A (IN)EFICIÊNCIA DO CONSENTIMENTO COMO BASE LEGAL DO DIREITO À PROTEÇÃO DOS DADOS PESSOAIS NO CONTEXTO DA LEI 13.709/2018

THE (IN)EFFICIENCY OF CONSENT AS THE LEGAL BASIS OF THE RIGHT TO PROTECTION OF PERSONAL DATA IN THE CONTEXT OF LAW 13.709/2018

ELÍSIO AUGUSTO VELLOSO BASTOS[1]
YASMIN LAISE PIRES PEREIRA[2]

RESUMO

O perigo apresentado pela coleta de dados pessoais originou, a nível nacional, a Lei Geral de Proteção de Dados (LGPD), a qual se utiliza do consentimento, uma de suas bases legais, como principal método protetivo. Contudo, dada a hipervulnerabilidade do cidadão em relação às instituições que tratam seus dados, torna-se necessário identificar se o consentimento cumpre de fato essa agenda protetiva. Para realizar tal análise, o presente trabalho revisitou conceitos fundamentais à proteção de dados, como a privacidade e a autodeterminação informativa, e os relacionou com a base normativa da LGPD. Também se estudou as dificuldades atuais à aplicação do consentimento, relativas tanto ao despreparo do cidadão quanto a falhas redacionais da lei. A metodologia utilizada foi a bibliográfica, correlacionando a doutrina consagrada sobre o tema com o levantamento de pesquisas mais recentes, a fim de analisar com clareza o contexto social, econômico, político e cultural em que tais questões emergem.

Palavras-chave: LGPD; consentimento; autodeterminação informativa.

ABSTRACT

The danger posed by the collection of personal data gave rise, at national level, to a Lei Geral de Proteção de Dados (LGPD), which uses the legal basis of consent as the main protective method. However, given the hyper-

1 Doutor em Direito do Estado pela faculdade de Direito da Universidade de São Paulo (USP). Professor em Direitos Humanos e em Teoria Geral da Constituição (Graduação) e em Teoria da Constituição no Centro Universitário do Estado do Pará-CESUPA. Coordenador do Grupo de Pesquisa Inteligência Artificial, Democracia e Direitos Fundamentais. Procurador do Estado do Pará. Advogado. ORCID iD: https://orcid.org/0000-0001-8183-5920.

2 Graduanda em Direito pelo Centro Universitário do Pará (CESUPA). Estagiária do escritório Bastos & Dias Advogados e Consultores. Membro da 1ª Liga Acadêmica de Direito Econômico e do Consumidor (LADEC), bem como da Liga Acadêmica de Direito Digital (LADDIGI). Membro efetivo do grupo de pesquisa Inteligência Artificial e Direitos Fundamentais e do grupo de pesquisa Análise Econômica do Direito. Monitora bolsista das matérias Teoria Geral da Constituição, Direito Constitucional I e Direito Constitucional II. ORCID iD: https://orcid.org/0000-0003-3592-4580.

Como citar esse artigo:/*How to cite this article*:
BASTOS, Elísio Augusto Velloso; PEREIRA, Yasmin Laise Pires. A (in)eficiência do consentimento como base legal do direito à proteção dos dados pessoais no contexto da lei 13.709/2018. **Revista Meritum**, Belo Horizonte, v. 18, n. 1, p. 55-76, 2023. DOI: https://doi.org/10.46560/meritum.v18i1.8986.

vulnerability of citizens in relation to the institutions that process their data, it is necessary to identify whether consent actually fulfills this protective agenda. In order to carry out such an analysis, the present work revisited the fundamental concepts of data protection, such as privacy and informational self-determination, and related them to a normative basis of the LGPD. The current difficulties in the application of consent were also studied, related to both the citizen's unpreparedness and the law's drafting flaws. The methodology used for the bibliography, correlating the established doctrine on the subject with the survey of more recent researches, in order to clearly analyze the social, economic, political and cultural context in which such questions emerge.

Keywords: *LGPD; consent; informational self-determination.*

REVISTA MERITUM • v.18 • n.1 • p. 55-76 • Jan. - Abr. 2023

1. INTRODUÇÃO

No atual estágio vivenciado pelas transformações industriais, tornou-se coerente a famosa frase de Clive Humby, matemático londrino especializado em ciência de dados, de que "os dados são o novo petróleo" (Hirsch, 2013). Na economia da informação, nada faz mais sentido de que sejam os dados pessoais – que serão processados e tornados em informação – o preço a ser pago, tal qual foi a destruição ambiental à era da economia industrial.

É nesse contexto que surgem as leis de proteção de dados pessoais, e dentre elas, nacionalmente falando, a LGPD. Tendo em vista os prejuízos a nível social e individual que a utilização desregrada de dados pessoais poderia ocasionar – e já ocasiona – aos indivíduos e a certos grupos sociais, essa espécie de regulamentação mostrou-se necessária, buscando frear a utilização indevida dos dados pelo governo e pelo mercado.

Nesse intuito, um dos mais relevantes mecanismos utilizados foi o consentimento, uma das bases legais da LGPD. Tal vetor parte da ideia de que é necessária uma maior participação do indivíduo na destinação de seus dados para, então, ofertar a ele a possibilidade de anuir ou não com sua entrega ao operador. O consentimento funciona, nesses parâmetros, como uma espécie de instrumento de efetivação do direito à proteção de dados.

Contudo, o consentimento pode apresentar sérios problemas de eficiência. Em função da grande assimetria entre as pessoas e os detentores de poder, evidente pela conversão da sociedade da informação na chamada sociedade da vigilância, o indivíduo encontra-se em uma posição de *hipervulnerabilidade*, estando passível de manipulação.

É necessário, nesse contexto, questionar até que ponto o consentimento se configuraria como o exercício da autonomia do indivíduo e uma efetiva proteção de seus dados. Um simples "eu aceito" nas longas e cansativas políticas de privacidade diariamente assinadas de fato manifesta a vontade do usuário? Em que medida é provido a ele conhecimento o suficiente para tomar tal decisão? É possível falar em autonomia da vontade sem a possibilidade de negociar os termos do contrato ou estamos diante de um mero processo de exclusão social cujo filtro é a recusa do titular?

Pensar sobre essas e outras questões foi o que motivou o presente estudo, o qual objetiva investigar, por meio de uma análise acerca das suas dificuldades de aplicação, a eficácia da base legal do consentimento na lei 13.709/18.

Para tanto, o primeiro capítulo irá debruçar-se sobre a importância de proteger-se os dados pessoais por intermédio da explanação dos perigos destinados ao titular, especialmente na

era digital. O segundo capítulo irá destinar-se a uma breve remontagem dos conceitos e do panorama histórico que originaram as leis de proteção de dados, bem como à utilização do consentimento como vetor protetivo desses dispositivos. Já o terceiro capítulo analisará o consentimento em território nacional, ou seja, delineará o consentimento à luz da LGPD. Por fim, o quarto capítulo, central no presente trabalho, identificara os ainda existentes desafios à plena utilização da base legal do consentimento como um verdadeiro processo de tomada de decisão pelo titular dos dados.

2. A IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS

Embora muito se fale sobre o direito à privacidade de dados, principalmente após a emergência e a consolidação do mundo tecnológico, as razões pelas quais ela se faz necessária, são, muitas vezes, pouco claras – talvez, é possível especular, pela própria vontade daqueles que lucram com a desinformação popular de que assim o seja.

A LGPD define dado pessoal como uma "informação relacionada a pessoa natural identificada ou identificável" (Brasil, 2018). Isso significa, em outras palavras, que para se considerar uma informação como dado pessoal, será necessário que ela revele algo sobre o seu titular[3]. Mas, afinal, qual a necessidade de uma lei específica para proteger tais dados?

De fato, a ascensão das tecnologias, especialmente depois de descoberta sua capacidade funcional ao Capitalismo da Informação, suscita a urgência de medidas que protejam a pessoa humana e seus dados das grandes instituições, sejam elas públicas ou privadas, que as desejem obter a ponto de estarem dispostas a causar graves danos ao bem-estar social em prol de sua colheita.

Pegue-se, a exemplo do setor privado, a utilização da publicidade direcionada como uma das principais estratégias de marketing da contemporaneidade. Possibilitado pela ascensão digital-informacional, tal mecanismo consiste na utilização de aparatos tecnológicos para inferir os gostos, as características e as preferências de determinada pessoa para, posteriormente, propor a ela anúncios personalizados de acordo com o seu perfil.

O problema desse modelo, no entanto, decorre dos meios operacionais que utiliza para fomentar o consumo. No que pese certa crença de que a publicidade personalizada seria uma ferramenta proveitosa, baseado no argumento de que a utilidade dos anúncios personalizados poderia gerar comodidade ao consumidor, é preciso sempre considerar o objetivo final do mercado: o lucro. É com base nele que as empresas agem ou deixam de agir, sendo razoável concluir que nem sempre seus interesses se encontrarão alinhados com os anseios populares.

Tal fato pode ensejar, como já o faz, a implantação de mecanismos cruéis para a geração de lucro, tão vorazes e exploratórios quanto à época em que a economia se voltava ao acúmulo de metais preciosos; no entanto, atualmente, sendo as informações sobre a pessoa o bem a

3 No que pese o presente trabalho utilizar ambas as expressões como sinônimos, há uma diferença semântica marcante entre os vocábulos "dado" e "informação". Segundo Doneda (2011), o dado é uma espécie de pré-informação, pois é o conteúdo em sua forma bruta que, após ser tratado – por interpretação, catalogação, dentre outros – passará a ser uma informação. Dito de outra forma, informação é o dado sob o filtro do tratamento que lhe foi concedido.

ser versado pela atual fase capitalista, a tentativa incansável do mercado de apropriar-se delas demonstra-se extremamente perigosa.

As afirmações aqui veiculadas podem ser ilustradas pela utilização de anúncios predatórios, como apontou Cathy O'Neil (2016). Nesse sistema, quanto mais vulnerabilidade o dado coletado puder demonstrar sobre o seu titular, melhor será às empresas. Elas utilizam-se, precisamente, da fragilidade e do desconhecimento dos consumidores para recrutá-los a aderir determinado produto ou serviço, comumente vendendo falsos dados acerca das taxas de sucesso do que se está tentando vender ou das chances de ascensão social. Na tentativa de persuadir a pessoa a aceitar o que está sendo ali proposto, quanto maior a ignorância do recrutado sobre o tema e seu desespero para adquirir algum resultado, maior é a probabilidade do mercado de atingir seus objetivos.

Um grande exemplo dado por O'Neil (2016) desse tipo de publicidade nociva é o do Vatterott College, um instituto estadunidense de treinamento profissionalizante cujas atividades encontram-se, correnta e atualmente, encerradas. Em um relatório do comitê do Senado dos Estados Unidos de 2012 sobre universidades com fins lucrativos[4], expôs-se o, para dizer o mínimo, insensível manual de recrutamento que é concedido aos funcionários responsáveis pelas vendas: "Mãe no seguro-desemprego com filhos. Moças grávidas. Recém-divorciadas. Baixa autoestima. Emprego de baixa renda. Passou por perda recente na família. Tenha sofrido maus-tratos físicos ou psicológicos. Prisão recente. Em recuperação por uso de drogas. Trabalho sem perspectiva – sem futuro".

Esse documento deixa claro o objetivo dessas empresas: utilizar-se da vulnerabilidade para atrair possíveis consumidores aos seus negócios, mais suscetíveis a aceitá-los à medida em que o recrutador maliciosamente se utiliza de suas fraquezas como forma de persuadi-los. Essa estratégia é chamada de "ponto de dor" (O'Neil, 2016). Nela, visa localizar-se o ponto da fraqueza individual para, em prol dos interesses mercadológicos aos quais se busca servir, identificar e recrutar as pessoas mais predispostas a adquirirem determinado produto ou serviço.

Há, nesse cerne, uma demonstração prática do que postulou Stéfano Rodotà ao afirmar que "atualmente, podemos sustentar com segurança que a privacidade mental, a mais íntima esfera, está sob ameaça, violando a dimensão mais reclusa de uma pessoa" (2008). Com a verificação da tentativa mercadológica de invadir a mente das pessoas como forma de alavancar seus lucros, tal qual exposto por O'Neil, a vulnerabilidade de dados pessoais revela-se como um problema gravíssimo à própria dignidade humana.

E engana-se quem acredita tratar-se de um fenômeno exclusivo do setor privado. No famoso caso da Cambridge Analytica, empresa parceira do Facebook (atual Meta Platforms, Inc) à época das eleições presidenciais estadunidenses, os efeitos da utilização de dados demonstraram-se politicamente enviesados (Cadwalladr; Graham-Harrison, 2018). Em meados de 2014, a referida empresa, que trabalhava em conjunto com o time responsável pela campanha política de Donald Trump, utilizou-se da rede social para aplicar, em seus usuários, um teste de personalidade com fins supostamente acadêmicos.

4 Segundo O'Neil (2016), as universidades com fins lucrativos são "fábricas de diploma", geralmente pagas por empréstimos financiados pelo governo, cujas formações dela oriundas não possuem muito valor no mercado de trabalho. Entretanto, seu sucesso se dá exatamente pela utilização da publicidade predatória para captar estudantes, os quais são, majoritariamente, pessoas de classes baixas que aceitam realizar empréstimos para entrar na universidade com a esperança de ascender socialmente.

A real motivação do quiz, no entanto, era bem diferente. Utilizando-se de brechas na política de dados até então utilizada pelo Facebook e desrespeitando os fins aos quais a pesquisa poderia ser aplicada, a Cambridge Analytica coletou dados não só dos usuários que participaram do teste, mas também de todas as pessoas presentes na sua lista de amigos, para direcionar a elas propaganda política personalizada.

Por meio da identificação das inclinações políticas do usuário, já de possível alcance pelo sistema implementado pela empresa para a realização do questionário, direcionava-se a ele conteúdo positivo acerca de um candidato e negativo em relação ao outro, com o objetivo de persuadir o eleitor acerca de seu voto. Estima-se, segundo Christopher Wylie (Cadwalladr; Graham-Harrison, 2018), ex-funcionário da Cambridge Analytica e delator do caso, que 270 mil pessoas realizaram o teste. Isso significa que cerca de 50 milhões de pessoas tiveram seus dados coletados sem autorização, com seus titulares expostos a propaganda política enviesada.

Nesse contexto, para além da necessidade de se proteger os dados pessoais em razão da dignidade humana, salvaguardá-los demonstra-se essencial à própria manutenção das instituições democráticas. À medida em que podem ser utilizadas como artifícios para manipular campanhas políticas e influenciar pessoas a tomar determinadas decisões, tais informações se tornam uma arma social extremamente perigosa.

É exatamente por tais razões, reitera-se, que a urgência de se proteger os dados pessoais se torna evidente e dá luz às leis de proteção de dados. Ao passo em que as vulnerabilidades pessoais são capazes de catalogar as pessoas como se fossem produtos a serem utilizados de acordo com a preferência do cliente – compreendidos como os agentes econômicos ou as classes políticas – e de gerar ao indivíduo danos gravíssimos à sua vontade, personalidade e dignidade, o entendimento não pode ser outro a fim de que necessita haver uma legislação capaz de coibir tais práticas, visando a proteção dos direitos acima elencados.

É nesse sentido que se deu, a nível nacional, a criação da Lei Geral de Proteção de Dados, a qual, como será visto, utiliza-se do consentimento como um dos seus principais vetores normativos. Entretanto, é necessário pensar, dadas as próprias situações aqui retratadas, especialmente ao evidenciar-se a fragilidade do usuário, se essa seria uma forma legítima de proteger os dados do cidadão ou se funciona apenas como uma falsa crença de que se tem poder sobre eles.

3. PRIVACIDADE, CONSENTIMENTO, AUTODETERMINAÇÃO INFORMATIVA E O PERCURSO GERACIONAL DAS LEIS DE PROTEÇÃO DE DADOS: BREVES CONSIDERAÇÕES

É inegável a relação que o direito à proteção dos dados pessoais tem com o direito à privacidade. Mesmo que se configurem como direitos da personalidade distintos entre si – já que ambos têm enfoque no livre desenvolvimento pessoal do indivíduo –, a privacidade desenvolveu um papel fundamental para que esse outro, mais recente, fosse plenamente concebido.

Contudo, é necessário entender que a privacidade pode assumir múltiplos significados a depender, por exemplo, do contexto social ou temporal em que é tratada (Doneda, 2006). Não à toa, ela pode servir de base jurídica para a validação dos mais variados direitos, desde a proteção de dados pessoais, aqui retratada, até a inviolabilidade do domicílio, por exemplo.

Note-se que tais direitos têm propósitos diferentes, mesmo que advindos da mesma acepção fundadora. A inviolabilidade do domicílio possui como pressuposto uma modalidade do direito à privacidade cuja relevância foi acentuada a partir da publicação do artigo *The Right to Privacy* (Warren; Brandeis, 1890).

Os então advogados e autores do estudo reivindicavam a privacidade como forma de condenar a prática de exposição de suas vidas pela imprensa, que, à época, não necessitava de permissão ou não se preocupava em calcular os danos que a veiculação de informações pessoais poderia causar aos envolvidos (Warren; Brandeis, 1890). Dá-se origem, desse modo, ao importante "direito de ser deixado em paz", como âmbito normativo mais relevante da privacidade.

Não é, todavia, sobre essa concepção de privacidade, baseada em uma forte dicotomia entre o público e privado, de que se trata o direito à proteção de dados. Um dentre os vários possíveis entendimentos extraídos da terminologia da palavra é sua importância à formação personalíssima do indivíduo, e, consequentemente, à democracia.

Tal percepção aduz aos requisitos necessários à manutenção de um Estado democrático, pois só é possível haver democracia enquanto houver o pensamento autônomo do indivíduo. Os pensamentos massificados e reproduzidos sem criticidade não revelam, propriamente, ações protetivas à democracia, já que não é possível afirmar que refletem a vontade do povo.

É nesse sentido que a privacidade é necessária, e dá luz ao direito de proteção dos dados pessoais. Em vista da imprescindibilidade de preservar-se a autonomia de pensamento individual para que o sujeito desenvolva suas ideias e as utilize, caso assim deseje, como motor da democracia, deve ser resguardado seu espaço particular. É nele que o indivíduo poderá pensar, desenvolver sua personalidade e suas ideias, para, então, caso queira, levá-las a público.

Altera-se, desse modo, a concepção de privacidade numa esfera binomial de contraposição do público com o privado, à medida em que os interesses aparentemente individuais encontram relevância, também, na vida coletiva. Foi nesse sentido que postulou Stéfano Rodotà:

> "Sob o impulso dado por Louis Brandeis, emergiu uma visão na qual a privacidade foi vista também como uma ferramenta de proteção a minorias e opiniões dissonantes e, portanto, à livre manifestação e ao direito de livremente desenvolver a personalidade. Aqui surge um aparente paradoxo: a forte proteção da esfera privada em última instância não resguarda a privacidade nem a mantém protegida do olhar indesejável; na verdade, permite que crenças e opiniões individuais sejam tornadas públicas livremente. Isto abriu o caminho para aproximar ainda mais a associação entre privacidade e liberdade" (Rodotà, 2008, p. 16).

Passa a ser possível, com base nessas ideias, a superação de um entendimento limitado do direito à privacidade e a reivindicação, em contrapartida, de sua importância para o fortalecimento da democracia, ao passo em que concede o direito à personalidade de forma livre e indiscriminada.

Essa mesma acepção reverbera nas noções de Hannah Arendt (1994), quando afirma que todo pensamento, mesmo em se tratando da esfera pública, necessita de solidão. Para

ser possível desenvolver ideias autônomas e que visem os interesses pessoais e populares – dissociados do que almeja os detentores de poder – é necessário que a esfera privativa se preserve. Afinal, uma ideologia propagada sem a oportunidade de refletir-se sobre ela privativamente é nada mais do que manipulação de massas, como visto em diversos governos autocráticos ao longo do século XX.

Não coincidentemente, foi na segunda metade do referido século que essa noção da privacidade, enquanto um direito da personalidade, ganhou força e embasou a necessidade de proteger-se os dados pessoais. Posto que esses últimos são importantes para a plena construção da personalidade humana, resta evidente que são essenciais à própria manutenção das instituições democráticas, devendo, destarte, ser tutelados. Essa urgência é fortificada, ainda, pelo avanço crescente das novas tecnologias da informação e comunicação (NTIC)[5] e de sua consequente capacidade de gerar poder e capital, tanto aos governos quanto aos setores privados.

No novo panorama econômico emergido no mundo pós-industrial, fortemente marcado pela comercialização utilitarista da informação – vide o capítulo anterior – o direito à privacidade precisou superar seus contornos clássicos para conseguir abarcar todos os perigos apresentados à invasão do espaço pessoal, dando origem, com isso, ao direito à proteção de dados pessoais. À luz das NTIC, esse bem jurídico visa resguardar de que forma as informações pessoais são tratadas e utilizadas na contemporaneidade, haja vista sua capacidade de dano ao titular.

Exatamente nesse momento, em que se buscou formas de normatizar tal direito, é que ocorreu a ascensão do consentimento, entendido como uma manifestação da vontade de seu titular capaz de produzir a proteção de seus dados. Segundo Viktor Mayer-Scönberger (1997), cujo pensamento ressoa na doutrina, existem quatro gerações de leis acerca da proteção de dados pessoais que, de acordo com Doneda (2011, p. 96), são "leis que partem de um cerne mais técnico e restrito para, por fim, ampliar as disposições e as técnicas referentes às tecnologias modernas".

O consentimento, dentre as referidas gerações, possui um destaque bastante aparente. Excluindo-se a primeira delas, em que a regulação era realizada por meio de autorizações destinadas à própria tecnologia – a exemplo a lei estadunidense denominada *Privacy Act*, de 1978, que regulava a coleta e a operabilidade dos bancos de dados nacionais –, o consentimento sempre foi, senão seu elemento central, um dos mais relevantes (Bioni, 2019).

Já na segunda geração de leis – que, diferentemente da primeira, regulava não só a coleta de dados pelo Estado, mas também pelo setor privado – verifica-se uma tentativa de transferência da responsabilidade de proteção de dados ao próprio titular, utilizando-se, para isso, do seu consentimento (Bioni, 2019).

A explicação desse fato dá-se, segundo Bioni (2019), pela percepção de que a visão Orwelliana do "Grande Irmão", enquanto um vigilante único e supremo, já se encontrava superada. Na realidade da época, tal qual na corrente, o que há são "pequenos irmãos", diluídos de tal forma

5 As Novas Tecnologias da Informação e Comunicação podem ser entendidas como o conjunto total de tecnologias que permite o tratamento das informações – seja em forma de produção, de acesso ou de sua propagação – bem como as tecnologias que permitem a comunicação entre as pessoas (Rodrigues *et al*., 2014).

pelos governos e pelo setor privado que a normativa anterior, focada na regulamentação rígida acerca da utilização de cada banco de dados, não é mais viável.

No plano teórico, a solução de conceder ao indivíduo a autonomia de gerir as informações ao seu respeito condiz com a compreensão de Allan Westin (1970) acerca da privacidade, que seria uma "reivindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros".

Um importante julgado acerca do tema tratou da Lei do Censo alemã (*Volkszählunsgesetz*), de 1983. Em seu dispositivo original, previa-se que os indivíduos deviam conceder seus dados para fins estatísticos de distribuição espacial e geográfica da população. Entretanto, ao mesmo tempo, a lei também permitia que tais dados fossem cruzados com outros que já se encontravam em domínio estatal, para fins genericamente determinados de "atividades administrativas" (Bioni, 2019).

Essa obscuridade no destino das informações coletadas gerou grande comoção perante o Tribunal Constitucional Alemão, que, ao declarar a inconstitucionalidade parcial da referida norma– ficou decidido que os dados armazenados pelo censo se deveriam ater unicamente a fins estatísticos –, construiu uma tese fundamental à matéria: o indivíduo necessita ter controle sobre seus dados, a fim de ser capaz de *autodeterminar suas informações pessoais*. Nasce, dessa maneira, o conceito do direito à autodeterminação informativa.

Vale reiterar que, apesar de possuir forte correlação com a privacidade, o direito à proteção de dados, bem como à autodeterminação informativa, são direitos distintos entre si. Enquanto a privacidade pode assumir uma multiplicidade de significados, como já evidenciado, a autodeterminação informativa é o direito autônomo de autogerência de dados pessoais, a fim de garantir a pleno desenvolvimento personalíssimo.

Sob tais ideias, segundo Malheiro (2017), é possível afirmar que o consentimento é o mecanismo pelo qual se confere efetividade ao direito da autodeterminação informativa, pois, ao ofertar ao indivíduo a possibilidade de participação no tratamento de seus dados, o desenvolvimento de sua personalidade é, neste aspecto, salvaguardado. O direito à autodeterminação informativa, desse modo, funcionaria como uma "mola propulsora" da estrutura de proteção de dados.

Importante salientar, todavia, que esse direito não possui o consentimento como vetor único de efetivação. O julgado alemão supra mencionado, ao vetar a utilização dos dados para fins além do recenseamento, também foi um marco na argumentação de que é necessário limitar a atividade de processamento de dados em vista da preservação e do combate a violações do direito à personalidade.

Entende-se, desta feita, que o consentimento não esgota a responsabilidade estatal em orientar e limitar o manejo de dados. Levando-se em conta a grande assimetria de poder entre o Estado e o cidadão – o que caracteriza esse último como frágil e passível de manipulação – caso o consentimento fosse o único critério de proteção de dados, o sujeito tornar-se-ia um "objeto a ser ilimitadamente explorado" (Bioni, 2019).

Ao contrário disso, o direito à autodeterminação informativa foge da dicotomia entre o público e privado – tal como ocorria com o entendimento da privacidade como o *right to be alone* – para transfigurar-se em uma fusão de ambas as forças. De um lado, i) a pessoa possui efetiva

participação na tutela de seus dados, permitindo ou não a sua concessão ou uso; de outro, ii) os indivíduos responsáveis pelo controle dos dados devem, mesmo sob a égide do consentimento, orientar seu tratamento e destinação de forma a não ofender a personalidade humana.

A referida decisão da Corte Constitucional alemã foi emblemática para a terceira geração de leis, que expande ainda mais o protagonismo do portador dos dados. Se a segunda possibilita ao titular a participação em algumas etapas da movimentação de dados, a terceira abrange todas elas, desde a coleta ao compartilhamento. Seu intuito nada mais é do que alcançar o "êxtase da própria terminologia da 'autodeterminação informacional', pois, com tal participação, possibilitar-se-ia que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais" (Bioni, 2019).

Note-se que essa geração de leis foi simplista em seu entendimento do que seria a autodeterminação informativa, sendo incapaz de compreendê-la para além do consentimento do titular. Para suprir suas lacunas, bem como também em virtude de tais dispositivos só conseguirem abarcar um pequeno número de pessoas, a terceira foi superada e substituída pela quarta geração de leis.

Nessa quarta e última geração, vivenciada até a atualidade, alivia-se o peso atribuído ao titular dos dados na sua gestão por meio do enriquecimento de mecanismos e de proposições normativas que salvaguardem o usuário e suas informações da manipulação de terceiros. Conforme as palavras de Doneda:

> Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção (Doneda, 2011, p. 98).

No entanto, mesmo que o consentimento perca a autonomia outrora prevalente, ele não perde sua centralidade nas leis de proteções de dados. Na realidade, segundo Bioni (2019), o que há é uma maior regulamentação em seu entorno, evidente, por exemplo, pelo processo de adjetivação sofrido pelo consentimento. Ele deverá ser, portanto, para ter validade, livre, informado, inequívoco, explícito e/ou específico – dependendo, este último, do ordenamento a aplicá-lo.

Urge, assim, que se investigue o tratamento que a LGPD oferta ao consentimento, de modo a compreender como tal mecanismo opera na realidade nacional vigente.

4. A BASE PRINCIPIOLÓGICA DO CONSENTIMENTO NAS NORMAS NACIONAIS SOBRE PROTEÇÃO DE DADOS

4.1 A ANTESSALA DA LGPD: AS LEIS SETORIAIS DE PROTEÇÃO DE DADOS

Antes da LGPD, o Brasil dispunha de pouquíssimos dispositivos legais que se debruçassem sobre a proteção de dados. Tem-se como exemplo o Código do Consumidor, o qual disciplinou os bancos de dados e os cadastros dos consumidores, e a Lei do Cadastro Positivo,

que também versou sobre os bancos de dados, mas àqueles relativos a transações financeiras e de adimplemento para fins de concessão de crédito. O consentimento foi, em ambas as legislações, o instrumento utilizado para garantir a proteção de dados.

O mesmo ocorre no Marco Civil da Internet (Lei 12.965/2014), o qual, dentre a série de normativas por ele instauradas para regular o uso da internet, previa a proteção da privacidade e dos dados pessoais do usuário. Grande parte da preocupação com a proteção desses direitos virtuais deu-SE na era pós-Snowden[6], de forma que coube ao referido dispositivo conceber a eles maior amparo na esfera digital.

Entretanto, mesmo com o avanço apresentado pelo Marco Civil da Internet na proteção de dados, quando comparado às demais leis setoriais brasileiras, também se encarrega ao usuário o dever de executar essa tarefa. Em diferentes momentos, a lei retratada menciona o consentimento – na qualidade de "livre, expresso e informado" (Brasil, 2014) – como requisito necessário para operacionalização dos dados, desde a coleta até o seu compartilhamento, bem como prevê a possibilidade de o usuário revogar seu consentimento.

Para Bioni (2019), o princípio utilizado pela lei indicada foi o da autodeterminação informativa, em seu significado estrito de autonomia particular do titular dos dados. A LGPD buscou, como será demonstrado, superar tal visão simplista, indicando maneiras afins do consentimento para embasar a proteção de dados, apesar de sua relevância ainda ser evidente.

É acerca dessa importância ainda atribuída ao consentimento que se voltará o presente estudo, buscando aferir sua eficácia, identificar as lacunas deixadas e as possíveis formas de superá-las.

4.2 O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados foi promulgada em 2018 após quase uma década de discussões acerca de suas pautas, iniciadas em 2010. Bem como as demais legislações de proteção de dados já citada, ela dá grande valor ao consentimento, embora não o utilize, e não devesse mesmo utilizar, como seu único vetor de efetivação, tal qual se visualizava nas primeiras gerações de leis. Ao invés disso, o dispositivo prevê ao controlador[7] o dever de "enquadrar cada atividade de tratamento em uma base legal específica[8], conforme a finalidade desse tratamento" (Leonardi, 2019, p. 71).

Note-se, no entanto, que não há nenhuma disposição preferencial acerca da base legal a ser utilizada, desde que esteja adequada ao fim a que se destina o tratamento. É possível

6 É o movimento internacional de preocupação com a privacidade e com a proteção de dados pessoais, especialmente no meio virtual, em resposta ao esquema de espionagem realizado pelo governo norte-americano e delatado por Edward Snowden, ex-técnico da CIA. Como reação a tais denúncias, os países passaram a buscar medidas que protegessem seus cidadãos e sua própria soberania, a exemplo, no Brasil, da Lei do Marco Civil da Internet (Donahoe; Canineu, 2014).

7 Segundo a LGPD, é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Brasil, 2018). Em outras palavras, o controlador é quem definirá as finalidades do tratamento e os métodos pelo qual ele será operacionalizado. É o caso, por exemplo, de grandes empresas on-line como o Facebook, tal como pode ser visto a partir de sua política de privacidade.

8 As hipóteses em que o tratamento de dados poderá ser efetuado estão listadas nos incisos do art. 7º da LGPD, ofertando um total de dez bases legais possíveis sob as quais o tratamento será válido. São elas: consentimento do titular; legítimo interesse; cumprimento de obrigação legal ou regulatória; tratamento pela administração pública; realização de estudos e de pesquisa; execução ou preparação contratual; exercício regular de direitos; proteção da vida e da incolumidade física; tutela de saúde do titular; proteção de crédito.

afirmar, com isso, que há paridade entre o consentimento e as demais bases legais elencadas na LGPD, superando-se uma estrutura protetiva unicamente focada na anuência do titular.

Tal evolução deu-se após uma série de consultas públicas realizadas anteriormente ao envio do projeto ao Congresso Nacional, já que, nas primeiras versões do anteprojeto, o consentimento não era só central para o tratamento de dados pessoais, mas também a única base legal que o autorizava. Não obstante, a redação que foi de fato remetida ao Congresso, e posteriormente aprovada e sancionada, dizia respeito à configuração atual da LGPD, com dez bases legais hierarquicamente equivalentes (Leonardi, 2019).

Todavia, apesar da citada equidade entre as bases legais, é impossível negar o destaque central que o consentimento ainda possui no texto da lei, seja qualitativa ou quantitativamente. A comprovação dessa última modalidade resta comprovada em virtude de o vocábulo "consentimento" ser utilizado trinta e sete vezes durante a redação da lei 13.709/18, o que já demonstra sua forte influência.

Além disso, mesmo quando não há a sua presença expressa, o consentimento parece nortear diversos aspectos do dispositivo, tal qual se tentará demonstrar por meio de uma explicação acerca do tratamento dado pela lei a esse vetor.

Conceitualmente, em seu art. 5º, a LGPD prevê que se deve compreender tal base legal como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Brasil, 2018). Tal redação demonstra-se em consonância com demais legislações internacionais que também se utilizam do consentimento para autorizar o tratamento de dados, em especial a GDPR[9].

Assim, para Leonardi (2019), de forma individualizada, é possível afirmar que a validade do consentimento importa que ele seja: (a) livre, isto é, deve de fato refletir o desejo do titular, não sendo admitidos vícios de qualquer natureza; (b) informado, o que significa que a anuência do titular só poderá ocorrer após a sua cientificação acerca das finalidades do tratamento; (c) inequívoco, ou seja, para ser legítimo, o consentimento não pode ser passivo, necessitando de uma ação manifestadamente positiva do seu titular; (d) direcionado a uma finalidade determinada, de forma que só será válido enquanto atender ao fim previamente estabelecido e informado ao indivíduo.

Vale salientar que, em alguns casos previstos na lei, o consentimento deve ser, para além dos adjetivos supracitados, específico: o titular dos dados deve consentir individualmente com cada uma das finalidades destacadas pelo controlador. Essa quinta qualificação do consentimento é necessária, por exemplo, nos casos de tratamento de dados sensíveis ou cujos titulares sejam crianças e adolescentes.

Também estão previstas, na redação da lei 13.709/18, os casos em que o consentimento será considerado nulo, vide o artigo 8º, §3º e §4º, e artigo 9º, §1º, da LGPD. Tais dispositivos referem-se, respectivamente: à vedação dos tratamentos de dados realizados com consentimento viciado[10]; à nulidade de autorizações, por meio do consentimento, que não se destinarem a finalidades determinadas; à nulidade do consentimento quando as informações repassadas

9 Sigla para Geral Data Protection Regulation – livremente traduzido para Regulamento Geral de Proteção de Dados – legislação que trata da proteção de dados no território europeu.

10 As hipóteses de vício do consentimento se encontram listadas no Código Civil de 2002. São elas: o erro, o dolo, a coação, o estado de perigo e a lesão (Brasil, 2002).

ao titular contenham "conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca" (Brasil, 2018).

Outra observação relevante, que se manteve desde a legislação referente à proteção de dados presente na Lei do Marco Civil, é que o titular detém o poder de revogar seu consentimento a qualquer momento, para fins de controle do fluxo de suas informações, conforme pode ser constatado da leitura do art. 8º, § 5º da referida lei.

Essa caracterização extensiva do consentimento ao longo da lei, segundo Bioni (2019), é um dos primeiros sinais de que sua importância pilar não foi abandonada, mesmo que ao seu lado estejam outras bases legais de hierarquia verticalizada.

Soma-se a isso a verificação de que muitos dos princípios que regem a LGPD parecem construir seus limites em volta da figura do titular dos dados. Como postulado pelo autor:

> [...] grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio do quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles para, eventualmente, corrigi-los; b) de outro lado, princípios mais "modernos", como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade especificada para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos (minimização dos dados) (Bioni, 2019).

Dessa forma, para além da compreensão do consentimento como base legal, parece haver uma carga principiológica ao longo de toda a redação do dispositivo, o qual busca incutir no indivíduo o poder de controle sobre o fluxo de seus dados, utilizando-se, para tanto, da autonomia da vontade. Tal abordagem não só é extraída do direito à autodeterminação informativa – novamente reduzida à mera manifestação do querer do indivíduo – como também demonstra sua consagração como um dos pontos cardeais da LGPD.

Não há dúvidas, com isso, de que o consentimento ainda ocupa privilegiada posição na efetivação do direito à proteção de dados no Brasil, evidente por seu papel de destaque na LGPD, demonstrada, senão explícita, de forma substancial.

Cabe pontuar, mediante todas as informações já indicadas, que a simples possibilidade de autogerência do fluxo informacional sobre os próprios dados, concedida ao indivíduo pelo legislador, não é suficiente, por si só, para que seus direitos se efetivem. Isso se deve ao fato de não ser possível encarregar à vontade do sujeito a plena tutela de seus direitos, sejam eles a privacidade, a personalidade ou a proteção de seus dados.

É nesse sentido que a utilização do consentimento como pilar de proteção de direitos fundamentais é problemática, haja vista que nem sempre ela será efetiva ou refletirá de fato a escolha do titular, tanto em virtude dos artifícios mercadológicos para manipular o usuário quanto da escassez de conhecimento que é ofertada a ele para que seja plenamente capaz de realizar a tutela que a lei lhe incumbe.

O próximo tópico buscará destrinchar tais dificuldades, com o intuito de demonstrar a insuficiência da base legal do consentimento para a devida tutela de direitos.

5. DESAFIOS CONTEMPORÂNEOS À UTILIZAÇÃO DO CONSENTIMENTO COMO VETOR PROTETIVO DA LGPD

A larga utilização do consentimento como um dos mecanismos propulsores do direito à proteção dos dados do indivíduo na LGPD suscita uma óbvia questão a ser debatida: o titular dos dados está preparado para autodeterminar suas informações?

Há muitos desdobramentos a partir dessa indagação. Poderiam ser realizados desde debates mais amplos acerca da atual relação humana com a privacidade até discussões mais específicas acerca entendimentos extraídos da lei 13.709/18.

Nesse ínterim, para os fins pretendidos no presente trabalho, o qual não busca – e nem conseguiria – esgotar o tema, far-se-á a análise de dois principais eixos problemáticos à plena utilização do consentimento na LGPD: os seus entraves subjetivos e objetivos.

5.1 DIFICULDADES SUBJETIVAS

5.1.1 A COMPLEXIDADE DO FLUXO INFORMATIVO: UMA ANÁLISE A PARTIR DAS POLÍTICAS DE PRIVACIDADE NO AMBIENTE VIRTUAL

A qualificação do consentimento como uma manifestação livre, informada, inequívoca e determinada exige de seu titular uma quantidade considerável de conhecimento sobre tais assuntos, a fim de não se recair nas hipóteses de nulidade do consentimento, anteriormente mencionadas.

Isso porque, para atender às especificações incutidas a essa base legal, pressupõe-se que o titular anuente com determinada política de tratamento tem ciência de todo o processo que será interposto aos seus dados – como o seu controlador, as formas de tratamento, as finalidades, os outros controladores que porventura também terão acesso a esses dados, entre outros – sob pena de tal aceite não representar um processo legítimo de tomada de decisão.

Como se pode imaginar, isso raramente será compatível com a realidade. A ascensão das Novas Tecnologias acarretou uma dispersão informacional a níveis extremos, o que, dentro do escopo do tema aqui versado, significa que os dados são micropartículas de um complexo agrupamento informacional, cunhado de *Big Data*[11]. Esse sistema é tão vasto que, com a inserção massiva de dados, as informações nele presentes se tornam fluidas e interconectadas, de maneira a dificultar a compreensão completa, ou até mesmo parcial, desse processamento.

Um exemplo dessa fluidez pode ser identificado pela política de *cookies*[12] utilizada no *Facebook*, site responsável por ocupar o 3º lugar no ranking dos mais acessados no Brasil[13]. Segundo a referenciada política, uma das finalidades da utilização de *cookies* é informar outras empresas das preferências dos usuários do *Facebook* por meio de sua atividade na plataforma, com o intuito de direcionar a eles o conteúdo – isto é, a propaganda – mais adequada ao seu perfil (Facebook, 2022).

11 Tecnologia que permite o avolumamento e processamento de grandes quantidades de dados.

12 Pequeno arquivo de texto capaz de registrar a identidade do usuário para o navegador utilizado, de forma a armazenar dados de navegação como preferências, localização e frequência de cliques.

13 Pesquisa feita pela *SimilarWeb* em maio de 2021, a qual constatou os dez sites mais acessados no Brasil.

REVISTA MERITUM • v.18 • n.1 • p. 55-76 • Jan. - Abr. 2023

Tal operação, veiculada pelo *Facebook* e por inúmeras outras empresas *on-line* como uma maneira de "aprimorar a experiência do cliente" – a qual esconde o objetivo finalístico de monetizar suas informações – culmina no envolvimento de diversos outros agentes de controle além da plataforma original a quem o usuário concedeu seus dados. Isso significa, em outras palavras, que o consentimento adjetivado, da forma como prevê a redação da LGPD, exige que o usuário do *Facebook* conheça a totalidade das empresas que terão acesso aos seus dados por intermédio dos cookies, já que eles também serão controladores.

Dada a vasta quantidade de empresas parceiras de grandes corporações como o Facebook, bem como a sua própria política de cookies – a qual, excetuando-se breves explicações acerca dos cookies e tecnologias mais utilizados pelas empresas parceiras, não dispõe de nenhuma outra informação acerca desses controladores – é muito improvável que isso aconteça. Prevalece, em verdade, um generalizado desconhecimento sobre os indivíduos que terão acesso a tais dados, sendo possível afirmar que a qualificação do consentimento como "informado" não se caracteriza.

Outro importante fator para que se ateste a complexidade do fluxo informacional, ainda dentro do escopo das políticas de privacidade, é o custo temporal demandado pela leitura de tais documentos. Em 2008, um estudo realizado por pesquisadores da *Carnegie Mellon University*, nos Estados Unidos, buscou aferir o tempo anual que seria necessário para que o usuário lesse as políticas de privacidade dos serviços que usa.

O resultado demonstrou a inviabilidade dessa operação: de acordo com a pesquisa, a qual considerou que uma pessoa lê, em média, 250 palavras por minuto, e que o comprimento dessas políticas costuma ser de 144 a 7.669 palavras, constatou-se que o processo de leitura requereria do usuário 250 horas por ano do seu tempo, o que representa cerca de 30 dias de trabalho. Além disso, apesar do número expressivo, a referida pesquisa sequer levou em consideração a leitura de outros documentos que se baseiam na concordância do usuário – a exemplo dos termos de uso (Mcdonald, 2008) – os quais demandariam ainda mais tempo para que tais dispositivos sejam devidamente conhecidos.

Ao falar-se em fluxo informacional complexo, também é necessário conceber a forma dificultosa que tais políticas, mesmo quando de clara redação, são interpostas ao usuário para posterior anuência, pois é irrazoável, ou ingênuo, esperar que uma pessoa despenda tanto tempo da sua vida com uma leitura rigorosa desses dispositivos.

Dessa arte, estando ausente a anuência racional do titular, resta evidente que o consentimento não atingiu seus objetivos, falhando como base legal capaz de salvaguardar os direitos do titular.

5.1.2 MITO DA AUTODETERMINAÇÃO RACIONAL EM NÚMEROS: O DESPREPARO HUMANO PARA GERIR OS PRÓPRIOS DADOS

Vale salientar que as observações feitas acerca da complexidade do fluxo informacional se valem de uma visão notadamente otimista dos fatos. Para que o titular descubra que não possui total acesso à identidade dos controladores de seus dados, bem como às suas finalidades específicas, parte-se do pressuposto de que ele estará plenamente disposto e preparado a buscar tais informações acerca dos sites, das plataformas e dos serviços dos quais faz uso

cotidianamente, visando averiguar se determinada política se encontra de acordo com sua vontade de compartilhar dados.

Essa visão também soa fantasiosa.

No que pese, como anteriormente tratado, o entendimento da privacidade como o *right to be alone* já ter sido – ao menos teoricamente – superado, ainda é possível, na atualidade, identificar alguns efeitos decorrentes dessa percepção.

As acepções fundadoras da noção de privacidade – em especial a Democracia Liberal e o Contratualismo Social – culminaram na visão do homem como um ser atomístico, dissociado da sociedade, cuja autorreflexão sem intervenções externas seria suficiente para revesti-lo de autonomia (Debrabander, 2020).

Com efeito, não se discute aqui a importância da privacidade para a autorreflexão – vide o próprio entendimento deste como um direito da personalidade – mas sim se os indivíduos são plenamente capazes de utiliza-la como método de desenvolver sua autonomia, tal como poderia ser preconizado a partir de uma rasa compreensão sobre esses conceitos.

Segundo Debrabander (2020), o entendimento de que o desenvolvimento da autonomia humana se daria no momento em que seu direito à vida privada fosse resguardado é falho. Apesar do espaço particular ter sua importância à formação do indivíduo, não se pode imaginar que o mero ato de deixa-lo só iria, de forma independente, revesti-lo de autonomia, dada a própria concepção da palavra[14].

Dessa forma, ao lado do resguardo da privacidade – inicialmente necessária para o desenvolvimento embrionário de ideias, como postulou Arendt – a autonomia também necessita que o Estado propicie à população uma educação que possibilite a sua difusão. Além do pensamento crítico, a autonomia implica que o ser pensante tenha os conhecimentos necessários para realizar tais reflexões, as quais não poderão, pelo menos não em sua totalidade, ser efetuadas em solidão.

O mesmo, de forma análoga, parece acontecer com o uso do consentimento na LGPD. No que pese a previsão legislativa de outras possíveis bases legais de hierarquia equiparada, a vigência contemporânea do consentimento, bem como seu notório caráter central na lei 13.709/18, evidenciam que se transfere ao titular a responsabilidade principal de gestão dos próprios dados sem ofertar a ele, em contrapartida, suporte técnico para tanto.

Essa negligência educacional pode ser aferida pelo desconhecimento popular acerca da LGPD. Uma pesquisa realizada pelo Núcleo de Inteligência e Pesquisas do Procon-SP entrevistou 7.408 pessoas com o intuito de desvendar a percepção do consumidor sobre a proteção de seus dados, sobre a própria lei 13.709 e temas afins. Os resultados refletem os argumentos supramencionados: a esmagadora maioria da população não detém educação o suficiente sobre tais assuntos.

A primeira pauta da entrevista questiona aos participantes se eles sabem o que é dado pessoal. Apesar 89,52% dos entrevistados afirmarem que sim, quando questionados acerca

14 Segundo Debrabander (2020), a autonomia, enquanto manifestação da individualidade racional de seu portador, só poderá ser identificada no domínio público, quando levada a confronto com outras de iguais qualidades. Ter autonomia importa que, mesmo mediante divergentes ideologias, se permaneça arguindo suas próprias, caso mais robustas, ou as substitua por outras, caso não se demonstrem tão eficazes quanto se imaginava de início. Não é possível, portanto, desenvolver autonomia plena em solidão.

de qual conceito mediante três apresentados definiria corretamente o dado pessoal, apenas 45,33% deles responderam segundo os parâmetros fixados na LGPD. Tal situação se agrava ao somar-se os indivíduos que erraram o conceito certo com aqueles que afirmaram não saber o que é dado pessoal, pois, contabilizados em relação à totalidade dos entrevistados, representariam 59,42% dos participantes (Escola de Proteção e Defesa do Consumidor, 2021).

Essa constatação, por si só, já demonstraria a desinformação generalizada sobre a pauta. Sendo o dado pessoal um conceito não só primordial, mas também um dos mais básicos trazidos pela LGPD, como é possível afirmar que, ao anuir com determinada política de tratamento, tal ação representará de fato um processo de tomada de decisão racional do titular dos dados?

Não obstante, a referida pesquisa intentou resultados ainda mais evidentes. Questionou-se, após isso, se os entrevistados tinham conhecimento da Lei Geral de Proteção de Dados. Nessa seara, os resultados foram ainda mais preocupantes, com 65,04% dos participantes afirmando desconhecimento do dispositivo. Novamente, aqueles que afirmaram saber do que se tratava – 34,96% dos entrevistados – foram apresentados a três afirmativas sobre a LGPD, com somente uma delas sendo verdadeira. Nessa apuração, apontou-se que apenas 19,73% das respostas não possuía nenhuma incorreção (Escola de Proteção e Defesa do Consumidor, 2021).

Esses resultados demonstram o obscurantismo social acerca da pauta. O fato de que, em meio as 7.408 pessoas entrevistadas, somente 511 saberem de fato do que se trata a LGPD representa uma grave falha de efetividade do próprio dispositivo, haja vista que esse se utiliza fundamentalmente do consentimento como base legal garantidora da proteção de dados.

Há, a partir da relação desse obscurantismo social com a argumentação desenvolvida por Debrabander (2020), o que se pode chamar de mito da autodeterminação racional. Espera-se, nessa mentalidade, que o indivíduo desenvolva por si só – quase que "magicamente", nas palavras do autor – o conhecimento técnico necessário para ser capaz de autodeterminar seus dados, pois não se oferta a ele os mecanismos para tanto, tal como foi bem evidenciado na referenciada pesquisa.

Assim como a autonomia não será alcançada pela mera reserva do direito à privacidade, não se pode esperar que a mera previsão de que o consentimento seja legítimo, sem atribuir-lhe os meios de execução devidos, irá refletir a vontade racional do titular. Dessa forma, a qualificação do consentimento enquanto manifestação livre, informada, inequívoca e determinada se demonstra sumariamente falha, pois não é possível falar em anuência legítima do cidadão sem instrui-lo do que seria a LGPD, a proteção de dados ou qualquer outra pauta fundamental ao resguarde da formação da sua personalidade em âmbito nacional.

5.1.3 O PAPEL DA PRIVACIDADE NA ERA DO COMPARTILHAMENTO

Para além das dificuldades enfrentadas por quem possui interesse em resguardar seus dados pessoais e não o consegue, ou por aqueles que não recebem as ferramentas necessárias para tanto – vide os dois subtópicos anteriores – tem-se um problema de viés subjetivo muito mais amplo e complexo à utilização do consentimento como vetor protetivo da LGPD: a contemporânea desvalorização cultural da privacidade.

Debrabander (2020) afirmou, acertadamente, que "os cidadãos democráticos do século XXI têm uma paradoxal, crescente e contraditória relação com a privacidade" (tradução nossa).

Isso se dá porque, em que pese as pessoas afirmarem se preocupar com a sua privacidade e com o destino que seus dados pessoais terão quando recaídos nas mãos de instituições poderosas e mal-intencionadas, não se pode negar que se vive, atualmente, na era em que a exposição da vida pessoal é mais aceita e normalizada socialmente.

Impulsionados pela economia digital, na qual a não-inserção do indivíduo implica quase na sua não-existência perante a sociedade, as pessoas encontram-se levadas a utilizar suas redes sociais como um álbum de memórias ou um diário pessoal – não à toa a fama de plataformas como *Instagram* e *Twitter*, baseadas, respectivamente, na oferta dessas funcionalidades –, com a divergência de que esses, em lugar de estar alocados no espaço pessoal de seu dono, encontram-se acessíveis por todos, a qualquer momento e lugar.

Esse processo é denominado de cultura confessional (Debrabander, 2020). Nele, o intermediário da coleta de dados pessoais torna-se o próprio titular, que divulga suas informações, a despeito do quão pessoais, íntimas ou embaraçosas elas possam ser, no meio digital. É o próprio titular dos dados que fotografa sua rotina, inclui sua localização e publica-a nas redes sociais à vista de todos. É o próprio titular que expõe detalhes possivelmente comprometedores de sua vida pessoal, mesmo sabendo que seus chefes ou futuros empregadores estarão acompanhando-o atentamente on-line. É o próprio titular que faz desabafos acerca de sua vida íntima no *Twitter*, sem se importar com o alcance dessas revelações e quais impactos ela poderá acarretar a sua vida – muito pelo contrário disso, faz-se publicações esdrúxulas exatamente com o objetivo de ser notado publicamente!

Não importa, nesse dado sistema – ao menos não o suficiente para impedir o sujeito – o destino que essa superexposição acarretará, mesmo a par dos perigos enfrentados pela privacidade frente à ascensão do mundo on-line e da Economia Digital[15].

Não compete, importa ressaltar, ao presente trabalho, debruçar-se excessivamente sobre o tema da pós-privacidade, haja vista ser tão vasto e delicado que poderia ensejar a produção de estudos completamente autônomos. Entretanto, relevante ao escopo do presente estudo é pontuar como o atual cenário sociocultural pode impactar o processo racional de tomada de decisão que é exigido pela LGPD com a previsão da base legal do consentimento.

Tratando-se de uma sociedade que, apesar de afirmar preocupar-se com a privacidade de seus dados, revela espontaneamente suas informações no ambiente virtual, a utilização do consentimento torna-se uma ferramenta duvidosa à efetiva proteção dos dados do titular. Como se poderia incumbir ao indivíduo o poder de autodeterminar suas informações se ele não se preocupa, na prática, com tal exercício?

Tem-se, na atualidade, como bem afirmado por Holland (2011), o diagnóstico do chamado *paradoxo da privacidade*: mesmo que haja uma preocupação do cidadão com a proteção de suas informações que, tal receio não excederá o cunho teórico, haja vista a coleta de dados pessoais também ser, em última instância, um fenômeno não só consentido, mas efetuado por nós. Nessa exata medida, em que o titular afirma que se preocupa com suas informações sem, em contrapartida, agir segundo tal filosofia, é que é possível sugerir a questionabilidade do consentimento como método viável de proteção de dados.

15 Embora cada vez mais entrelaçada com a economia tradicional, o que dificulta seu delineamento objetivo – a exemplo das lojas que são, ao mesmo tempo, físicas e virtuais – a Economia Digital pode ser entendida pela incorporação mercadológica da internet, das tecnologias digitais e de suas ferramentas nas mais variadas etapas necessárias à comercialização.

Dessa maneira, no que consta à LGPD, mais uma vez, torna-se necessário avaliar até que ponto a anuência do titular refletiria a sua autonomia da vontade à luz da nova configuração cultural de compartilhamento voluntário da vida pessoal – padrão originado e incentivado pelo capitalismo informacional.

5.2 DIFICULDADES OBJETIVAS

5.2.1 A LACUNA LEGAL DA EFETIVIDADE DO CONSENTIMENTO E SEU CUSTO SOCIAL

Em virtude da argumentação previamente realizada neste trabalho, não resta dúvidas de que, apesar da forte preocupação da LGPD em qualificar o consentimento para conceder-lhe validade – bem como realizado por outras leis de proteção de dados internacionais que seguem o mesmo raciocínio, a exemplo da GDPR – há um grande vazio legislativo a respeito de como se daria essa operacionalização.

Em outras palavras, mesmo que fortemente presente na redação da lei 13.709/18 – seja por sua adjetivação, por sua reiterada incidência ou pela centralidade substancial que ocupa – não se conferiu ao consentimento a efetividade necessária para concretizá-lo de fato. Há, em verdade, a exemplo dos desafios subjetivos enfrentados pela população, uma extensa gama de lacunas à utilização adequada de tal base legal, o que pode ensejar sua aplicação inadequada.

Nessas ideias, outro produto nocivo da falta de efetividade do referido dispositivo, capaz de elucidar as afirmações aqui veiculadas, é a concepção das políticas de privacidade.

Em meio a esse panorama de incompletudes das leis de proteção de dados ao longo da história, o mercado necessitou se autorregular para conceber mecanismos que ventilassem a proteção dos dados do titular. Foram sob esses parâmetros que se originaram, como umas das principais ferramentas de legitimação da vontade do titular, as políticas de privacidade. Tais recursos, em seu intento fundador, aspiram captar a anuência do titular necessária à plena adequação dos sites às legislações de proteção de dados pessoais (Bioni, 2019).

É mediante esses ideais que se torna possível tratar de um desafio objetivo à plena utilização do consentimento como vetor protetivo. No que pese a porventura bem-intencionada tentativa mercadológica de se tentar adequar a tal panorama, verifica-se que as políticas de privacidade são, em verdade, genuínos contratos de adesão (Bioni, 2019) pautados no aceite do seu titular.

Isso porque, como cabe a ele meramente anuir ou rejeitar determinada política de privacidade – os famosos "li e concordo" ou "não concordo", que irão permitir ou negar o acesso do usuário – sem que haja, em contrapartida, qualquer possibilidade de barganhar os termos ali dispostos, verifica-se a vigência de uma política de "tudo" ou "nada". Nesse sistema, não existe meio-termo. Ou o usuário/consumidor concede seu aceite integral às plataformas, recebendo em troca o mero acesso a elas, ou as rejeitará completamente – não importando se ele discorda apenas parcialmente de seus termos – sendo, então, deliberadamente excluído desse acesso (Bioni, 2019).

No que tange à LGPD, apesar das mudanças por ela implementadas às políticas de privacidade, ainda há uma carência de superação desses problemas. As alterações a que se referem a redação da lei 13.709/18 objetivaram, sinteticamente, clarear o tratamento de dados realizado pelas plataformas ao seu titular, bem como ofertar a ele alguns direitos – e a informação sobre a previsão legal deles – acerca dessa autogestão, a exemplo da possibilidade de saber quais dados seus o controlador detém.

Percebe-se, com isso, que o poder decisório do usuário ainda é limitado. Ao passo em que seu controle é delimitado pelo mero aceite ou recusa integral do tratamento a ser realizado, mesmo que informado, a escassez de opções das quais dispõe aduzem à ideia de que não se pode afirmar, de fato, que a atual configuração da base legal do consentimento representa a sua vontade explícita. Sem que o titular possa fazer uma contraproposta, um processo pleno de tomada de decisão não é de alcance possível.

O direito à autodeterminação informativa, nesses termos, soa extremamente falacioso. A previsão legal do direito à proteção de dados – cujo mecanismo principal na lei 13.709/18 é a anuência do usuário – demonstra-se falha num dos seus objetivos mais primordiais: garantir a legitimidade desse instrumento. À medida em que a autoridade do usuário sobre seus próprios dados se encontra limitada a ações que não interferem praticamente na forma como o tratamento é realizado, a base legal do consentimento demonstra-se, novamente, duvidosa.

Tais operações, nesses termos, põem em xeque a real eficácia da anuência do usuário como fruto legítimo de decisão racionalizada. Em decorrência da impossibilidade de negociar-se tais termos, há meramente uma exclusão digital – que, em tempos de economia digital, equivale a exclusão social em si – cujo filtro é o aceite ou a recusa do titular da concessão de seus dados. Esse indivíduo, impulsionado pela necessidade sociocultural de inserir-se na nova realidade digital, tenderá a ceder a tais políticas, mesmo que essas não reflitam a autonomia de sua vontade (Bioni, 2019).

Esse é o custo social gerado por tais políticas. É possível afirmar, a partir dessas ideias, que o consentimento não é uma possibilidade tangível à medida em que não se oferta ao usuário uma decisão razoável acerca da disposição de seus dados. Não se pode esperar, quando é a própria inserção social da pessoa que está em xeque, que ela priorizará a privacidade de dados que ela nem mesmo compreende ao certo quais suas funções e relevância. Tal visão seria, além de completamente desconectada com a realidade, uma maneira de legitimar o controle social daqueles que detém o poder.

6. CONSIDERAÇÕES FINAIS

O presente trabalho teve como escopo analisar a viabilidade da base legal do consentimento como mecanismo de proteção dos dados pessoais do titular. Para tanto, realizou-se estudos acerca do próprio portador dos dados – já que ele é a figura central dessa sistemática – bem como acerca dos métodos de aplicação da lei 13.709/18, a fim de aferir se haveria, ou não, real efetividade na tutela de direitos pretendida pela LGPD.

Os resultados obtidos no que consta à figura do titular, aqui chamados de desafios subjetivos, explicitam que ele não é munido de capacidade, conhecimento ou até mesmo de vontade o suficiente – vide a influência das forças de mercado atuais, em especial o Capitalismo Informativo – para conseguir manejar seus dados acertadamente.

Com a percepção de que é interposto a ele um complexo fluxo informacional, uma baixíssima ou nula instrução acerca de como gerir seus dados e uma noção de privacidade socialmente defasada, conclui-se que o titular não é apto a exercer o papel de gerência que a redação da LGPD lhe atribui. Desta feita, estando ele desqualificado para gerir seus dados, também se desqualifica o próprio direito à proteção de dados, já que, embora previsto em lei, ele não é dotado de efetividade.

A mesma falha pode ser identificada a partir da verificação de lacunas na aplicabilidade da lei, aqui cunhada de desafios objetivos à efetivação da base legal do consentimento. No citado exemplo das políticas de privacidade, que mais se comportam como contratos de adesão entre o titular e a empresa a quem se consente a coleta dos dados, percebe-se que não há a possibilidade de barganha entre as partes, cabendo meramente o aceite ou a recusa da parte mais fraca da relação – o portador dos dados.

Em verdade, essa dinâmica funciona como um método de exclusão social cujo filtro é a anuência do usuário/consumidor, já que sua não-adesão aos termos dispostos implicará meramente no seu afastamento da plataforma, caso o indivíduo permaneça com a recusa, e sua adesão incorrerá no aceite integral dos termos dispostos pelos controladores.

Percebe-se, em ambos os casos, uma grave falta de legitimidade nas condutas adotadas pelos titulares dos dados, seja por falta de meios que os tornem de fato indivíduos capazes de autodeterminar suas informações, ou pela presença de lacunas legislativas na LGPD que dificultam sua efetividade. Como o processo de tomada de decisão não se baseia na vontade genuína do portador, o consentimento demonstra-se uma base legal ineficiente, ao menos nos termos atuais, para salvaguardar os direitos de seu titular mediante as poderosas instituições que almejam obter lucro e poder mediante suas informações.

Tais fragilidades, destarte, deixam evidente que o status de hipervulnerabilidade do titular não é plenamente solvido com o sancionamento da LGPD, haja vista que a base legal do consentimento, central no dispositivo, desconsidera a sua delicada posição em meio as forças que incidem sobre ele.

Uma proteção de dados eficiente e resolutiva, capaz de tutelar plenamente os direitos pretendidos, precisa considerar essas vulnerabilidades e dispor ao titular todos os aparatos necessários para lidar com elas. Sem tais esforços, a previsão legal do consentimento permanecerá inefetiva em seu escopo normativo.

REFERÊNCIAS

ARENDT, Hannah. **As origens do totalitarismo**: antissemitismo, imperialismo, totalitarismo. Cia das Letras, São Paulo, 1991.

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

BRANDEIS, Louis; WARREN, Samuel. **The right to privacy**. Harvard law review, v. 4, n. 5, p. 193-220, 1890.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 3 out. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 3 de out. 2021.

BRASIL. **Lei nº 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico crédito. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 3 de out. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 out. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 3 out. 2021.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Revealed**: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 7 out. 2021.

DEBRABANDER, Firmin. **Life after Privacy**: Reclaiming Democracy in a Surveillance Society. Maryland Institute College of Art. Sept. 2020.

DONAHOE, Eileen; CANINEU, Maria Laura. A internet pós-Snowden: EUA trilharam o caminho da vigilância em massa. **O Globo**, Rio de Janeiro, 6 jun. 2014. Disponível em: https://oglobo.globo.com/opiniao/a-internet-pos-snowden-12736908. Acesso em: 7 out. 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, [*S. l.*], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 3 out. 2021.

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

ESCOLA DE PROTEÇÃO E DEFESA DO CONSUMIDOR. **Pesquisa comportamental**: percepção do consumidor quanto à proteção dos seus dados e a LGPD. São Paulo: Procon-SP, 2021. Disponível em: https://www.procon.sp.gov.br/wp-content/uploads/2021/07/Relatorio_LGPD.pdf. Acesso em: 7 out. 2021.

HIRSCH, Dennis D. The glass house effect: Big Data, the new oil, and the power of analogy. **Me. L. Rev**., v. 66, p. 373, 2013.

HOLLAND, H. Brian. **Privacy Paradox 2.0.** 4 Apr., 2010. Disponível em: http://ssrn.com/abstract=1584443. Acesso em: 8 out. 2021.

KARINA, Souza. Quais são os 10 sites mais acessados no Brasil? Veja ranking. **Exame**, Rio de Janeiro, 7 jul. 2021. Disponível em: https://exame.com/tecnologia/ranking-mostra-os-10-sites-mais-acessados-no-brasil-e-no-mundo/. Acesso em: 7 out. 2021.

LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. *In*: SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). **Caderno Especial**: Lei Geral de Proteção de Dados (LGPD). São Paulo: Revista dos Tribunais, 2019. p. 71-85.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet**: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. 2017. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Faculdade de Direito, 2017. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em: 3 out. 2021.

MAYER-SCÖNBERGER. General development of data protection in Europe. *In*: AGRE, Phillip; ROTENBERG, Marc (org.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997.

MCDONALD, Aleecia M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for Information Society**, v. 4, p. 543-570, 2008.

META. **Facebook**, c2004. Política de cookies. Disponível em: https://www.facebook.com/policies/cookies. Acesso em: 12 out. 2021.

O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. New York: Crown, 2016. ISBN 9780553418811.

RODOTÀ, Stefano. **A Vida nas Sociedades da Vigilância**: A Privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: São Paulo: Recife, Renovar, 2008.

RODRIGUES, Ricardo B. *et al.* A cloud-based recommendation model. *In*: EURO AMERICAN CONFERENCE ON TELEMATICS AND INFORMATION SYSTEMS, 7., 2014. **Proceedings** [...]. 2014.

WESTIN, Alan F. **Pivacy and Freedom**. New York: Atheneum, 1970.

Dados do processo editorial

- Recebido em: 21/03/2022
- Controle preliminar e verificação de plágio: 21/03/2022
- Avaliação 1: 30/08/2022
- Avaliação 2: 18/04/2023
- Decisão editorial preliminar: 18/04/2023
- Retorno rodada de correções: 01/05/2023
- Decisão editorial/aprovado: 01/05/2023

Equipe editorial envolvida

- Editor-chefe: 1 (SHZF)
- Editor-assistente: 1 (ASR)
- Revisores: 2