1 Introdução

O presente estudo objetiva desenvolver uma análise do papel e os limites do consentimento do titular de dados na aplicação da política nacional de proteção de dados pessoais no Brasil - implantada com o advento da Lei Geral de Proteção de Dados pessoais (Lei Federal nº 13.709/2018), a fim de responder se tal instrumento, sozinho, é capaz de garantir a autodeterminação informativa de consumidores, ou se a centralidade do consentimento deve ser desconstruída, e este deve ser observado como um instrumento a ser considerado em conjunto a diversos outros, igualmente aptos a promover a proteção de dados pessoais e a autodeterminação informativa de consumidores.

A problemática surge em decorrência do contexto atual, caracterizado por um volume excessivo de dados pessoais, os quais são processados em uma velocidade jamais vista, e dotados de um relevante valor de mercado, contexto o qual ficou conhecido como *Big Data*. Com isso, têm-se diversos mecanismos que atuam extraindo dados pessoais e produzindo informações precisas e preditivas sobre os seus titulares.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor em setembro de 2020, influenciada pelas demais legislações de proteção de dados que surgiram ao redor do globo, as quais foram resultado de pressões e da necessidade da criação de políticas públicas de proteção de dados pessoais em razão do crescimento exponencial do mercado de dados e da vigilância.

A LGPD exige expressamente que o consentimento do titular dos dados pessoais, para fins de tratamento, seja livre, expresso e inequívoco. Nesse sentido, constrói-se uma perspectiva que atribui ao consentimento o papel de promover a segurança e proteção de dados pessoais, bem como, o de conceder aos seus titulares a capacidade de exercer a prometida autodeterminação informativa, ou seja, o controle sobre suas informações pessoais.

Dentre os acontecimentos que desencadearam o surgimento de recentes legislações de proteção de dados no mundo, destacam-se escândalos de vazamento de dados de milhares de pessoas, a eclosão de novas tecnologias de informação, de uma nova economia informacional, e principalmente, o crescimento exponencial dos atores responsáveis pela coleta e mineração de dados, visto que, os mecanismos de vigilância dos indivíduos, para fins públicos e privados, políticos e econômicos, estão cada vez mais presentes no cotidiano. Entretanto, a vigilância não é mais ostensiva, ela se tornou opaca, assim como o fluxo informacional e os algoritmos.

Nesse cenário, surge o questionamento sobre a centralidade do consentimento dos titulares de dados na promoção de uma política de proteção, visto que, o consentimento é tido como um instrumento central, entretanto, diante de um cenário no qual os algoritmos das grandes corporações e governos são considerados como verdadeiras "caixas-pretas impenetráveis", é questionável se a mera anuência do uso de informações pessoais é suficiente para promover o exercício da prometida autodeterminação informativa, em decorrência da falta de conhecimento sobre o processamento e a finalidade do uso de tais informações (ZUBOFF, 2021; BIONI, 2019; O'NEIL, 2020; PASQUALE, 2015).

O contexto criado coloca o elo mais fraco da relação em uma posição de vulnerabilidade agravada, em decorrência da alta complexidade do mercado de dados e dos problemáticos métodos de aceite presentes no mundo virtual. Sendo assim, a partir de de uma pesquisa de natureza aplicada, de abordagem qualitativa, com referencial advindo de pesquisa bibliográfica, e uso do método hipotético-dedutivo, o estudo contempla a hipótese de necessidade de desconstrução da centralidade do consentimento, o qual deve ser observado em conjunto a diversos outros instrumentos, igualmente capazes de promover a proteção de dados pessoais.

Inicialmente, será apresentado o contexto do *Big Data*, e das plataformas digitais, para que seja possível, em seguida, analisar o papel do consentimento qualificado – livre, expresso e inequívoco - previsto pela LGPD, bem como, suas limitações, para que, por fim, seja possível analisar se o consentimento, sozinho, é suficiente para promover a autodeterminação informativa de consumidores e a proteção de dados.

2 O Big Data, as plataformas digitais e a proteção de dados

O *Big Data* é a informação potencializada em volume, velocidade e variedade, o qual requer tecnologias especificas e métodos analíticos para a sua transformação em valor. Sendo assim, ele é caracterizado pelo excessivo volume de dados; pela velocidade a qual estes são coletados e disseminados e pela variedade de informações geradas, bem como, pelo valor atribuído a elas.

Fato é que, é propriamente nas plataformas digitais que o *Big Data* vem atraindo atenção, visto que, são espaços que ofertam um ecossistema de constante otimização de contatos e trocas econômicas, servindo efetivamente como infraestrutura e exercendo diversas formas de controle de informação (FRAZÃO, 2020).

Nos últimos anos, na indústria da tecnologia, a busca por uma maior quantidade de informações vem aperfeiçoando métodos de coleta e armazenamento de dados pessoais, bem como, a criação, através do sistema de algoritmos, de verdadeiros perfis virtuais dos usuários, os quais não atuam unicamente com a finalidade de armazenar os dados pessoais, mas também com a finalidade de modular comportamentos, para que os indivíduos sigam em uma direção preestabelecida, bem como, que permaneçam cada vez mais conectados e sejam influenciados pelos produtos, serviços e ideais propagados na Internet (ZUBOFF, 2021).

Com o advento da Internet e o avanço dos algoritmos, as informações pessoais disponibilizadas, produzidas e distribuídas a todo o instante pelos usuários das redes se tornaram matéria prima para novas transações econômicas, visto que, a necessidade de determinar as preferências de indivíduos e grupos impulsionou o sistema capitalista de tal forma que, se tornou um mercado. Dessa forma, quanto maior a precisão sobre as preferências, os padrões de comportamentos, as emoções e vulnerabilidades dos indivíduos, maiores são os lucros alcançados pelas transações (ZUBOFF, 2021).

A economia do *Big Data* é caracterizada por imensos volumes de dados, a promessa de ganhos espetaculares e a possibilidade de um único programa de computador vasculhar milhares de currículos ou pedidos de empréstimos em um segundo, organizando-os em listas impecáveis, com os candidatos mais promissores no topo (O'NEIL, 2020).

Dessa forma, matemáticos e estatísticos passam a estudar os desejos, as movimentações e o poder de compra de cada um, tornando possível prever a credibilidade e calcular o potencial dos indivíduos. Com isso, o foco deixa de ser nos movimentos dos mercados financeiros globais e passa a ser nos seres humanos (O'NEIL, 2020, p. 7).

Na era do *Big Data*, a coleta e a extração de dados configuram, apenas, a primeira fase de uma cadeia produtiva, pois os dados colhidos devem ser processados para que gerem valor. Isso significa que, o mero acesso aos dados, sem a possibilidade efetiva de transformá-los em informação, é insuficiente para alimentar este mercado, no qual a informação se tornou um ativo de suma importância (O'NEIL, 2020; FRAZÃO, 2021).

Desse modo, o desafio é saber como os dados acessados por diferentes agentes econômicos são convertidos em informação, e, por conseguinte, em poder econômico, o que se torna desafiador justamente porque os modelos utilizados por estes agentes não são transparentes (O'NEIL, 2020; FRAZÃO, 2021).

Conforme dispõe Bioni (2019, p. 135), a ideia de vigilância, revelada pelo romance de George Orwell, era ostensiva, pois a figura do observador e do observado eram bem

delimitadas. Entretanto, houve uma evolução do conceito para os tempos atuais, a atividade não possui mais uma única face, a vigilância não é mais ostensiva, é opaca (BIONI, 2019).

Nesse sentido, as gigantes corporações da indústria da tecnologia estão comprometidas em melhorarem cada vez mais seus mecanismos de atração e vigilância dos indivíduos, a fim de promover uma coleta de informações mais eficiente e precisa sobre os seus usuários.

Sendo assim, a economia entra em uma nova fase, de tal forma que, a monetização de dados adquiridos por vigilância faz surgir um novo sistema capitalista, o capitalismo de vigilância. Vivemos então, diante de uma nova ordem econômica, na qual os dados pessoais, a previsão comportamental dos indivíduos e a possibilidade de intervir nestas passam a ser objeto de transações, com fins comerciais. As estratégias utilizadas pela indústria da tecnologia são desconhecidas pelos usuários das redes, ao passo que, as informações disponibilizadas e extraídas com ou sem a anuência destes são a principal matéria prima destas novas transações econômicas (ZUBOFF, 2021).

Sabe-se que estas informações são utilizadas para fundamentar tomadas de decisões econômicas, políticas e sociais, ou seja, tal fator pode afetar a vida em sociedade, a economia e a democracia. Entretanto, nada se sabe sobre como se dá a operação de tais algoritmos que produzem as informações preditivas, e tampouco sobre a sua finalidade.

Nesse sentido, modelos de algoritmos opacos e invisíveis são a regra, e os transparentes, a exceção. No caso de empresas como a Google, a Amazon e o Facebook, seus algoritmos precisamente talhados valem, sozinhos, centenas de bilhões de dólares, e são caixas-pretas impenetráveis, cujo conteúdo é segredo corporativo altamente protegido. Assim, os três elementos que fazem com que alguns destes modelos venham a ser nocivos - chamados de “Arma de Destruição Matemática” - são opacidade, escala e dano (O’NEIL, 2020).

Quando um modelo ganha escala, ele passa a afetar toda a vida dos indivíduos. É o que ocorre, por exemplo, com o modelo de crédito, que acaba determinando se o indivíduo consegue ou não um apartamento, um emprego ou um carro. Estes modelos matemáticos são opacos e os seus mecanismos invisíveis a todos, exceto aos que possuem domínio sobre eles (O’NEIL, 2020).

É nesse sentido que Frank Pasquale (2015) menciona a existência de um espelho de direção única, ou “*one way mirror”*, ou seja, a vida em sociedade hoje se assemelha a um espelho de direção única, o qual recolhe todas as informações possíveis sobre os indivíduos,

enquanto estes pouco ou nada sabem sobre o funcionamento de algoritmos e a finalidade de tais informações (PASQUALE, 2015).

Cumpre mencionar que existe uma grande disparidade entre a proteção da privacidade de consumidores e associações civis em comparação a proteção destinada às grandes corporações e governos. É reconfortante crer que os dados pessoais de todos os consumidores estão tão protegidos quanto às informações das instituições bancárias, por exemplo. Contudo, não é o que ocorre, visto que, o mundo contemporâneo se assemelha a um espelho de uma única direção, no qual as corporações possuem todo o conhecimento necessário sobre o que fazemos a cada minuto, enquanto não sabemos nada sobre como estas informações são utilizadas para influenciar tomadas de decisões futuras (PASQUALE, 2015).

Nos últimos anos, a privacidade e a vigilância se tornaram assuntos de maior interesse, atenção e cuidado dos usuários das redes. Em paralelo, a demanda pelos serviços de extração e compartilhamento de dados aumentou, o que fez com que tais mecanismos se multiplicassem e fossem utilizados para as mais diversas finalidades, principalmente por fornecedores que buscam informações mais precisas sobre consumidores, de modo que possam realizar sua segmentação de acordo com características comuns.

Diante disso, em atenção ao grande fluxo informacional proveniente da sociedade da informação, surgem leis de proteção de dados pessoais na União Europeia - o *Regulamento Geral sobre a Proteção de dados* (GDPR); bem como, na California - o *California ConsumerPrivacy Act of 2018* (CCPA). Não obstante, em setembro de 2020, passa a vigorar no ordenamento jurídico brasileiro a Lei Geral de Proteção de Dados - Lei Federal nº 13.709/2018 (BRASIL, 2018), com o objetivo de garantir a privacidade e a autodeterminação informativa dos titulares de dados, visto que, de acordo com a legislação, o tratamento de dados é licito quando observa o consentimento voluntário de seu titular, salvo exceções.

3 A lei geral de proteção de dados e o consentimento informado, livre e inequívoco

Com a evolução e o impacto causado pelo uso excessivo dos dados pessoais no cotidiano, a LGPD é observada como um marco regulatório no nosso ordenamento jurídico, fruto da quarta geração de leis de proteção de dados. As legislações provenientes desta geração abrangem alguns aspectos das gerações anteriores, porém diferenciam-se pela disseminação de autoridades independentes para a aplicação de leis e proposições normativas, as quais não mais deixam à mercê do indivíduo a escolha sobre o processamento de alguns tipos de dados pessoais, como os sensíveis, por exemplo, relativizando, assim, a centralidade

do consentimento, presente desde a segunda geração de legislações (BIONI, 2020; DONEDA 2021).

Nesse sentido, o consentimento pode ser analisado em duas perspectivas diferentes, quais sejam, como um processo, um verdadeiro diálogo entre os autores, capaz de assegurar a troca das informações necessárias para uma autorização qualificada, a qual pode, inclusive, se prolongar no tempo, ou, pode ser observado como um ato estático e delimitado no tempo, no qual há o dever pontual de informação e a simples coleta da autorização, estando, portanto, limitado a assinatura de um termo de consentimento (BIONI, LUCIANO, 2020).

A abordagem procedimental, na qual o consentimento é apenas um termo assinado pelo titular dos dados ditou as regras da implantação das leis de proteção de dados ao redor do mundo, com isso, a abordagem do consentimento como um processo, a qual foi estabelecida com a finalidade de garantir a autodeterminação informativa do titular dos dados vem sendo pouco explorada (BIONI, LUCIANO, 2020).

Não obstante, uma análise acerca das gerações de leis de proteção de dados demonstra que o consentimento esteve sempre presente como elemento central capaz de assegurar a proteção de dados pessoais. Nas últimas gerações, inclusive, este recebeu uma série de qualificadores, dessa forma, conforme se extrai da redação da LGPD, o consentimento deve ser livre, inequívoco, específico e expresso. Essa multiplicidade de adjetivos atribuídos ao consentimento demonstra que deve haver um processo racional e informado de tomada de decisão, o qual o titular dos dados não é capaz de atingir sem a cooperação da contraparte que processa seus dados (BIONI, LUCIANO, 2020).

Portanto, observa-se a existência de uma serie de deveres ao controlador de dados, dentre os quais se destaca o dever de informação, o qual exige que ao cidadão sejam propiciados elementos necessários para o inicio de um processo de tomada de decisão no que tange ao fluxo de dados, o que só possível quando se dá forma ao fluxo informacional e se especifica as suas finalidades (BIONI, LUCIANO, 2020).

Dessa forma, é possível reduzir a assimetria de informação que circunda todas estas relações, bem como, estabelecer uma relação mais sincera, transparente e menos danosa, de maneira que a opacidade e a obscuridade com relação ao trânsito de dados pessoais sejam reduzidas.

Ademais, é exigido que o consentimento seja livre e inequívoco, ou seja, que retrate uma ação espontânea, na qual o titular dos dados possui espaço para modular o quão profunda será a sua *persona e* sobre o que poderá influenciá-lo, bem como, que os dados sejam

colhidos para uma finalidade especifica e explicita. Dessa forma, qualquer declaração de vontade deve ter um direcionamento (BIONI, LUCIANO, 2020).

Na era da informação, a privacidade passa a estar associada à noção de autodeterminação informativa, segundo a qual, o individuo é responsável pelas decisões sobre a utilização de seus dados pessoais, de modo que lhe deve ser assegurada a possibilidade de conhecer e controlar a obtenção, tratamento e transmissão de informações referentes a ela, ou seja, a proteção também abrange a liberdade e o poder de discernir, decidir e agir sobre o uso das informações.

Diante disso, é imprescindível que os indivíduos possuam acesso facilitado às informações disponibilizadas, que tenham conhecimento sobre a finalidade, a forma e duração do tratamento de dados, bem como, a identificação do controlador e como se dará o seu uso e compartilhamento (BIONI, 2019; DONEDA, 2020).

Ocorre que, no contexto apresentado, caracterizado por uma maçante coleta e processamento de dados pessoais através de algoritmos, os quais muito pouco se sabe a respeito, o almejado consentimento informado, livre e inequívoco, dotado de uma clara e transparente especificação do fluxo informacional dificilmente configura uma realidade.

Diante de um complexo ecossistema formado por diversos agentes econômicos capazes de lidar com dados pessoais acumulados, o fluxo informacional se torna completamente volátil. Dessa forma, o titular dos dados pessoais deveria ter consciência a respeito de todos os atores envolvidos e de suas respectivas práticas de mineração de dados, para que, ao final, pudesse gerenciar as suas informações pessoais. Entretanto, diante da racionalidade limitada do ser humano, sabe-se que, pouco provavelmente este será capacitado para tanto (BIONI, 2019).

Dessa forma, atribuir ao titular dos dados a responsabilidade por controlar o fluxo de suas informações, através do consentimento, não necessariamente configura um ato de empoderamento deste cidadão. Diante das habilidades cognitivas limitadas do ser humano, a sua capacidade de absorver, memorizar e processar todas as informações relevantes para um processo de tomada de decisão é questionável. A memorização dos inúmeros atores que compõem as redes de troca de dados, bem como, o processamento e o tratamento destinado a tais informações não é de fácil compreensão para grande parcela da população (BIONI, 2019).

Nesse sentido veremos na seção seguinte os aspectos formais consonantes ao consentimento, a fim de averiguar se, na prática, o instrumento vem sendo utilizado para promover a redução de assimetrias existentes ou, se, pelo contrario, tal mecanismo vem sendo

empreendido para reforçá-las. Assim, é possível concluir se o instrumento é apto a promover a proteção de dados pessoais e a autodeterminação informativa de consumidores.

4 Consentimento como instrumento apto a promover a proteção de dados pessoais e a autodeterminação informativa?

Inicialmente, é nítido que, muitos mecanismos não se ocupam em assegurar o consentimento qualificado dos titulares, visto que, o uso da internet se naturalizou de tal forma que, os usuários navegam nas redes porque necessitam, sendo assim, ao acessar determinado site ou utilizar determinada rede social, não calculam o ônus que lhes é imposto, qual seja, de serem compelidos a fornecerem as suas próprias informações de navegação, os chamados "*cookies",* para que estas sejam objeto de transações econômicas que filtram suas preferências e se transformam em estratégias de mercado, e, portanto, beneficiam os provedores de navegação e eventuais anunciantes, podendo-lhe causar prejuízos.

Ademais, mesmo que os usuários das redes se atentem ao uso dos *cookies,* não lhes é garantido qualquer direito de modulação sobre o tratamento que será destinado a estes, bem como, quais dados serão coletados e por quanto tempo.

Nesse sentido, inexiste poder de barganha sobre os dados fornecidos e a finalidade que lhes será dirigida, visto que, o titular fica impedido de modular ou selecionar os dados que deseja fornecer, ou optar por não fornecer quaisquer dados (BIONI, 2019; MAZZIVIERO, ROCHA, 2020).

Com a Lei Geral de Proteção de Dados, alguns sites passaram a inserir abas que informam o uso de *cookies* e exigem que o usuário preste sua anuência através de um clique, enquanto outros apenas colocaram abas informando o uso de *cookies*, sem exigir a anuência dos usuários. Contudo, caso o usuário não preste a sua ciência sobre o uso de suas informações pessoais, fica impedido de prosseguir navegando. Dessa forma, o indivíduo é compelido a prestar ciência caso haja necessidade de acessar o site, o que não configura um consentimento qualificado, pois o titular encontra-se inserido em uma lógica de tudo ou nada.

> Na verdade, é possível visualizar o aceite dos termos e condições de uso ou dos cookies como uma assinatura de contrato de adesão, visto que, tais termos foram previamente estabelecidos pelo fornecedor, sem que o consumidor possa selecionar quais dados deseja fornecer, por isso a problemática do "consentimento involuntário" obtido com apenas um clique (MAZIVIERO, ROCHA, 2020, p. 12).

Com isso, pode-se afirmar que as políticas de privacidade de *sites* e plataformas digitais são contratos de adesão, diante da massificação das relações contratuais ordinárias, há uma padronização dos instrumentos contratuais. Sendo assim, ao consumidor cabe apenas aderir ou não a referida política de privacidade (MAZIVIERO, ROCHA, 2020; BIONI 2019).

Dessa forma, quem dita os rumos do fluxo informacional é o fornecedor, o qual acaba eliminando qualquer faixa de controle a ser exercida pelos titulares dos dados. Por isso, fala-se sobre a mistificação da autodeterminação informacional, visto que, tais políticas de privacidade utilizam ferramentas inapropriadas para garantir ao consumidor o controle de suas informações pessoais (BIONI, 2019).

Vale ressaltar que a tecnologia pode ser usada como ferramenta capaz de promover a tutela dos dados pessoais, como propõe as *Privacy Enhancing Technologies/PETS*. Trata-se de tecnologias que facilitam o controle e a proteção dos dados pessoais por seus titulares, as quais empoderam o consumidor e proporcionam que este esteja municiado em meio à corrida tecnológica da vigilância, exercendo controle sobre a captação e mineração de seus dados. Entretanto, tal agenda merece ser objeto de estratégias regulatórias, podendo auxiliar na aplicação de uma política de proteção de dados pessoais mais efetiva (BIONI, 2019).

Não obstante, a LGPD não regulou de forma clara como se daria a forma do consentimento do titular de dados no meio digital. Portanto, uma reformulação nesse sentido seria ideal, para que efetivamente seja alçada uma maior autonomia por parte do elo mais fraco da relação, facilitando o processo de tomada de decisão. Dessa forma, a debilidade do vulnerável para tomar decisões genuínas seria amenizada (BIONI, 2019).

Enquanto isso, os consumidores continuam prestando a sua anuência através de um clique, sem saber sobre o destino das informações compartilhadas, as quais podem ser utilizadas indevidamente, de maneira tendenciosa, com a finalidade de modular comportamentos deste titular ou até mesmo discriminá-lo, causando, portanto, consequências nocivas a ele.

A previsão do art. 2º, II da LGPD fornece ao titular dos dados uma falsa sensação de que possui controle e autonomia sobre os seus dados e a disposição deles, quando, na realidade, a autodeterminação informativa é impossível de ser assegurada nesse contexto, diante da ausência de escolhe a qual é submetido.

> Essa ausência de escolha é mascarada pela referida "autodeterminação informativa" (artigo 2º, inciso II), porém não passa de um "consentimento involuntário", em que o consumidor se vê forçado a aceitar o que lhe é imposto para que possa acessar o serviço, fazendo com que seus dados fiquem armazenados pela empresa,

> desconhecendo o destino e a segurança deles no banco de dados. (MAZIVIERO, ROCHA, 2020, p. 14)

Portanto, verifica-se que a LGPD não se ocupou em regular o consentimento qualificado de maneira clara, pois não determina os meios como as condições de aceite dos termos de uso e dos *cookies* serão apresentadas aos usuários, o que enfraquece a proteção jurídica, em razão da ausência de informação aos indivíduos sobre as consequências do aceite e sobre a necessidade de proteção de seus dados pessoais (ROCHA, MAZIVIERO, 2020, p. 13).

Com isso, o consentimento como um mecanismo a assegurar a autodeterminação informativa e garantir a proteção de dados pessoais tem se mostrado falho, ao reforçar a assimetria inerente ao mercado informacional, bem como, por se tratar de uma ferramenta que não assegura, efetivamente, o cidadão a exercer controle sobre suas próprias informações (BIONI, 2019).

Não obstante, o consentimento não qualificado é naturalizado por muitos modelos, sendo, portanto, conseqüência dos problemáticos métodos de aceite no mundo virtual, bem como, da impossibilidade de negociação e o grande *déficit* informacional existente nestas relações.

Apesar da vulnerabilidade acentuada caracterizada, o consentimento ainda assume um papel de destaque na legislação, assim como ocorreu durante todo o percurso geracional normativo da proteção de dados pessoais. Não obstante, o titular dos dados pessoais dificilmente possuirá controle direto sobre o fluxo de suas informações pessoais, em decorrência da exacerbada assimetria existente, bem como, da complexidade inerente às novas tecnologias e aos algoritmos.

A coleta e o compartilhamento de dados é uma prática necessária para a manutenção da internet e de todo o mercado virtual dela decorrente, visto que, é o que mantém o meio virtual na atividade, sendo, portanto, imprescindível para o seu funcionamento. Sendo assim, é o custo pago pelos indivíduos para utilizarem os mecanismos digitais.

Entretanto, tal custo vem aumentando sem precedentes, visto que, a) a Internet se desenvolveu de tal maneira que se tornou uma extensão do mundo real, sendo assim, se torna cada vez mais difícil se manter distante das redes e, portanto, dos mecanismos de algoritmos e de vigilância; b) os usuários das redes não possuem a opção de não ceder suas informações pessoais ou modular os dados que desejam fornecer quando acessam sites ou redes sociais; c) os indivíduos não possuem conhecimento acerca do fluxo de seus dados pessoais que são

fornecidos ou extraídos, em razão da complexidade do meio virtual; d) configura-se uma nova vulnerabilidade informacional, técnica e econômica do titular dos dados, a qual deve ser analisada de maneira objetiva e não subjetiva, visto que, é fruto de um aspecto objetivo, qual seja, a emergência de uma nova economia movida a dados.

A LGPD exige o consentimento informado, livre e inequívoco dos titulares, o qual, conforme observado acima, não vem sendo alcançado na navegação no mundo digital. Sendo assim, esta "hipertrofia do consentimento" traz implicações normativas importantes, visto que, ao mesmo tempo em que se preocupa em programar um consentimento extremamente qualificado, corre o risco de limitar o terreno por ele ocupado, visto que, tal consentimento dificilmente será alcançado na prática, assim, é possível que haja uma fuga para as outras hipóteses de tratamentos de dados previstas na legislação, as quais não exigem a presença da anuência qualificada (BIONI, 2019; BIONI, LUCIANO, 2020).

Sendo assim, o papel do titular dos dados como ponto focal nas leis de proteção de dados pessoais persiste, e merece ser revisto, assim como, a vinculação da licitude do tratamento de dados ao consentimento do indivíduo, visto que, com a emergência de novas tecnologias, a atividade da coleta e do uso de dados ficou mais complexa e menos transparente.

A assimetria existente entre a figura do consumidor e do controlador de dados fica cada vez mais evidente, especialmente, em uma perspectiva voltada ao contexto do *Big Data*, caracterizado pela atuação das grandes plataformas digitais, pelo monitoramento e pela vigilância constante dos indivíduos, pelas dificuldades de regulamentar o mercado e pela tenacidade com que as corporações defendem seus novos territórios (FRAZÃO, 2021, p. 537; ZUBOFF, 2020).

Ocorre que, a estratégia regulatória segue uma lógica contrária a constatação da hipervulnerabilidade do titular de dados pessoais, pois, apostam-se todas as fichas normativas no elo mais fraco da relação, considerando que o sujeito é livre, capaz e racional para fazer valer a proteção de seus dados pessoais (BIONI, 2019).

O protagonismo do consentimento demonstra a contradição intrínseca dessa estratégia regulatória, pois, atribuir ao titular dos dados o protagonismo quanto à proteção e ao controle de seus dados pode contribuir para que a assimetria de poder existente seja acentuada (BIONI, p. 116, 2020; MAIOLINO; MARQUES; TIMM, 2020).

A própria lógica das trocas provenientes da econômica de dados pessoais demonstra que, frente a tal arquitetura de escolhas de decisões, a crença de que o cidadão é um agente racional capaz de desempenhar um processo genuíno de tomada de decisão não se sustenta

neste contexto, em decorrência de toda a complexidade inerente ao fluxo das informações pessoais, visto que, ele está em uma situação de vulnerabilidade específica, diante de uma relação assimétrica.

Existe uma grande discrepância entre o paradigma normativo da proteção de dados pessoais, pautado na autodeterminação informativa, e o funcionamento do mercado informacional. Diante disso, observa-se a necessidade de complementar a problemática com tecnologias que funcionem através de uma arquitetura de empoderamento do consumidor hipervulnerável.

Entretanto, o consentimento do titular da informação não deve ser considerado o único recurso a ser utilizado para promover a proteção de dados pessoais, visto que, isso seria limitar-se a uma abordagem unicamente procedimental, instrumentalizando o titular da informação com o direito em autodeterminar as suas informações.

Em que pese toda a literatura crítica teórica e empírica do consentimento como a estratégia central para a proteção de dados pessoais, é necessário analisar soluções alternativas, visto que, surge a necessidade de não deixar toda a carga de proteção dos dados pessoais sob responsabilidade do indivíduo. Sendo assim, impor limites ao consentimento contribui para alcançar um fluxo informacional apropriado (BIONI, 2019).

5 Considerações finais

Em suma, procurou-se demonstrar que a programada autonomia dos consumidores para controlar seus dados pessoais é mitigada pelo mercado sedento por um ativo econômico, dessa forma, a lógica da economia de dados pessoais prevalece e impõe as suas forças sobre a parte mais vulnerável da relação.

Nesse contexto, os consumidores se mostram impotentes para fazer valer o seu desejo de controlar seus dados pessoais, especialmente, em observância ao contexto do *Big Dat*a, no qual os agentes econômicos de grande porte processam informações em uma velocidade e volume jamais vistos na história.

A análise se volta ao contexto do *Big Data*, visto que, as transações e os algoritmos se tornaram mecanismos dotados de tamanha complexidade que, uma especificação do fluxo informacional se torna inviável, e, portanto, diante de uma predominância da opacidade em detrimento da transparência, dificilmente o titular dos dados será capaz de exercer controle sobre suas informações.

Sendo assim, a almejada autodeterminação informativa não será alcançada caso não sejam considerados o *déficit* informacional natural destas relações e o contexto de vulnerabilidade no qual o individuo se encontra, para fins de implementação de novos métodos de aceite, os quais são essenciais para que a autodeterminação informativa não seja mais uma falácia imposta pelo mercado de dados pessoais, o qual mistifica a capacidade dos cidadãos de autoproteção de seus dados pessoais.

Diante desta complexidade e inviabilidade de especificação do fluxo informacional em inúmeras situações, a figura do consentimento informado, claro e inequívoco merece ser melhor investigada, visto que, atribuir ao titular dos dados a responsabilidade em conduzir o fluxo informacional, quando tal agente não está munido de ferramentas capazes de reduzir a assimetria inerente a estas relações pode ser contribuir para aumentar ainda mais a discrepância existente entre os polos da relação extremamente assimétrica.

Conforme objetivou demonstrar, a forma pela qual o titular dos dados costuma consentir com o uso de suas informações não foi adequadamente regulada pela legislação, e, portanto, na prática, não vem contribuindo para reduzir a assimetria existente, em decorrência dos problemáticos métodos de aceite, da impossibilidade do titular dos dados modular as informações que deseja desejar ou a finalidade que lhes será destinada. Nesse sentido, a LGPD carece de dispositivos destinados a estabelecer a metodologia adequada para que o processo de consentimento seja assegurado, e assegurar de forma suficiente o consentimento voluntário dos indivíduos.

Conclui-se, portanto, que o consentimento de titulares de dados dificilmente será um mecanismo capaz de, sozinho, proporcionar que os titulares exerçam o almejado controle sobre suas informações pessoais, em que pese a importância e necessidade de tal instrumento, no momento presente, caracterizado por uma exacerbada assimetria entre os polos que configuram as relações no meio virtual, o consentimento não deve ser um elemento central em uma política de proteção, especialmente por não considerar a vulnerabilidade agravada dos titulares de dados e não configurar um instrumento que se ocupa em reduzi-la.

REFERÊNCIAS

BASTOS, Elísio Augusto Velloso, MIRANDA, Cristina Pires Teixeira de. Sociedade em Rede, Novas Tecnologias, Privacidade, Consumo e Vulnerabilidade: Necessidade de Proteção Eficiente do Consumidor no Ambiente das Novas Tecnologias de Informação e comunicação. In: VERBICARO, Dennis; VERBICARO, Loiane; VIEIRA, Janaina (Cord.); **Direito do consumidor digital**. Rio de Janeiro: Lumen Juris, 2020.

BAUMAN, Zygmund. **Modernidade Líquida**. Rio de Janeiro: Jorge Zahar, 2001.

BAUMAN, Zygmund. **Vida para consumo**. Rio de Janeiro: Jorge Zahar, 2001.

BIONI, Bruno Ricardo, LUCIANO. Maria. O consentimento como processo: Em busca do consentimento válido. In: BIONI, Bruno; DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang (Coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2020.

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

BRASIL. Câmara dos deputados. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados pessoais.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 26 nov 2020.

CASTELLS, Manuel. A sociedade em rede. **A era da informação: Economia, sociedade e cultura**. Vol. 1. 21ª ed. São Paulo, SP: Paz&Terra, 2020.

DONEDA, Danilo. A autoridade nacional de proteção de dados e o conselho nacional de proteção de dados. In: BIONI, Bruno; DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang (Coord**.). Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

E SILVA, Leandro Novais; MOURÃO, Carlos. A proteção de dados pessoais à luz do direito concorrencial: Portabilidade de dados, infraestruturas essenciais e open banking. **Revista de Defesa da Concorrência**. P. 31-53, Vol 8, nº 2, Dez. 2020. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/649. Acesso em: 16 jul. 2021.

FRAZÃO, Ana. Big Data e aspectos concorrenciais do tratamento de dados pessoais. In: BIONI, Bruno; DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas Digitais e o Negócio de Dados: Necessário Dialógo entre o direito da concorrência e a regulação de dados. **Revista Direito Público**, Brasília, DF, Vol. 17, nº 93, p. 58-81, Mai/Jun 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3695>. Acesso em 17 jul 2021.

GUARDIAN, THE. Edward Snowden: '**As pessoas ainda estão impotentes, mas agora estão cientes**'.Disponível em: https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware. Acesso em: 04 dez. 2020.

GUARDIAN, THE. **Revelado: 50 milhões de perfis do Facebook coletados para Cambridge Analytica em grande violação de dados**. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 04 dez. 2020.

LYPOVESTKY, Gilles. **A felicidade paradoxal: Ensaio sobre a sociedade do hiperconsumo**. São Paulo: Companhia das Letras, 2007.

MAIOLINO Isabela; MARQUES Leonardo Albuquerque; TIMM, Luciano Benetti. Desafios para a defesa do consumidor, proteção de dados e concorrência: necessidade de coordenação entre os sistemas. In: DONEDA; Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Boas (Org). **Lei Geral de proteção de dados (Lei 13.709/2018): A caminho da efetividade: Contribuições para a implementação da LGPD**. São Paulo, SP: Thomson Reuters Brasil, 2020.

MAZIVIERO, Luiza Nobre, ROCHA, Luiz Alberto. Por um Clique: Como a Lei Geral de Proteção de Dados Pessoais possibilidade o "consentimento involuntário de fornecimento de informações de Particulares a Empresas. In: VERBICARO, Dennis; VERBICARO, Loiane; VIEIRA, Janaina (Cord.); **Direito do consumidor digital**. Rio de Janeiro: Lumen Juris, 2020.

O'NEIL, Cathy. **Algoritmos de destruição em massa: Como o big data aumenta a desigualdade e ameaça a democracia**. Tradução de Rafael Abraham. Santo André, SP: Rua do Sabão, 2020.

ORWELL, George. **1984**. Tradução de Alexandre Hubner e Heloisa Jahn. São Paulo, SP: Companhia das Letras, 2009.

PASQUALE, Frank. **The Black Box society: The secret algoritims that control Money and information**. Cambridge, Massachussets: Havard University Press, 2015.

SCHWARTZ. Fábio. Análise Econômica da Responsabilização Civil das Plataforamas Virtuais na Economia Compartilhada.In: VERBICARO, Dennis; VERBICARO, Loiane; VIEIRA, Janaina (Cord.); **Direito do consumidor digital**. Rio de Janeiro: Lumen Juris, 2020.

TIMES, THE NEW YORK. **NSA triplica coleta de dados de empresas de telefonia dos EUA**.Disponível em: https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html. Acesso em: 04 dez. 2020.

TIMES, THE NEW YORK.**Cambridge Analytica e Facebook: The Scandal and the Fallout So Far**.Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 04 dez. 2020.

ZUBOFF, Shoshanna. **The Age Of Surveillance Capitalism: The fight for a human future at the new frontier of power**. PublicAffairs, 2019.

ZUBOFF, Shoshanna.Big other: Capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (org.) **Tecnopolíticas da Vigilância: Perspectivas da margem**. Boitempo, 2018.

ZUBOFF, Shoshannna. **Um capitalismo de vigilância**. Le monde diplomatique, 2019. Disponível em: https://diplomatique.org.br/um-capitalismo-de-vigilancia/ Acesso em: 26 dez. 2020.