtenção de seu consentimento (aparentemente) informado deixa de lado algo mais complexo: a real capacidade do titular dos dados pessoais de substancialmente compreender e avaliar os riscos e prejuízos que poderão advir de seu consentimento, sobretudo *online*.[18] No que diz respeito à privacidade e à proteção de dados, essas limitações cognitivas podem minar substancialmente os pressupostos do "*notice and consent*" (LI, SARATHY; XU, 2011; SOLOVE, 2020, p. 12).

Apesar da grande relevância dada à apresentação de informações pela entidade responsável pelo tratamento de dados[19], estudos têm indicado que, ao tomar decisões sobre sua privacidade e sobre seus dados, os indivíduos muitas vezes sequer leem regularmente as "*Políticas de Privacidade*" ou "*Informações sobre o Uso de Dados*" que lhe são apresentadas (MILNE; CULNAN, 2004), o que pode tornar a medida inócua. Mais do que isso, as informações disponibilizadas costumam ser de difícil compreensão, haja vista a complexidade e sofisticação do tratamento de dados na espécie, envolvendo vários conceitos técnicos e jurídicos ou até mesmo o tamanho das letras e a extensão do texto. Em verdade, o próprio excesso de informações pode ser prejudicial, sobrecarregando a cognição do titular dos dados acerca dos efeitos atinentes às questões apresentadas (MACEDO JUNIOR, 1999, p. 247). Além disso, até mesmo a maneira com que essas regras e essas escolhas são disponibilizadas (*framed*) pode influenciar sensivelmente o processo decisório de se consentir ou não (ACQUISITI, 2009, p. 83).[20]

Nessas situações, o próprio consentimento individual se torna incapaz de corresponder com a vontade real do titular dos dados, pois esse sequer compreende os efeitos que eventual decisão pode causar para os seus direitos de personalidade, tornando a valorização excessiva na obtenção do consentimento expresso dos titulares inadequada para alcançar o objetivo de conferir efetiva autonomia e proteção a eles (ACQUISITI; GROSSKLAGS, 2007, p. 363; BIONI, 2019).

3.2 Desigualdade de poderes e dependência dos serviços da sociedade da informação

[18] "[T]he extent to which individuals can fully understand and meaningfully evaluate the various risks and harms that their personal data might be subject to." (WHITLEY, 2009, p. 156).

[19] Para uma revisão pormenorizada da literatura a respeito do "*notice*" como ferramenta regulatória, formulando uma abordagem construtiva, vide (CALO, 2012).

[20] Para uma análise, em língua portuguesa, sobre as limitações cognitivas no âmbito da proteção de dados, vide os tópicos 4.1.2 e 4.1.3 de (BIONI, 2019).

A *segunda* insuficiência vivenciada pelo paradigma do consentimento advém da desconsideração da assimetria de poderes existente na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados (MENDES, 2014). É que, sob essa perspectiva, o consentimento do indivíduo se apresenta como base legitimadora para praticamente toda a operação de tratamento de dados, independentemente das assimetrias existentes quanto ao poder de barganha das partes, o que poderia prejudicar a tomada de uma decisão realmente livre e autônoma.

Ocorre que, em não raras vezes, o titular dos dados pessoais se encontra em situação de vulnerabilidade nessa relação contratual eletrônica (MARQUES; MIRAGEM, 2012, p. 117). Primeiro, pois, como já dito, os termos das políticas de privacidade podem ser demasiadamente complexos e abstratos, impossibilitando uma compreensão mais transparente a respeito do concreto emprego dos dados. Segundo, porque vários desses termos negociais se baseiam em uma lógica binária[21] "*take it or leave it*": consentir ou não consentir, sem outras opções. Porém, ao não consentir, o custo é o de não desfrutar o serviço almejado, *v.g.*, o uso de uma rede social ou de um aplicativo online (BALKIN, 2018, p. 3).

Dessa forma, mesmo estando exposto a tamanhos riscos, o titular dos dados pessoais pode acabar realizando seu consentimento com base em proveitos tais como: a conexão com suas amizades, a disponibilidade de meios de comunicação em tempo real, a possibilidade de ouvir músicas e assistir filmes etc. Assim, muitas vezes esse consentimento é meramente aparente (SCHWENKE, 2006, p. 58), sendo questionável sua contribuição para o objetivo de proteger o titular dos dados. Dessa forma, coloca-se em dúvida o grau concreto pelo qual ele reflete a *autonomia decisória* desse titular.

Trata-se do cenário retratado por Spiros Simitis (1984, p. 401) no qual o consentimento é meramente uma *ficção*, uma vez que o indivíduo carece de efetiva autonomia decisória para se proteger dos possíveis perigos e danos à sua personalidade. Nessas situações, a decisão individual de consentir não é livre e autônoma ou oriunda da avaliação dos ônus e dos bônus envolvidos. Ao revés, ela se origina de uma verdadeira imposição estabelecida por terceiro: consentir ou simplesmente não desfrutar de serviço/produto, que, muitas vezes, sob a perspectiva do indivíduo, é essencial para a sua sociabilidade ou acesso à informação na era digital.

3.3 Novas tecnologias e o potencial de agregação da informação: impossibilidade de gerenciamento individual dos riscos no momento da coleta dos dados

[21] "That binary choice is not what the privacy architects envisioned four decades ago when they imagined empowered individuals making informed decisions about the processing of their personal data" (CATE; MAYER-SCHÖNBERGER, 2013, p. 67).

A *terceira* insuficiência de uma visão centrada no consentimento advém de sua menor capacidade em oferecer respostas aos desafios decorrentes da "massificação da produção, coleta, armazenamento, tratamento e compartilhamento de dados pessoais" (QUEIROZ; PONCE, 2020, p. 75).

Apesar do nome sugestivo, a proteção de dados não se volta exclusivamente aos dados em si. O seu enfoque protetivo está no *titular* desses dados: quem arcará com os riscos e com as eventuais consequências prejudiciais do uso de seus dados pessoais. Nesse sentido, o papel regulatório é mais amplo: disciplinar a *informação* gerada a partir do processamento e do tratamento dos dados pessoais, em um devido contexto.[22] São as informações extraídas a partir desses dados, e não eles próprios, que formarão a representação virtual do indivíduo na sociedade. Os dados precisam ser processados e organizados para a extração dessas informações. A partir delas, por exemplo, são geradas decisões ou interpretações que podem ampliar ou reduzir as oportunidades do titular no mercado, formatar sua "imagem" perante os setores público e privado, bem como desenvolver sua personalidade dentro da comunidade digital.

Conforme bem elucidam Viktor Mayer-Schönberger e Kenneth Cukier (2014, p. 5-7), em um cenário marcado pelo *Big Data*, o tratamento dos dados pessoais não pode ser visto como algo estático, cuja utilidade político-econômica se exaure no momento em que alcançada a finalidade para que foram coletados, como a realização de um censo pelo Governo ou uma operação de determinada empresa privada. Ao contrário, com tecnologias que se utilizam de *Big Data*, inteligência artificial e algoritmos é possível extrair novas informações totalmente descoladas da finalidade original que ensejou a coleta desses dados. A partir do posterior processamento, cruzamento e análise de grandes bancos de dados, pode-se gerar novas formas de valor político-econômico com o condão de impactar difusamente toda a sociedade e afetar sensivelmente o próprio regime democrático, tal como observado nos escândalos eleitorais envolvendo a *Cambridge Analytica* (CARVALHO; GUIMARÃES; OLIVEIRA, 2018, p. 385).[23]

Dados considerados "irrelevantes" ou "públicos" como idade, altura, nacionalidade, os locais de moradia e de trabalho podem servir de insumo para correlações, predições e ranqueamentos acerca da personalidade do titular dos dados pessoais ou de determinados grupos sociais (O'NEIL, 2018). Essas decisões

[22] "The goal of data protection is not the protection of data but of the individuals to whom the data refer. The object of protection, then, is not the personal data per se. […] Nonetheless, data are not meaningful per se, but rather as 'potential information'." (ALBERS, 2014, p. 222).

[23] Em linhas gerais, essa empresa britânica teria coletado dados pessoais de até oitenta e sete milhões de usuários do *Facebook* e, segundo investigações conduzidas, também teria os utilizado para influenciar pleitos eleitorais ao redor do mundo, sobretudo (i) as eleições dos EUA de 2016 e (ii) o referendo do "Brexit" no Reino Unido (VERONESE, FONSECA, 2018).

possuem a capacidade prática de determinar "a vida das pessoas: desde a seleção de currículos para uma vaga de emprego, chegando até os seguros, acesso ao crédito e serviços do governo" (TEFFÉ; MEDON, 2020, p. 309-311).

Em suma, a criação de detalhados perfis a respeito dos cidadãos pode criar sérios riscos à sua personalidade na medida em que essas representações virtuais têm o condão de diminuir ou de aumentar oportunidades sociais "em aspectos centrais da vida humana" como "emprego, moradia, crédito, justiça criminal" (QUEIROZ; PONCE, 2020, p. 81-82), justamente de acordo com a classificação ou o *score* conferido ao seu perfil. Dessa maneira, dados inexatos ou incompletos e vieses do programador do algoritmo, por exemplo, podem gerar predições, inferências e interpretações verdadeiramente discriminatórias acerca de um indivíduo ou de um segmento social (MENDES; MATTIUZO, 2019, p. 40-41).

Ademais, o fluxo desses dados perpassa por uma complexa rede de atores que os utilizam por meio de práticas e de operações com fins diversos. É impossível que o titular de dados tenha conhecimento prévio de todos esses elementos, não só por limitações de cognição, mas também por questões estruturais (SOLOVE, 2013). É dizer: seja pela escala em que a informação é processada, seja pela enorme capacidade de agregação da informação pelas novas tecnologias, é improvável que o indivíduo, no momento da coleta, gerencie plenamente algo que ocorrerá no futuro e que envolve inúmeras incertezas acerca de como todas as informações e dados acerca de um indivíduo serão agregados, cruzados ou utilizados.

Por conseguinte, apesar de o dado em si permanecer importante ponto de referência regulatória para a disciplina da proteção de dados pessoais, é preciso observar essa cadeia mais ampla e pensar na regulação global dos seus usos, que vão muito além do processo de coleta inicial: as informações geradas a partir de seu processamento; as decisões tomadas a partir dessas informações; e, sobretudo, os efeitos adversos oriundos dessas decisões, porque capazes de afetar a vida e liberdade dos indivíduos envolvidos (ALBERS, 2014, p. 222-224).

Logo, não se trata de limitar todo e qualquer tipo de tratamento de dados ou de simplesmente abandonar o consentimento individual como instrumento protetivo. Ao revés, cuida-se de avaliar sua capacidade para efetivar essa proteção a partir do contexto particular em que inserido. Em um mundo marcado pela tecnologia do *Big Data*, muitas inovações tecnológicas positivas decorrem justamente dessa habilidade de "reutilizar uma mesma base de dados para propósitos diferentes" (BIONI, 2019, p. 317). Entretanto, não se pode deixar de garantir a necessária proteção dos titulares dos dados. Helen Nissenbaum (2010) bem elucida que, para esse objetivo, muito além da legitimação a partir do consentimento individual autorizando a coleta dos dados, a avaliação perpassa pelo respeito à *integridade contextual* (*contextual integrity*) do fluxo desses dados, observando a proteção de dados como vetor de garantia de um fluxo apropriado e esperado à luz das "normas informacionais" aplicáveis ao contexto em debate (*context-relative informational norms*) (NISSENBAUM, 2011, p. 33).

Apesar de não abordar diretamente o uso de *Big Data*, o exemplo oferecido pela autora esclarece bem essa visão contextual (NISSENBAUM, 2011, p. 33-34). No caso de dados sobre a saúde de um paciente, via de regra, espera-se maior zelo e até certa confidencialidade. Caso o profissional da saúde decida compartilhá-los com um especialista de outra área médica a fim de ampliar o diagnóstico ou tratamento necessário, não parece haver violação da integridade contextual: o fluxo foi esperado e apropriado. Todavia, caso haja compartilhamento desses mesmos dados a fim de vantagens econômicas, uma quebra dessa integridade contextual já se apresenta mais visível, se não ocorrer em benefício dos interesses do titular dos dados.

Novos riscos e maneiras de se explorar os dados pessoais demonstram que a proteção de dados deve englobar parâmetros de legitimidade mais amplos do que a existência de um consentimento individual prévio (NISSENBAUM, 2010, p. 140), levando em consideração a compatibilidade entre o contexto da relação e as características do tratamento. Não sendo mero "cheque em branco", o consentimento inicialmente expressado é analisado posteriormente de acordo com as "legítimas expectativas" para o contexto daquele tratamento (BIONI, 2019, p. 322).

Essas "legítimas expectativas" passam a ser avaliadas a partir de elementos como: *(i)* o *contexto* em que a suposta violação ocorreu (qual era o ambiente social que estruturava o fluxo de informações analisado?); *(ii)* os *atores* envolvidos (quem eram os emissores, receptores e sujeitos do fluxo de informação?); *(iii)* os *atributos* da informação analisada (que tipo de informação se estava lidando? Informações médicas, bancárias, preferências pessoais?); *(iv)* os *princípios de transmissão* aplicáveis (quais eram os constrangimentos aplicáveis ao fluxo de informações analisado, ele estava condicionado à confidencialidade, reciprocidade, necessidade?) (NISSENBAUM, 2010, p. 182).

4. TENDÊNCIAS CONTEMPORÂNEAS DE MATERIALIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Como visto na seção anterior, existem diversas situações em que a efetividade do instrumento do consentimento se torna questionável para garantir a autonomia decisória do indivíduo quanto aos seus dados pessoais. Esse déficit, no entanto, não significa o abandono do consentimento como instrumento protetivo. Além disso, tampouco pode figurar como justificativa para a adoção de uma postura puramente paternalista, isto é, simplesmente diminuindo a liberdade do titular dos pessoais à sua revelia. Entre outros fatores, a adoção desse raciocínio pode inviabilizar todo um mercado personalizado e inovador, no âmbito digital, e até mesmo a construção de políticas públicas balizadas por evidências empíricas.

Ao contrário, o que parece mais adequado é a formulação de perspectivas mais complexas e sofisticadas de *autonomia* para além de uma acepção formal, rumando para uma *autodeterminação* do titular dos dados como expressão do livre

desenvolvimento de sua personalidade e de sua própria dignidade (MENDES, 2015). Trata-se de concretizar uma *autonomia material* do indivíduo na proteção de dados pessoais, em linha com as tendências de materialização, expressadas por Claus-Wilhem Canaris como a marca do direito privado no século XX (CANARIS, 2000).

No entanto, mais especificamente para os fins deste trabalho, passo importante é levar em consideração instrumentos, conceitos e estratégias complementares para adequar a proteção de dados pessoais a esse novo cenário, buscando apaziguar as insuficiências mencionadas acerca do foco excessivo no consentimento (SCHERMER; CUSTER; HOF, 2014) e tornando-o mais eficaz (CATE; MAYER-SCHÖNBERGER, 2013, p. 69).

Nesta seção, serão brevemente exploradas três abordagens, já adotadas por atuais legislações de proteção de dados e discutidas em alguns trabalhos acadêmicos, que podem ser importantes nesse sentido: (i) a proteção de dados por meio da tecnologia; (ii) a análise de risco e a instauração de uma regulação pautada pela ideia de accountability; e (iii) o estabelecimento de limites materiais em torno do consentimento.

4.1 Proteção de dados por meio da tecnologia e da arquitetura dos sistemas informacionais

Desde muito, Lawrence Lessig (1999) vem ressaltando o fato de que o direito não é o único vetor regulador da Internet. De outra sorte, ele convive com outras dimensões responsáveis para tanto: as constrições sociais, as dinâmicas do mercado privado e a própria tecnologia, a qual é capaz de estabelecer arquiteturas e *designs* que podem propiciar um espaço virtual tanto favorável quanto desfavorável à fruição de direitos fundamentais como liberdade, igualdade e privacidade. Novas tecnologias não possuem apenas efeitos benefícios *ou* efeitos maléficos, elas são "um fardo *e* uma benção"[24] capazes de propagar ambos os efeitos, a depender da forma em que concebidas e utilizadas. Por um lado, é bem verdade que as inovações tecnológicas têm gerado grandes riscos à personalidade dos indivíduos. Por outro lado, elas podem ser verdadeiras ferramentas em favor dessa proteção.

Nessa linha, Julie Cohen (2000, p. 1436-1437) esclarece a necessidade de se utilizar tecnologia e direito no estabelecimento de melhores condições para permitir escolhas substancialmente autônomas. Sozinho, o direito não consegue estruturar completamente um ambiente virtual favorável à proteção de dados. Entretanto, a tecnologia também não é exclusivamente capaz de "proteger os cidadãos de violações e ofensas a direitos fundamentais" (ZANATA, 2015, p. 465). Assim, aliá-los de forma complementar é essencial para estruturar parâmetros regulatórios e institucionais compatíveis com os valores ético-sociais e os preceitos

[24] Tradução livre de "Every technology is both a burden and a blessing; not either-or, but this-and-that" (POSTMAN, 1992, pp. 4-5).

jurídicos de determinada sociedade. Nesse sentido, importante tarefa é, por exemplo, incentivar o desenho de sistemas tecnológicos seguros e assegurar a presença dos princípios que guiam a proteção de dados não só nas leis e/ou nos termos contratuais, mas também nos sistemas tecnológicos utilizados para tanto (RUBINSTEIN, 2011).

Trata-se de estimular a incorporação da ideia de *autodeterminação informativa*[25] nos sistemas, códigos, arquiteturas e procedimentos tecnológicos: aplicar o direito fundamental à proteção de dados na concepção e na aplicação das tecnologias que permeiam os serviços e produtos disponíveis aos usuários. É que, em ordem de se alcançar um consentimento material e efetivo, antes é preciso preencher diversas condições tecnológicas para tanto. Em especial, ao máximo quanto tecnologicamente possível, (i) aumentar a confiança dos indivíduos no sistema utilizado e no tratamento de dados realizado, assegurando que ambos serão livres e adequados, longe de manipulações, interceptações ou acessos indevidos, bem como (ii) permitir com que o titular dos dados possa configurar e determinar suas preferências acerca do que é feito com os desdobramentos virtuais de sua personalidade (MENDES, 2013, p. 246).

É o que suscitam, por exemplo, os princípios da segurança e da prevenção, respectivamente, art. 6°, incisos VII e VIII da LGPD (BRASIL, 2018). O primeiro angariando a confiança dos indivíduos quanto aos sistemas de informação, por meio de medidas técnico-administrativas aptas a coibir acessos não autorizados aos dados pessoais, bem como efeitos adversos oriundos de situações acidentais ou ilícitas. Já o segundo incorporando, na própria tecnologia, medidas técnicas capazes de prevenir a ocorrência de danos à personalidade dos indivíduos em face de tratamentos de dados pessoais.

Esse é também o propósito das PETs (*Privacy Enhancing Technologies*), tecnologias que reforçam a proteção de dados pessoais e/ou simplesmente são facilitadoras da fruição desse direito. As PETs podem auxiliar nessa complexa tarefa de "regenerar a atrofiada estratégia regulatória" caracterizada pelo extenso uso do "consentimento do titular da proteção de dados pessoais" (BIONI, 2019, p. 204-207).

Alguns exemplos atuais merecem destaque, como a "criptografia de ponta a ponta" [26] utilizada por aplicativos como o Whatsapp a fim de converter mensagens de texto, voz e vídeo em dados cifrados. Assim, apenas os participantes da comunicação (as "pontas" representadas pelo emissor e receptor ou o grupo envolvido) podem decifrá-los (ABREU, 2017, p. 26). Nesse sentido, a medida é benéfica à proteção de dados ao aumentar a confiança dos seus usuários e a segurança do sistema tecnológico, impedindo ou dificultando acessos indevidos.

[25] Para as múltiplas interpretações acerca do conceito, vide (MENDES, 2014; 2015; BIONI, 2019).

[26] Para as complexas discussões envolvendo os argumentos a favor e contra esse tipo de criptografia, vide (ABREU, 2017).

Os mecanismos de gerenciamento de privacidade pelo usuário também constituem exemplo relevante. O *Google Dashboard* atua como uma "central de gerenciamento" que busca esclarecer, de forma mais acessível e concentrada, de que modo os serviços da empresa utilizados pelo titular dos dados têm efetivamente armazenado seus dados pessoais, permitindo assim a configuração personalizada de opções diversas de coleta e uso de dados (CALO, 2012, p. 1043-1044).

Enfim, as PETs e outras iniciativas envolvendo a própria tecnologia, embora estejam ainda em fase de desenvolvimento, representam inovações promissoras que muito podem contribuir para aumentar a efetividade da proteção do titular dos dados pessoais e para melhor amparar o seu consentimento (CALO, 2012, p. 1044). A ideia de que o próprio sistema deve concretizar o conceito de autodeterminação informativa é fundamental e deve continuar direcionando futuras inciativas.

4.2 Análise de Risco e Accountability

Conforme elucidam Colin Bennett e Charles Raab (2018), uma grande tendência incorporada nas contemporâneas legislações de proteção de dados é a de se apegar aos conceitos de *risco* e de *accountability*. [27] Trata-se da ideia de que a responsabilidade pela proteção de dados pessoais em um complexo ambiente digital deve ser compartilhada entre todos os atores, não podendo ficar restrita ao gerenciamento individual do titular por meio exclusivo do seu consentimento.

No atual contexto tecnológico e social de um complexo tratamento de dados por meio de *Big Data* e de algoritmos de seleção e predição, cresce a importância de se adotar uma análise prévia dos riscos oferecidos pelo tratamento de dados em questão (*risk analysis*). Por meio dela, é possível adotar medidas de segurança compatíveis com o grau de probabilidade relacionado à ocorrência de "impactos, ameaças ou danos" a direitos e a liberdades (CIPL, 2016, p. 14).[28] Para tanto, as legislações mais recentes têm buscado distribuir responsabilidade e deveres de transparência entre os atores envolvidos, com foco especial no agente responsável pelo tratamento dos dados, seja ele público ou privado.

No cenário europeu, o artigo 18 da antiga Diretiva sobre proteção de dados (Diretiva 95/46/CE) estabelecia, aos agentes de tratamento, a obrigação de notificar todas as suas atividades para as autoridades de controle. De outra sorte, o novo Regulamento Geral de Proteção de Dados (RGPD) confere um "voto de confiança" a esses agentes e fixa o *risco* como crivo para essas notificações: elas são necessárias

[27] "While the labels remain the same, however, the conceptual foundations for their legitimation and justification are shifting as a greater emphasis on accountability; risk; ethics and the social/political value of privacy have gained purchase in the policy community." (BENNETT; RAAB, 2018).

[28] Para uma análise da operacionalização dessa *análise de risco* na proteção de dados, vide (GELLERT, 2017).

somente quando o tratamento puder gerar "alto risco para os direitos e liberdades fundamentais" (Considerando n° 89 do RGPD).

Outro exemplo da realidade europeia é a apresentação de relatórios de impacto à proteção de dados (*privacy impact assessments*) por parte desses agentes. No ponto, o art. 35, 1, do RGPD é claro: "quando um certo tipo de tratamento [...] for suscetível de implicar elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento", antes de inicia-lo, deverá elaborar tal relatório de avaliação de impacto. Tendo o risco como fator central, esses relatórios são obrigatórios, *v.g.*, caso o tratamento envolva dados sensíveis do titular (art. 35, 3, "b"), tendo em vista a magnitude dos possíveis danos à personalidade dos indivíduos causados por usos indevidos de dados enquadrados nesta categoria[29].

No Brasil, a LGPD também prevê a necessidade de se elaborar os relatórios de impacto à proteção de dados quando os "processos de tratamento de dados pessoais" possam "gerar riscos às liberdades civis e aos direitos fundamentais" (art. 5°, XVII). Nesse diapasão, o controlador (agente competente para tomar as decisões atinentes ao tratamento de dados) deverá não só descrever esses processos, como também apresentar "medidas, salvaguardas e mecanismos de mitigação" dos riscos identificados.

Percebe-se, portanto, uma mentalidade regulatória pautada pela ideia de *accountability* na proteção de dados.[30] Mais do que prever direitos, são necessárias condições institucionais para garanti-los a partir da atuação dos múltiplos atores envolvidos. Essas obrigações relacionadas à implementação de medidas de segurança preventivas demandam participação ativa dos próprios agentes responsáveis pelo tratamento, tanto nas estratégias de combate e de mitigação dos riscos gerados por suas atividades, quanto na maior transparência ao conduzir esses tratamentos. A ideia subjacente é a de se construir um modelo regulatório híbrido e multifocal (ARANHA, 2019, p. 99-147), no qual os diversos atores envolvidos "compartilham responsabilidade pela elaboração e cumprimento" (ZANATTA, 2015, p. 448) dos parâmetros de proteção de dados pessoais por meio de instrumentos legislativos ou por via de iniciativas voluntárias por exemplo (CIPL, 2018, p. 4).

De um lado, confere-se maior liberdade a esses agentes, que deverão se reportar às autoridades somente quando houver um efetivo risco envolvido, bem como quando esse risco não puder ser mitigado por medidas tecnológicas empregadas

[29] Segundo o art. 5°, I, da LGPD (BRASIL, 2018), a categoria "dado sensível" engloba o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

[30] Segundo o CIPL (2020, p. 5), a *accountability* na proteção de dados possui sete elementos centrais: liderança e direção; análise de risco; políticas e procedimentos; transparência; treinamento e consciência; monitoramento e verificação; responsividade e *enforcement*.

por eles ou pelo desenvolvimento de cláusulas-padrão e normas corporativas globais validadas por selos, certificados e códigos de conduta (art. 33, II, LGPD). De outro lado, essa liberdade demanda também maior responsabilidade e transparência. Assim, esses agentes prestam conta aos titulares de dados e à autoridade independente, por exemplo, *(i)* demonstrando a "adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais" (art. 6°, X, LGPD), bem como *(ii)* apresentando-lhes "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento" (art. 6°, VI, LGPD).

4.3 Limites materiais e contextuais da proteção de dados

Abordagens preventivas e procedimentais, todavia, podem ser combinadas com considerações éticas e limites jurídicos (BENNETT; RAAB, 2018, p. 29) sobre as formas de coleta, uso e tratamento dos dados, bem como ao próprio consentimento (MENDES, 2015, p. 92).

No paradigma do consentimento, os ideais de autonomia e de empoderamento individual assumem, diversas vezes, contornos meramente formais. Desconsideram-se questões envolvendo o contexto em torno do consentimento e do tratamento em questão, tais como os perigos acerca da *natureza* dos dados envolvidos. Nesse cenário, o consentimento se torna um modo conveniente de viabilizar a coleta e o uso de dados sem, contudo, "confrontá-los com os valores centrais em jogo"[31]. Afinal, caso derive de uma decisão em que a livre vontade do titular dos dados é sensivelmente questionável, torna-se igualmente questionável a capacidade do consentimento em garantir esses ideais de autonomia e de empoderamento.

Nesse sentido, institutos civis já estabelecidos, relacionados aos vícios de vontade e aos abusos de poder ou a cláusulas gerais como a boa-fé e a tutela da confiança, podem ser utilizados na busca pela materialização dessa autonomia e na análise do consentimento frente ao contexto em que realizado (KOHTE, 1985, p. 234; MENDES, 2015, p. 84). O Marco Civil da Internet (Lei n° 12.965), por exemplo, determina que serão nulas, de pleno direito, as cláusulas negociais que violem a privacidade e a liberdade de expressão (art. 8°, *caput* e §1°). De igual maneira, a LGPD condiciona a legitimidade e legalidade do tratamento de dados à observância da boa-fé (art. 6°, *caput*) vedando que ele ocorra "mediante vício de consentimento" (art. 8°, §3°) ou que possua "fins discriminatórios, ilícitos ou abusivos" (art. 6°, IX).

O intuito é *adequar* o consentimento com a finalidade do tratamento, porém não de forma rígida, mas sim de acordo com o contexto em que inseridos. Nesse equilíbrio, a própria natureza dos dados é levada em consideração. Caso

[31] Tradução livre de "Consent often becomes a convenient way to reach outcomes without confronting the central values at stake." (SOLOVE, 2013, p. 1903).

enquadrados como sensíveis, a análise do consentimento e do tratamento ocorre a partir de parâmetros mais rígidos quanto à sua forma e à sua finalidade. Enseja-se, assim, maior cautela na própria formação de bancos de dados, pretendendo garantir qualidade, exatidão, clareza e atualização dos elementos que os compõem. Nas palavras de Solon Barocas e de Helen Nissenbaum (2014, p. 66):

> Chegou a hora de contextualizar o consentimento, dando maior foco ao panorama [em que inserido]. Chegou a hora de explorar e de enriquecer o *background* dos direitos, obrigações e legítimas expectativas para que o consentimento possa cumprir com o seu papel adequado.[32]

A imposição de limites materiais não aponta para banir o consentimento ou inviabilizar importantes processos de tratamento de dados.[33] Trata-se, ao revés, de revitalizar o consentimento como instrumento legítimo para o tratamento de dados, deslocando-o de um mecanismo meramente formal para um instrumento imerso no contexto real. Vale lembrar que o próprio conceito de "legítimo interesse do controlador" (SOUZA; VIOLA; PADRÃO, 2019), estabelecido como base legal na LGPD e no Regulamento Europeu, busca considerar elementos materiais e concretos do tratamento de dados, ao prever o balanceamento entre os direitos do titular e os interesses do agente de tratamento.

Embora se possa argumentar uma maior abertura para conceitos subjetivos, trata-se de medida extremamente importante para a efetividade da proteção de dados contemporânea, pois permite que a intensidade dos critérios de avaliação do consentimento seja responsiva à realidade, uma vez que os seus contornos fático-tecnológicos se alteram com constância e vão muito além do que rígidos e fixos aspectos jurídicos podem captar.

5. CONSIDERAÇÕES FINAIS

Ao longo das últimas cinco décadas, o tema da proteção de dados pessoais ganhou considerável espaço nas discussões acadêmicas, bem como se tornou um assunto de grande relevância nas agendas regulatórias e empresariais. Nesse período, várias mudanças tecnológicas ocorreram e, por conseguinte, alteraram estruturalmente as dinâmicas relacionadas ao tratamento e ao fluxo de dados pessoais no mundo, assim como seus usos e finalidades. Em atenção a esse cenário, o presente artigo buscou reforçar a necessidade de se revisitar os pressupostos e as

[32] Tradução livre de "It is time to contextualize consent by bringing the landscape into focus. It is time for the background of rights, obligations, and legitimate expectations to be explored and enriched so that notice and consent can do the work for which it is best suited."

[33] "The law should develop and codify basic privacy norms. Such codification need not to be overly paternalistic" (SOLOVE, 2013, p. 1903).

bases que nortearam o desenvolvimento da disciplina normativa voltada à proteção de dados pessoais, com destaque para o enfoque no consentimento como seu núcleo prático essencial.

O objetivo foi explorar as insuficiências trazidas por um paradigma de proteção de dados com ênfase excessiva no consentimento para, em seguida, apresentar outros instrumentos e estratégias que podem auxiliar na tarefa de enfrenta-las.

No tocante às insuficiências, destacou-se primeiramente as limitações cognitivas do titular dos dados no ambiente *online*. Em segundo lugar, mencionou-se a assimetria de poderes existente na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados. Nesse contexto, o consentimento pode ser meramente uma *ficção*: consentir ou simplesmente não desfrutar de serviço/produto, que, muitas vezes, é essencial para a sua sociabilidade, para o seu trabalho, e até para o acesso à informação. Em terceiro lugar, destacou-se o potencial de novas tecnologias, sobretudo apoiadas em *Big Data*, que tornam improvável o gerenciamento pelo indivíduo, no momento da coleta, dos riscos futuros advindos do potencial de agregação da informação.

Para superar essas insuficiências, tendências contemporâneas de materialização da proteção de dados apresentam-se como soluções interessantes, tornando-a mais responsiva tanto aos riscos gerados pelo tratamento, como aos obstáculos concretos a uma decisão livre e autônoma. Neste texto, exploraram-se três caminhos nesse sentido: (i) por meio da tecnologia e do desenho dos sistemas informacionais (*privacy by design*), que podem auxiliar o titular no controle de seus dados; (ii) por meio de um sistema robusto de prestação de contas pelos agentes de tratamento (*accountability*), apto a dimensionar os riscos prévios ao tratamento de dados pessoais; e (iii) por meio do controle substantivo e contextual do consentimento.

Nesse contexto, a garantia da autodeterminação informativa continua a ser importante objetivo da proteção de dados pessoais. Essa autodeterminação, contudo, somente pode ser concretizada quando considerados os limites resultantes do fenômeno da informação e de contextos sociais que muitas vezes impossibilitam a tomada de uma decisão livre pelo indivíduo (MENDES, 2015). Uma proteção de dados pessoais efetiva precisa ir além da garantia meramente formal do consentimento individual. É preciso garantir os pressupostos materiais dessa proteção para se construir um espaço de liberdade no qual o indivíduo esteja apto a configurar as suas relações informacionais.

REFERÊNCIAS

ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, pp. 24-42, 2017.

ACQUISITI, Alessandro; GROSSKLAGS, Jens. **What Can Behavioral Economics Teach Us About Privacy**? *In:* ACQUISITI, Alessandro; GRITZALIS, Stefano; LAMBRINOUDAKIS, Costos; VIMERCATI, Sabrina. (Edit.). **Digital Privacy**: Theory, Technologies, and Practices, Boca Raton: Auerbach Publications, 2007.

ACQUISITI, Alessandro. Nudging privacy: The behavioral economics of personal information. **IEEE Security & Privacy** v. 7, n. 6, pp. 82–85, 2009.

ALBERS, Marion. **Realizing the Complexity of Data Protection**. *In:* GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Edit.). **Reloading Data Protection**: Multidisciplinary Insights and Contemporary Challenges. Berlin: Springer, 2014.

ARANHA, Marcio Iorio. **Manual de Direito Regulatório**. 5. ed. London: Laccademia Publishing, 2019.

ARANHA, Marcio Iorio; LOPES, Othon. **Estudo sobre Teorias Jurídicas da Regulação apoiadas em incentivos**. Pesquisa e Inovação Acadêmica sobre Regulação apoiada em Incentivos na Fiscalização Regulatória de Telecomunicações, ANATEL/UnB, 2019.

BALKIN, Jack M. Fixing Social Media's Grand Bargain. **Hoover Working Group on National Security Technology, and Law**, Aegis Paper Series n. 1814, October 2018.

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

BENNETT, Colin J. **Regulating Privacy**: Data Protection and Public Policy in Europe and the United States. Ithaca: Cornell University Press, 1992.
BENNETT, Colin; RAAB, Charles D. **Revisiting "The Governance of Privacy"**: Contemporary Policy Instruments in Global Perspective. August, 2018. Disponível em: <https://ssrn.com/abstract=2972086>. Acesso: 05 de abril de 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL, **Lei n. 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso: 10 de março de 2020.

BRASIL, **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso: 10 de março de 2020.

CALO, M. Ryan. Against notice skepticism in privacy (and elsewhere). **Notre Dame Law Review**, v. 87, issue 3, p. 1027-1072, 2012.

CANARIS, Claus-Wilhelm. Wandlungen des Schuldvertragsrechts – Tendenzen zu seiner „Materialisierung". **Archiv für die civilistische Praxis,** v. 200, p. 273, 2000.

CAROLAN, Eoin. The continuing problems with online consent under the EU's emerging data protection principles. **Computer Law & Security Review**, v. 32, n. 3, p. 462-473, June 2016.

CARVALHO, Victor Miguel Barros de; GUIMARÃES, Patrícia Borba Vilar; OLIVEIRA, Adriana Carla Silva de. Monetização de dados pessoais na Internet: competência regulatória a partir do Decreto n° 8.771/2016. **REI - Revista Estudos Institucionais**, Rio de Janeiro, v. 4, n. 1, p. 376-416, ago. 2018.

CATE, Fred H; MAYER-SCHÖNBERGER, Viktor. Notice and consent in a world of Big Data. **International Data Privacy Law**, v. 3, n.2, p. 67-73, 2013.

CIPL, Centre for Information Policy Leadership. **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. CIPL GDPR Interpretation and Implementation Project, 21 December 2016.
CIPL, Centre for Information Policy Leadership. **The Case for Accountability:** How it Enables Effective Data Protection and Trust in the Digital Society. Discussion Paper 1, 23 July 2018.

CIPL, Centre for Information Policy Leadership**. What Good and Effective Data Privacy Accountability Looks Like**: Mapping Organizations' Practices to the CIPL Accountability Framework**.** Report of the CIPL Accountability Mapping Project, May 2020.

COHEN, Julia. Examined Lives: Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, p. 1373-1438, 2000.

DONEDA, Danilo. **Da privacidade à proteção de dados**. São Paulo: Revista dos Tribunais, 2019.

FUX, Luiz; FONSECA, Gabriel Campos Soares da. **Regulação e "Nudge**": como a economia comportamental (*behavioral economics*) pode influenciar políticas regulatórias? *In:* FONSECA, Reynaldo Soares da; COSTA, Daniel Castro Gomes da. (Coord). **Direito Regulatório**: desafios e perspectivas para a Administração Pública. Belo Horizonte: Fórum, 2020.

GELLERT, Raphael. **Understading the risk-based approach to data protection**: an analysis of the links between law, regulation, and risk. Bruxelas: Vrije Universiteit Brussel, 2017.

GELLMAN, Robert. **Fair Information Practices**: a basic History. October 7, 2019, p. 11. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020> Acesso: 10 de março de 2020.

KOHTE, Wolfhard. Die Rechtfertigende Einwilligung. **Archiv für die civilistische Praxis**, v. 185, n. 2, 1985.

LI, Han; SARATHY, Rathindra; XU, Heng. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. **Decision Support Systems**, v. 51, issue 3, pp. 434-445, June 2011.

MACEDO JÚNIOR, Ronaldo Porto. Privacidade, mercado e informação. **Justitia**, São Paulo, v. 61, n. 185/188, pp. 245-259, jan./dez. 1999.
MARQUES, Claudia Lima; MIRAGEM, Bruno. **O Novo Direito Privado e a Proteção dos Vulneráveis**. São Paulo: Revista dos Tribunais, 2012.

MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. *In:* AGRE, Philip E.; ROTENBERG, Marc. (Edit.). **Technology and privacy**: the new landscape. Cambridge: The MIT Press, 2001.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data:** A Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2014.

MCDONALD, Aleecia M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for the Information Society**, v. 4, p. 543-568, 2008.

MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. **Revista de Direito do Consumidor**, São Paulo, v. 22, n. 90, nov./dez. 2013.

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. **Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung**: Eine Analyse der Rechtmäßigkeit der Datenverarbeitung im Privatrecht. Berlin: De Gruyter, 2015.

MENDES, Laura Schertel; BIONI, Bruno R. **O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira**: mapeando convergências na direção de um nível de equivalência. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados e suas repercussões no direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel; MATTIUZO, Marcela. Discriminação Algorítmica: conceito, fundamento legal e tipologia. **Revista de Direito Público**, Porto Alegre, v. 16, n. 90, pp. 39-64, nov./dez. 2019.
MILNE, George R; CULNAN, Mary J. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. **Journal of Interactive Marketing**, v. 18, issue 3, pp. 15-29, 2004.

NISSENBAUM, Helen. **Privacy in Context:** Technology, Policy, and the Integrity of Social Life. Palo Alto: Stanford University Press, 2010.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. **Daedalus, the Journal of the American Academy of Arts & Sciences,** v. 140, n.4, pp. 32-48, Fall 2011.

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. London: Penguin Books, 2018.

PAIXÃO, Cristiano. **Arqueologia de uma distinção** - o público e o privado na experiência histórica do direito. *In*: OLIVEIRA PEREIRA, Claudia Fernanda (org.). ***O novo direito administrativo brasileiro***. Belo Horizonte: Forum, 2003.

POSTMAN, Neil. **Technopoly**: The Surrender of Culture to Technology. New York: Vintage Books, 1992.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, n.1, v. 1, p. 64-90, 2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUBINSTEIN, Ira S. Regulating Privacy By Design. **Berkeley Technology Law Journal**, v. 26, pp. 1409-1456, 2011.

SCHERMER, Bart W; CUSTERS, Bart; HOF, Simone van der. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. **Ethics and Information Technology**, v. 16, pp. 171-182, 2014.

SCHWARTZ, Paul M. Internet Privacy and the State. **Connecticut Law Review**, v. 32, pp. 815-859, 2000.

SCHWENKE, Mathias. **Individualisierung und Datenschutz**. Wiesbaden: Deutscher Universitäts-Verlag, 2006.

SIMITIS, Spiros. Die informationelle Selbstbestimmung. Grundbedingung einer verfassungskonformen Informationsordnung. **Neue Juristische Wochenschrift**, v. 37, pp. 398-405, 1984.

SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, v. 126, pp. 1880-1903, 2013.

SOLOVE, Daniel J. **The Myth of the Privacy Paradox**. GWU Legal Studies Research Paper no. 2020-10**,** 2020. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265> Acesso: 10 de março de 2020.

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na Lei Geral de Proteção de Dados Pessoais. **Revista Direito Público**, Porto Alegre, v. 16, n. 90, 2019.

TEFFÉ, Chiara Spadaccini; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca de inteligência artificial na tomada de decisões empresariais. **REI - Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 1, p. 301-333, abr. 2020.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, 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 Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>. Acesso: 10 de março de 2020.

VERONESE, Alexandre; FONSECA, Gabriel. Desinformação, *fake news* e mercado único digital: a potencial convergência das políticas públicas da União Europeia com os Estados Unidos para melhoria dos conteúdos comunicacionais. **Cadernos Adenauer**, São Paulo, v. 19, n. 4, p. 35-54, 2018.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, pp. 193-220, December 1890.
WHITLEY, Edgar A. Informational privacy, consent and the "control" of personal data. **Information Security Technical Report**, v. 14, n. 3, pp. 154-159, 2009.

ZANATTA, Rafael A. F. **A proteção de dados entre leis, códigos e programação:** os limites do Marco Civil da Internet. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. **Direito & Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015.