

Big Data E Manipulação On-Line Dos Usuários: Revisão Sistemática Da Literatura À Luz Do Direito De Personalidade À Liberdade

Big Data And Online Manipulation Of Users: A Systematic Literature Review In Light Of The Personality Right To Freedom

Ana Elisa Silva Fernandes *

Dirceu Pereira Siqueira **

RESUMO: Na contemporaneidade têm surgido diversos estudos sobre as novas tecnologias e os seus impactos sobre os direitos da pessoa. Nesse contexto, este artigo tematiza as possíveis tensões entre o direito de personalidade à liberdade e a manipulação comportamental realizada pelas mídias sociais por meio do big data. O problema que orienta a pesquisa pode ser assim sintetizado: em que medida há estratégias de manipulação comportamental dos usuários nas mídias sociais e como a literatura estrangeira perspectiva a temática? Parte-se da hipótese inicial de que há um contexto de manipulação on-line dos comportamentos que acarreta tensões aos direitos de personalidade, como o direito de personalidade à liberdade e à autonomia humana. O objetivo geral do estudo consiste em analisar a noção de manipulação on-line e investigar quais perspectivas são formuladas na literatura estrangeira sobre o tema, sob o viés dos direitos da personalidade. O texto está dividido em duas seções que correspondem aos seus objetivos específicos. Na primeira seção apresenta os fundamentos teóricos que conduziram à hipótese inicial. Na segunda seção, analisa os resultados da revisão sistemática da literatura realizada. Utiliza-se o método hipotético-dedutivo e a técnica de investigação de revisão bibliográfica comum na primeira seção, e revisão sistemática da literatura estrangeira na base de dados Web of Science, na segunda seção.

ABSTRACT: In contemporary times, several studies on new technologies and their impacts on the rights of the individual have emerged. In this context, this article discusses the possible tensions between the personality right to freedom and the behavioral manipulation carried out by social media through big data. The problem that guides the research can be summarized as follows: to what extent are there strategies of behavioral manipulation of users in social media and how does the foreign literature approach the issue? We start from the initial hypothesis that there is a context of online manipulation of behavior that causes tensions to personality rights, such as the personality right to freedom and human autonomy. The general objective of the study is to analyze the notion of online manipulation and investigate which perspectives are formulated in the foreign literature on the subject, from the perspective of personality rights. The text is divided into two sections that correspond to its specific objectives. The first section presents the theoretical foundations that led to the initial hypothesis. The second section analyzes the results of the systematic literature review. The hypothetical-deductive method is used and the research technique of common literature review is employed in the first section, and systematic review of foreign literature in the Web of Science database in the second section.

PALAVRAS-CHAVE: Direito de personalidade. Direito geral de liberdade. Mecanismos de poder. Governamentalidade algorítmica.

KEYWORDS: Personality rights. General right of freedom. Mechanisms of power. Algorithmic governmentality.

SUMÁRIO: Introdução. 1 Capitalismo de vigilância, governamentalidade algorítmica e comportamento *on-line*: entre controle e a ameaça aos direitos da pessoa. 2 Análise dos resultados na revisão sistemática da literatura sobre *big data* e manipulação *on-line*. 3 Conclusão. Referências.

* Doutoranda em Direito com ênfase em Direitos da Personalidade pela UNICESUMAR. Bolsista no Programa de Suporte à Pós-Graduação de Instituições de Ensino Particulares PROSUP/CAPES (módulo Bolsa) pelo Programa de Pós-Graduação em Ciências Jurídicas na UNICESUMAR. Membro do Grupo de Pesquisa do CNPq: “Políticas Públicas e Instrumentos Sociais de Efetivação dos Direitos da Personalidade”. Mestre em Ciências Jurídicas com ênfase em Direitos da Personalidade pela UNICESUMAR. Graduada em Direito pela Pontifícia Universidade Católica do Paraná.

** Coordenador e Professor Permanente do Programa de Doutorado e Mestrado em Direito da Universidade Cesumar, Maringá, PR (UniCesumar); Pós-doutor em Direito pela Faculdade de Direito da Universidade de Coimbra (Portugal), Doutor e Mestre em Direito Constitucional pela Instituição Toledo de Ensino - ITE/Bauru, Especialista Lato Sensu em Direito Civil e Processual Civil pelo Centro Universitário de Rio Preto, Pesquisador Bolsista - Modalidade Produtividade em Pesquisa para Doutor - PPD - do Instituto Cesumar de Ciência, Tecnologia e Inovação (ICETI), Professor nos cursos de graduação em direito da Universidade de Araraquara, (UNIARA) e do Centro Universitário Unifafibe (UNIFAFIBE), Professor Convidado do Programa de Mestrado University Missouri State – EUA, Editor da Revista Direitos Sociais e Políticas Públicas (Qualis B1), Consultor Jurídico, Parecerista, Advogado.

INTRODUÇÃO

Na sociedade contemporânea, marcada pelo viés tecnológico, têm surgido estudos sobre as novas tecnologias e seus impactos sobre os direitos da pessoa humana. A construção teórica sobre as mídias sociais e *big data*, como o desenvolvido por Shoshana Zuboff (2020) na obra *Capitalismo de Vigilância*, indica a existência de um novo poder, o instrumentalismo, que atua para modificação, predição, monetização e controle dos comportamentos humanos, a partir dos *superávits* comportamentais. Esses mecanismos também objetivam a formulação de previsões comportamentais e a orientação do comportamento do usuário inclusive no mundo *off-line*, de forma velada.

O tema deste artigo, então, recai sobre os estudos que abordam essa problemática. Diante da existência de um cenário de possível violação a direitos de personalidade, busca-se responder ao seguinte problema de pesquisa: em que medida há estratégias de manipulação comportamental dos usuários nas mídias sociais e como a literatura estrangeira perspectiva a temática? Parte-se da hipótese inicial de que há um contexto de manipulação *on-line* dos comportamentos que acarreta tensões aos direitos de personalidade, como o direito de personalidade à liberdade e a autonomia humana, que também se espalha para o mundo *off-line*.

Como desdobramento do objetivo geral, os objetivos específicos estão distribuídos e organizados nas duas seções do artigo. A primeira seção analisa os fundamentos teóricos que conduziram ao questionamento e hipótese inicial sobre as perspectivas de manipulação e controle realizada nas mídias sociais, como as teorias do Capitalismo de Vigilância de Zuboff (2020) e governamentalidade algorítmica de Antoinette Rouvroy (2015). Na segunda seção, o estudo apresenta a revisão sistemática da literatura e os resultados encontrados.

Como percurso metodológico para o desenvolvimento da pesquisa, foi utilizado o método de abordagem hipotético-dedutivo e a técnica de investigação de revisão bibliográfica comum na primeira seção, e revisão sistemática da literatura estrangeira na base de dados *Web of Science*, na segunda seção.

Espera-se, com a revisão sistemática, encontrar fundamentos empíricos que confirmem ou não a hipótese que, teoricamente, tem sido defendida pelos autores citados na primeira seção, isto é, de que existe um cenário de possível violação à liberdade e autonomia humana por meio

da manipulação *on-line* possibilitada pelo *big data*, com reflexos no mundo *off-line*. Ressalta-se que esta pesquisa não pretende esgotar a temática, mas pretende visualizar em que medida a manipulação *on-line* tem sido discutida na literatura estrangeira, diante as evidências teóricas de uma possível tensão das tecnologias de informação frente à liberdade e autonomia humana.

1 CAPITALISMO DE VIGILÂNCIA, GOVERNAMENTALIDADE ALGORÍTMICA E COMPORTAMENTO *ON-LINE*: ENTRE CONTROLE E A AMEAÇA AOS DIREITOS DA PESSOA

O uso das tecnologias de informação *on-line* tornou-se realidade na vida de grande parte das pessoas na sociedade contemporânea. Essas tecnologias têm impactado a sociedade e seus diversos setores, tal como a economia e a política, adentrando na vida dos sujeitos e seus relacionamentos. A internet foi transformada em um sistema orientado principalmente por elementos informacionais para permitir a comunicação e a cooperação entre os usuários. Nessa medida, houve o crescimento exponencial da quantidade de conteúdo *on-line* e plataformas que possibilitam a entrada de elementos informativos como as redes sociais e comunidades, assim como as plataformas de compra com perfis individualizados (ALLMER, 2015, p. 44-45).

Nesse contexto, a internet pode ser entendida como um sistema tecno social triplo, de cognição humana, comunicação e cooperação, na medida em que sua infraestrutura é composta por sistemas tecnológicos (subsistema tecnológico; rede de redes de computadores) e atores humanos (subsistema social; rede de redes sociais). Ambos os subsistemas estão relacionados na medida em que a estrutura técnica é um meio e resultado da agência humana (ALLMER, 2015, p. 53).

Segundo Fuchs (2008, p. 122-123), a estrutura tecnológica das redes armazena o conhecimento humano objetivo ao possibilitar que as pessoas ajam, se comuniquem ou cooperem de tal forma que o conhecimento armazenado pela estrutura tecnológica muda, é atualizado e expandido. Em outras palavras, há a subjetivação do conhecimento objetivo das pessoas quando elas consomem o conteúdo digital, se comunicam e cooperam com outros sujeitos por meio da internet. A estrutura tecnológica tornou-se a ferramenta que intermedia, na

contemporaneidade, as atividades humanas e resulta em aspectos emergentes do pensamento e da ação.

Acontece que, para que essas plataformas se tornassem cada vez mais eficazes, foram aprimoradas formas de vigilância para a coleta e tratamento de dados. Quanto mais dados, melhores condições tecnológicas as plataformas entregam, o que facilita o dia a dia das pessoas. Assim, as tecnologias de vigilância, de coleta e tratamento de dados evoluíram. Conseqüentemente, houve uma extensão e intensificação de ameaças à privacidade e riscos de vigilância em contextos econômicos, políticos e culturais nos últimos anos, também baseados no emprego de várias tecnologias de vigilância (ALLMER, 2015, p. 54).

Nesse contexto, a literatura crítica no tema tem refletido sobre a existência de um exercício de vigilância e controle sobre as pessoas cada vez mais abrangente, profundo e irrefletido. Nos estudos que se destacam na análise das novas tecnologias *on-line*, há teóricos que apontam a existência de uma nova relação de poder e controle sobre as pessoas. Allmer (2012, p. 74-90) identifica dois grandes posicionamentos nos estudos contemporâneos sobre vigilância *on-line*. De um lado, estariam as abordagens que consideram a vigilância de modo mais negativo, como uma forma de controle e de dominação sobre as pessoas¹. Do outro lado, estão as abordagens que a concebem de modo mais neutro e não necessariamente negativo².

No contexto da primeira perspectiva, tem destaque a tese do capitalismo de vigilância de Zuboff (2020), segundo a qual há uma nova ordem econômica que se estrutura a partir da vigilância dos usuários nas redes. Nessa perspectiva, por meio da análise e tratamento de dados, transformam-se os dados comportamentais dos usuários em um *superávit comportamental* a ser comercializado no que a autora chama de “mercado de comportamentos futuros” (ZUBOFF, 2020, p. 22).

Esses dados de não mercado referem-se a dados colaterais que deixam em evidência o comportamento do usuário nas mídias sociais e que não se referem necessariamente a compras

¹ Destacam-se autores como Greg Elmer (1997), Dwayne Winseck (2003), Manuel Castells (2001), Michael Levi e David Wall (2004), Joseph Turow (2006), Marc Andrejevic (2004; 2007), John Edward Campbell e Matt Carlson (2002), Ashlee Humphreys (2006), Ian Brown e Douwe Korff (2009), Brian Krueger (2005), Michael Mehta e Eric Darier (1998) e MacGregor Wise (2004).

² Dentre os autores que seguem essa posição, destacam-se David Lyon (1994; 1998; 2001; 2003), Seumas Miller e John Weckert (2000), Jeffrey Stanton e Elizabeth Weiss (2000), Barbara Kaye e Thomas Johnson (2002) e Hille Koskela (2006).

on-line (como o número e padrão de termos de busca; pontuação; ortografia; tempo de visualização; padrões de cliques; localização) (ZUBOFF, 2020). Trata-se não só de dados pessoais ou dados pessoais sensíveis relevantes, mas de todo e qualquer tipo de informação que, embora não identifique o usuário, dizem respeito ao seu comportamento *on-line*.

Segundo Allmer (2015, p. 56), as ações de vigilância são cruciais no processo de produção de mercadorias no capitalismo. E, no atual contexto, a vigilância é um aspecto importante para garantir a produção de mais-valia e acúmulo de lucro nas esferas da produção, circulação e consumo do capitalismo de vigilância. Então, as plataformas desenvolveram algoritmos de vigilância que coletam os rastros digitais da personalidade, como vozes, imagens, preferências, reações *on-line*, dentre outros, que se encontram nos perfis das mídias sociais dos usuários e compõem os chamados dados comportamentais *on-line* de não mercado (COSTA; OLIVEIRA, 2019, p. 26). Esses algoritmos são programados para a extração de padrões e inferências a sobre os usuários que são desconhecidos deles. A partir dessas inferências, segundo Frazão (2019, posição 1051), serão tomadas, de forma automatizada, decisões sobre questões objetivas e subjetivas para a maior personalização dos perfis.

Para tanto, as plataformas criam bancos de dados comportamentais sobre os usuários (*big data*), por meio da coleta automatizada de dados (*dataveillance*). O *big data* é constituído por todo tipo de rastro digital coletado do tráfego de dados na internet, (cliques, compartilhamentos em mídias sociais, rastreamento de GPS, dados móveis, imagens de câmeras de segurança e de satélite, transações bancárias etc). Diversos dispositivos são responsáveis por produzir dados, emitindo informações sobre o usuário e alimentam grandes bancos de dados, ainda que *off-line* (ALVES, 2019, p. 10).

Toda essa evolução das tecnologias, como expressão do capitalismo contemporâneo, seguiu acompanhada da ascensão de grandes corporações de tecnologias chamadas de *Big Techs* (como Google, Apple, Facebook, Amazon e Microsoft etc). Embora elas sejam modernas em termos de sofisticação, toda a tecnologia empregada pelas *Big Techs* não é neutra e essas grandes empresas representam o atraso civilizatório no que tange à flexibilização e redução de direitos, a centralização e concentração de capitais e o poder das corporações privadas acima dos espaços públicos, além de outros processos que caracterizam as soluções capitalistas para suas crises (INSTITUTO TRICONTINENTAL DE PESQUISA SOCIAL, 2021, p. 13).

Na sociedade contemporânea, essas empresas assumiram o papel de meios de comunicação e de agentes ideológicos privilegiados na sociedade. Acontece que por trás das tecnologias acessíveis aos usuários, há o trabalho de especialistas cientistas/analistas de dados que trabalham para projetar determinadas políticas na opinião pública (INSTITUTO TRICONTINENTAL DE PESQUISA SOCIAL, 2021, p. 13).

Por tratar-se de um mercado próspero e diante do potencial de utilização dos dados para fins mercadológicos, as *Big Techs* passaram a investir em mecanismos de vigilância para coleta, análise e tratamento de dados dos usuários cada vez mais imperceptíveis. O objetivo desse investimento pelas grandes empresas de tecnologia era proporcionar “melhorias nas campanhas de marketing com personalização e *profiling*, acesso a novos possíveis clientes, personalização de produtos e serviços e, conseqüentemente, a nova perspectiva de lucratividade” (DORNELAS, 2021, p. 82).

Diante deste cenário, tem-se discutido na literatura sobre a potencialidade desse capitalismo de vigilância ameaçar o direito à privacidade das pessoas. Mas, para além da privacidade, a partir da tese de Zuboff (2020), nesta pesquisa, vislumbra-se também uma possível ameaça à liberdade e autonomia humana - noções basilares ao Direito, especialmente pela liberdade tratar-se tanto de um princípio fundamental quanto de um direito de personalidade.

Segundo Zuboff (2020), no capitalismo de vigilância surge uma nova forma de poder, o *instrumentalismo*, que busca a “instrumentação e instrumentalização do comportamento para propósitos de modificação, predição, monetização e controle” sobre as pessoas (ZUBOFF, 2020, p. 402). Em outras palavras, há uma relação de poder que tem por finalidade conhecer e moldar o comportamento humano em prol das finalidades e objetivos alheios, a partir dos *superávits* comportamentais. O objetivo final do capitalismo de vigilância é de chegar a previsões que tenham desdobramentos também no mundo *off-line*, sendo possível a orientação de comportamentos do usuário, de forma velada (ZUBOFF, 2020, p. 132).

Nesse contexto, Zuboff (2020, p. 113) alerta para o fato de que as *Big Techs*, encontraram uma forma de não só monitorar o comportamento humano online, mas manipulá-lo, na medida em que os dados são utilizados para produzir desejos aos usuários

(MONTEAGUDO, 2021, p. 1731). O *superávit* comportamental tornou possível, não só satisfazer demandas, mas também criar demandas aos usuários.

Alinhado a isso, ao se estudar as relações de poder e controle sobre as pessoas na história da humanidade, ganham destaque os estudos do filósofo francês Michel Foucault (2008; 1999; 1995; 2014) que se dedicou a estruturar uma “análise do poder” e a compreender como o poder é concebido, quais seus mecanismos, efeitos e as relações dos dispositivos de poder na dinâmica social. Em suas pesquisas, Foucault (2008) indicou a existência de três modos de funcionamento do poder com estratégias distintas: os mecanismos de soberania (baseados no sistema jurídico), os mecanismos disciplinares (baseados em estratégias de vigilância e correção dos indivíduos) e os dispositivos de segurança ou de governamentalidade (baseados em cálculos de probabilidade e em levantamentos estatísticos visando regular uma população).

No final dos anos 1970, o filósofo francês passou a estudar as relações de poder nos termos de práticas de governo, e delineou o processo chamado de *governamentalidade*, uma forma emergente de governo que acompanhou o surgimento do Estado moderno e está ligado ao desenvolvimento do aparelho administrativo e de um conjunto de análises e saberes sobre a arte de governar (FOUCAULT, 2008). A governamentalidade foucaultiana faz uma dupla referência às ideias de governo e mentalidade; racionalidade governamental (*gouverne/mentalité*) (ALVES, 2019, p. 6). Trata-se de uma racionalidade sistematizada que vai além de um exercício espontâneo de um poder específico, mas opera por mecanismos dispersos de poder.

Nos termos propostos por Foucault (2008, 1995), o governo visa o direcionamento de condutas de indivíduos ou grupos, ou seja, o direcionamento dos comportamentos por meio de incitação, indução, sedução, constrangimento e proibição sobre as ações dos outros de modo mais ou menos calculado, no sentido de estruturar o campo da ação possível, visando fins específicos. Assim, o exercício do poder consiste em “conduzir condutas” e em ordenar a probabilidade.

Ainda na década de 1990, diversos autores passaram a estudar as reflexões de Foucault (2008) sobre a governamentalidade, dentre os quais se destaca Antoinette Rouvroy (2015), pesquisadora do Direito do Centro de Pesquisa sobre Informação, Direito e Sociedade na Universidade de Namur, na Bélgica. A autora estuda reflexões filosóficas, políticas e jurídicas

relacionadas ao fenômeno da digitalização e da automação do mundo e dedicou-se a analisar a ascensão de um novo tipo de governamentalidade, que se apoia na otimização algorítmica dos comportamentos, das relações sociais e da própria vida dos indivíduos: a “governamentalidade algorítmica”.

A governamentalidade algorítmica pode ser definida como um tipo de racionalidade governamental que se baseia na “coleta, agregação e análise automatizada de dados em quantidade massiva de modo a modelizar, antecipar e afetar, por antecipação, os comportamentos possíveis” (ROUVROY; BERNS, 2015, p. 42). Trata-se de uma nova estratégia de governo, de direcionamento de condutas, que se vale do uso das novas tecnologias, principalmente dos algoritmos (ALVES, 2019, p. 8).

Essa nova forma de governo não se baseia em leis ou procedimentos disciplinares de normalização, mas nos inúmeros rastros comportamentais individuais dispersos no espaço digital e em códigos algorítmicos, isto é, regras técnicas, instruções em linguagem computacional que estabelecem o que pode ou não ser feito no ambiente digital (LESSIG, 2006). O algoritmo “é um conjunto de instruções matemáticas, uma sequência de tarefas para alcançar um resultado esperado em um tempo limitado” (KAUFMAN, 2018). Trata-se de um conjunto de instruções descritas por meio de uma linguagem de programação utilizado nas mídias sociais, nos sites de buscas e serviços de *streaming* – como Google, Facebook, Instagram e Netflix - de forma implícita, sem que os sujeitos que utilizam estes acessos tenham plena consciência das operações algorítmicas que a eles subjazem (ALVES, 2019, p. 8).

Alves (2019, p. 12) explica que essa nova forma de governo pautada na vigilância e nos algoritmos se alimenta de dados individuais em princípio insignificantes - rastros digitais ou dados de não mercado - para criar modelos de comportamento ou perfis supraindividuais sem jamais convocar o sujeito a dar-se conta por si mesmo daquilo que ele é ou daquilo que poderia tornar-se (ROUVROY; BERNS, 2015, p. 42; ROUVROY; STIEGLER, 2015, p. 122). Assim, o atual exercício do poder pretende dirigir condutas futuras, de forma a governar ou domesticar a incerteza (ALVES; ANDRADE, 2022, p. 1015).

Alinhada à tese do capitalismo de vigilância, é possível refletir sobre as ameaças e tensões causadas à liberdade e autonomia humana. Isso porque essas perspectivas teóricas conduzem a horizontes de potencial manipulação dos usuários, do seu sentir, pensar e agir

(FISCHER, 2022, p. 329). Isso se tornaria possível por meio de tecnologias de informação de vigilância que utilizam de dados comportamentais dos usuários para formulação do *big data* e, com o auxílio de sistemas de inteligência, produzir inferência sobre as pessoas, o que teoricamente tornaria possível a manipulação dos usuários das mídias sociais (ZUBOFF, 2020). Neste contexto, quanto mais previsível for atividade do usuário em determinada plataforma digital, maior a chance de lhe ser oferecida uma opção que irá orientá-lo a determinado comportamento, sem que isso seja sequer percebido.

Esse mecanismo de poder é efficientíssimo na sociedade pós-moderna, pois são os próprios usuários, por meio da disponibilização de cada vez mais dados pessoais, que o sustentam. E, quanto mais dados são disponibilizados, mais as pessoas se tornam transparentes para os algoritmos, sendo por eles conhecidas nos mínimos detalhes. Logo, cada vez mais os algoritmos estarão mais próximos de antecipar condutas, oferecer serviços, direcionar ações e produzir desejos, de forma mais sofisticada e imperceptível.

Segundo Alves (2019, p. 13), a antiga imagem de navegação na internet, “que remetia a uma espécie de aventura no oceano aberto da informação, deve ser substituída por outra imagem, a de uma excursão guiada e controlada em um lago artificialmente produzido.” Sem perceber, a liberdade é subjugada; o sujeito é objetificado e não livre. Para Alves e Andrade (2022, p. 1018), as correlações e predições ensejadas na governamentalidade algorítmica causam a redução das subjetividades, o que ameaça a própria base da autonomia e da liberdade humanas, pois, sem que o indivíduo sequer perceba, seu comportamento pode ser, sutilmente, modelado por operações algorítmicas.

Couldry e Mejias (2019, p. 14) ao analisarem o “colonialismo de dados³” – que tornou a vida humana um objeto de monitoramento e vigilância contínuos em prol do capitalismo –, argumentam que o processo de extração de dados pode dismantlar a integridade mínima do “eu”, atingindo a autonomia e liberdade humana. Os autores defendem que, no colonialismo de

³ O colonialismo de dados é definido pelos autores como um fenômeno de extração sistemática de dados da experiência humana por ferramentas digitais para a geração de lucro. É a tentativa sistemática de transformar todas as vidas e relações humanas em insumos para geração de lucro. Em outras palavras, o colonialismo de dados é uma ordem emergente para a apropriação da vida humana por meio de dados extraídos por ferramentas digitais, para fins lucrativos. O resultado é minar a autonomia da vida humana de uma forma fundamental que ameaça a própria base da liberdade, que é exatamente o valor que os defensores do capitalismo exaltam (COULDRY; MEJIAS, 2019, p. 10, 14).

dados, há um espaço de tensão da liberdade em razão do controle e moderação de conteúdos, e pelo uso de conteúdos direcionados que influenciam emocionalmente as pessoas. Nesse contexto, o poder de coletar e manter dados em grande escala tem impactos sobre a capacidade dos indivíduos de pensarem em si mesmos como atores livres (COULDRY; MEJIAS, 2019, p. 163-165).

A liberdade é tutelada pelo direito geral de liberdade. Trata-se de um direito subjetivo fundamental que resguarda a esfera de liberdade pessoal que não deve sofrer interferências de terceiros e na qual o indivíduo pode desenvolver, livremente, sem intromissão, intervenção ou coação, suas faculdades e vontades naturais (MARTINS, 2018, p. 440). O bem protegido pelo direito à liberdade corresponde à manutenção de uma “indiscriminada ausência de obstáculos ao exercício de sua atividade, apta a satisfazer aquilo que, na linguagem corrente, pode chamar-se a necessidade de fazer o que melhor lhe parece e lhe agradar” (DE CUPIS, 2008, p. 104).

Nesse direito de liberdade localizam-se os dois sentidos de liberdade: liberdade positiva e liberdade negativa, para garantir um grau cada vez maior de realização pessoal da pessoa humana e o desenvolvimento de sua personalidade. Assim, não basta ter a ausência de impedimentos se a pessoa não possui as condições ou possibilidades para se autodeterminar e ter condutas autônomas. Logo, um sentido caminha *pari passu* ao outro.

Esse direito geral de liberdade é um direito de personalidade e, portanto, essencial ao livre desenvolvimento da personalidade humana. Ensina De Cupis (2008, p. 24) que os direitos de personalidade são aqueles sem os quais a personalidade humana estaria completamente irrealizada, privada de todo o valor concreto, constituem a medula da personalidade. Nesse contexto, a liberdade é um direito sem o qual a pessoa e sua dignidade não se realizam. E nessa liberdade encontra-se tanto o agir sem impedimentos como o agir autonomamente, que se interrelacionam, efetivam o desenvolvimento da personalidade e a vida digna. Inclusive, Capelo de Sousa (2011, p. 256), afirma que a “proteção jus-civilística do bem da liberdade humana decorre diretamente da tutela geral da personalidade”.

É possível concluir, então, que há um panorama teórico que visualiza ameaças à liberdade e autonomia por meio da manipulação *on-line* dos usuários. Diante deste cenário e para responder ao problema de pesquisa, na próxima seção, utiliza a técnica de revisão sistemática para analisar a literatura estrangeira a fim de identificar em que medida a

manipulação on-line tem sido visualizada nessa literatura e as discussões que têm sido realizadas em torno dessa temática. Espera-se, com a revisão, encontrar fundamentos empíricos que confirmem ou não a hipótese que tem sido formulada em discussões teóricas, isto é, de que existe um cenário de possível violação à liberdade e autonomia humanas.

2 ANÁLISE DOS RESULTADOS NA REVISÃO SISTEMÁTICA DA LITERATURA SOBRE *BIG DATA* E MANIPULAÇÃO *ON-LINE*

A pesquisa de revisão sistemática da literatura foi realizada na base de dados *Web of Science* - Coleção Principal (Clarivate Analytics)⁴. Foram utilizadas, como descritores, as seguintes palavras-chaves: “*big data*” AND “*behavioral manipulation*” OR “*on-line manipulation*” sem restrição de tempo, e obteve-se 44 (quarenta e quatro) artigos como resultados. Deste total, 2 (dois) artigos foram descartados por não ser possível encontrá-los on-line, e 26 (vinte e seis) artigos foram descartados por não abordarem especificamente a manipulação *on-line* de comportamento de usuários, mas abordaram outros temas não necessariamente ligados à tecnologia, como: linguagem (2), neurociência (6), medicina (3), engenharia (4), robótica (2), eletrônica (2), mecatrônica (2), informática (4).

Considerando que a metodologia de pesquisa empregada nesta investigação é a hipotética-dedutiva, os resultados da revisão sistemática serão utilizados para testar a hipótese inicialmente lançada, isto é, de que há um contexto de manipulação *on-line* dos comportamentos que acarreta tensões ao direito de personalidade à liberdade e autonomia humana, que também se espalha para o mundo *off-line*.

Pela revisão sistemática da literatura foi possível visualizar que o debate sobre manipulação das pessoas já era tema de estudos na área do *marketing* comportamental. Segundo Spencer (2020, p. 963), há várias décadas os pesquisadores de *marketing* visualizavam que os consumidores eram susceptíveis de manipulação pelos fabricantes devido às suas vulnerabilidades cognitivas na tomada de decisão. Segundo explica o autor, o campo da

⁴ As buscas foram realizadas entre os dias 1, 2 e 3 de dezembro de 2022 e as análises ao longo do mês de dezembro de 2022.

economia comportamental identificou muitas razões pelas quais as pessoas decidiam de forma equivocada ou de forma ineficazes, e passou a explorar essas razões.

Exemplificando, Kahneman e Tversky são citados por Spencer (2020) por serem considerados os fundadores da economia comportamental, especialmente pela obra “Rápido e Devagar - Duas Formas de Pensar” em que explicam os dois sistemas de tomada de decisão predominantes: o sistema 1, um modo de pensar rápido, automático e amplamente inconsciente, eficiente e que requer pouca energia ou atenção, mas é vulnerável a preconceitos, vieses e erros sistemáticos; e o sistema 2, um modo de pensar lento, trabalhoso e controlado, que requer mais energia e atenção, mas, uma vez engajado, pode mitigar as vulnerabilidades do sistema 1. Segundo Kahneman, citado por Spencer (2020), o sistema 2 é mobilizado apenas em situações em que o sistema 1 não consegue lidar. E nesse contexto, os manipuladores podem influenciar a decisão de um sujeito explorando vieses cognitivos (tema abordado à frente) que contornam o sistema 2 e desencadeiam uma ação rápida do sistema 1 (SPENCER, 2020).

Spencer (2020) e Susser (2019) descrevem que as pesquisas em psicologia cognitiva e social e economia comportamental revelam mecanismos que ajudam a explicar como as pessoas formam julgamentos e tomam decisões. Malgieri (2021), menciona que há pesquisas⁵ que indicam que a capacidade racional individual não é mais o elemento principal da tomada de decisão humana, mesmo em contextos puramente “autônomos”, e que outros elementos relevantes desempenham um papel fundamental na tomada de decisão, como a atenção, a memória e as emoções.

Esses mecanismos recebem diversos nomes, como heurística, padrões de comportamento, vieses cognitivos, dentre outros. Susser et al. (2018; 2019, p. 6, nota 17) afirmam que os vieses seriam atalhos mentais não confiáveis usados na tomada de decisão cotidiana e que as pessoas são suscetíveis a muitos tipos de vieses cognitivos e nem todas são suscetíveis aos mesmos vieses no mesmo grau. Ademais, apresentam estudos empíricos que sugerem que as diferenças individuais na personalidade, cultura e humor (entre outros), podem modular como os indivíduos são afetados pelos vieses. Para Spencer (2020, p. 963) esses vieses ajudam a explicar por que as pessoas costumam tomar decisões de maneiras que fogem de um modelo idealizado de tomada de decisão racional.

⁵ Indica-se a leitura de KRAMER, et al., 2014 e CLIFFORD, 2017, citados por MALGIERI, 2021.

A discussão sobre os vieses cognitivos encontra-se relacionada ao tema da manipulação, na medida em que ela busca explorar as vulnerabilidades humanas para induzir certos comportamentos. E essas vulnerabilidades são encontradas nos vieses. Spencer (2020, p. 963) evidencia que tanto o *marketing* como a economia comportamental já debatem essas questões no âmbito da manipulação de comportamentos há alguns anos. Acontece que as novas tecnologias têm conduzido as possibilidades de manipulação a novos patamares.

Em 1967, Westin (2015, p. 331) já alertava sobre “toda a gama de dispositivos, técnicas e substâncias futuras que entra[riam] na mente para implantar influências ou extrair dados”. Dellarocas (2006, p. 1577), há mais de dez anos, sinalizou que os fóruns de opinião na Internet representavam tentativas de manipulação da percepção do consumidor sobre determinados produtos ou serviços, antes de tomar uma variedade de decisões de compras; e que os fóruns desempenham um papel cada vez mais importante na formação da opinião pública (DELLAROCAS, 2006, p. 1578).

Essa é a perspectiva que se visualiza na construção teórica da primeira seção, porém, de forma mais sofisticada. Para Susser, et al. (2019, p. 2), nos últimos anos, o escopo dessas preocupações se expandiu em razão das descobertas sobre o uso da tecnologia da informação capaz de influenciar não apenas a esfera comercial, mas representar uma ameaça em outros setores, em nível macro e micro. Os autores ainda afirmam que as interações entre seres humanos e tecnologias inteligentes apontam para um cenário de manipulação com consequências drásticas para o bem-estar e a autonomia. E embora reconheçam que as práticas de manipulação possam direcionar o comportamento do usuário para escolhas que lhe ofereçam vantagens como facilidade de uso, serviços gratuitos e gratificação imediata, defendem a existência de impactos adversos no bem-estar individual e coletivo que minam a autonomia individual (SUSSER, et al., 2019).

Em semelhança, Spencer (2020, p. 961), apesar de focar sobre a manipulação *on-line* comercial, alerta que ela não se limita a atores comerciais, e que, com o surgimento de novas tecnologias pautadas no *big data*, poderá incidir em outras áreas. Assim, afirma que a era digital, com as tecnologias de coleta e técnicas de tratamento de dados e sistemas inteligentes conduziram as potencialidades de manipulação *on-line* a novos níveis, na medida em que tornou cada vez mais possível identificar as vulnerabilidades individuais dos usuários (tal como os

vieses) e adaptar o conteúdo para explorar essas vulnerabilidades, e até mesmo *criar* vulnerabilidades em assuntos individuais e, então, explorá-las (SPENCER, 2020, p. 966, 983).

Diante desta consideração, não é difícil imaginar ferramentas digitais detectando vulnerabilidades cognitivas e as plataformas aproveitando-as para estruturar intervenções específicas sobre os usuários (SUSSER, et al., 2019, p. 6). Também, Spencer (2020, p. 977) afirma ser possível que as plataformas e profissionais de *marketing* consigam adaptar seus conteúdos para melhor explorar os vieses e vulnerabilidades de cada usuário individualmente considerado.

Estas práticas podem influenciar, por exemplo, decisões de compras, induzir as pessoas a passarem mais tempo em determinada mídia social para intensificar a coleta de dados e induzir os usuários a aceitar recursos invasivos da privacidade, ameaçando o direito à proteção de dados pessoais e autodeterminação informacional. Além de prejudicar as proteções legais à pessoa no espaço digital, a manipulação *on-line* também priva os indivíduos, de forma inconsciente, de sua capacidade para tomada de decisão independente (BONGARD-BLANCHY, 2021, p. 763).

Nesse sentido, Klenk (2022, p. 86) afirma já existirem tecnologias comportamentais projetadas para mudar ou apoiar mudanças no comportamento humano. E essas tecnologias levantam questionamentos éticos sobre a legitimidade do tipo de influência que exercem sobre os usuários, especialmente em razão dos custos baixos para implantação, ampla disponibilidade e o potencial para otimizar os meios de influência pela aprendizagem de dados.

Segundo o mesmo autor, nos últimos anos, parece haver maior preocupação com a manipulação por tecnologias *on-line*, em particular devido ao advento de novas vulnerabilidades e hierarquias de poder que influenciam de forma oculta e sutil as pessoas (KLENK, 2022, p. 91). Sobre isso, Bongard-Blanchy et al. (2021) elucidam que essas tecnologias e as plataformas que as utilizam, são dotadas de “práticas manipulativas”, disseminadas em razão do baixo custo para implementação, em larga escala. Elas atuam com sofisticação, sem precedentes e com alta eficácia em ambientes dinâmicos, interativos, intrusivos e adaptativos. Frischmann e Selinger (2018) enfatizam que isso acontece sutilmente com o auxílio de tecnologias e práticas de vigilância onipresentes.

Para Klenk (2022, p. 101), o problema ético com a manipulação por meio de tecnologias não é que a tecnologia ofereça um potencial ainda maior de influência oculta (embora isso

também possa ser verdade, para os mais vulneráveis). O problema é que muitas dessas influências podem não revelar seus motivos aos usuários. Essas influências podem ser qualificadas como manipuladoras e não aumentariam a capacidade das pessoas de agir de maneira responsiva à razão. E nesse sentido, o autor menciona que há pesquisadores que defendem que essas interações são manipulativas (KLENK, 2022).

Exemplificando, para Richards (2013), aquele que sabe ou infere sobre as preferências, interesses e hábitos de uma pessoa, seus amigos e conhecidos, educação, emprego, saúde, posição financeira etc, encontra-se em uma posição de exercício de considerável influência sobre essa pessoa. Essa influência é descrita pelo autor como “persuasão” ou “formas sutis de controle” (RICHARDS, 2013). Susser et. al. (2019, p. 2), entendem que essas formas de influência devem ser identificadas como formas de “manipulação”. No mesmo sentido, Bongard-Blanchy et al. (2021, p. 763), apontam que os pesquisadores têm se atentado para essas práticas manipulativas com o objetivo de denunciar esta realidade e elaborar possíveis soluções.

Visualiza-se, então, que diversos autores debatem sobre a manipulação *on-line*, pela Internet, que teria nas mídias sociais em casos de manipulação da opinião pública quanto às eleições presidenciais de 2016 nos Estados Unidos; cenário que agrava ao se considerar que as mídias sociais foram (e são) cada vez mais difundidas e desde então fazem parte da vivência social das pessoas (PENNEKAMP, et al., 2019, p. 197). Essa é a preocupação de Menczer (2020) ao descrever que, à medida que as mídias sociais se tornaram os principais canais de difusão de notícias e informações, tornou-se fundamental entender como a complexa interação entre vieses cognitivos, sociais e algorítmicos, desencadeados pela dependência das mídias sociais, tornou as pessoas mais vulneráveis à manipulação *on-line*.

Os textos analisados procuraram definir a manipulação *on-line*. Susser et al. (2019, p. 6) definiram a manipulação *on-line* como aquela facilitada pela tecnologia da informação para influenciar secretamente a tomada de decisão de outra pessoa, para a exploração de vulnerabilidades na tomada de decisão. Nessa definição tem destaque a ideia de que a manipulação é oculta, isto é, o estímulo manipulativo ou o mecanismo manipulativo age secretamente e que se explora vulnerabilidades. Fischer (2022, p. 334-335), por outro lado, aduz que tanto a influência secreta quanto o engano não seriam condições necessárias para a manipulação *on-line*, mas sim fatores que podem amplificá-la.

Já Spencer (2020, p. 960, 989), define a manipulação como uma tentativa intencional de influenciar o comportamento de um sujeito e contornar o processo de tomada de decisão racional do sujeito pela exploração de um viés ou vulnerabilidade. O autor enfoca na intencionalidade e exploração de vulnerabilidade, mas não indica atuação secreta como um elemento⁶.

Malgieri (2021), ao contrário dos demais, sustentou que uma definição única para manipulação *on-line* é inviável e contraproducente tendo em vista o avanço veloz das tecnologias. Por isso, devem ser identificados apenas elementos chaves das práticas manipulativas tecnológicas. Como exemplo, citou a declaração sobre capacidades manipulativas de processos algorítmicos do Conselho da Europa que mencionou algumas características da manipulação algorítmica, como: a capacidade de usar dados pessoais e não pessoais para classificar e micro alvo de pessoas; de identificar vulnerabilidades individuais e explorar conhecimento preditivo preciso; e de reconfigurar ambientes sociais para atender a objetivos específicos e interesses escusos (COUNCIL OF EUROPE, 2019; MALGIERI, 2021).

Para Malgieri (2021), a manipulação *on-line* por meio de tecnologias contaria com as seguintes características: práticas personalizadas com base em dados (pessoais) previamente coletados; processos dinâmicos baseados em feedback contínuo; mecanismos ocultos ou não transparentes; e ferramentas avançadas de análise de dados (técnicas de mineração de dados, análise preditiva/prescritiva etc.). Esses elementos estariam intrinsecamente conectados na medida em que as práticas personalizadas se baseiam nos dados coletados por meio de ferramentas algorítmicas avançadas não transparentes que fornecem *feedback* contínuo sobre a eficácia de tais práticas, e que são continuamente ajustadas e aprimoradas (MALGIERI, 2021).

⁶ Spencer (2020) cita dois casos que evidenciam a capacidade de manipulação online. O primeiro trata-se do relatório elaborado por executivos do Facebook e descrevia como descrevia como a rede social reunia informações psicológicas sobre jovens australianos e neozelandeses, e afirmava que a rede social conseguia monitorar postagens e fotos em tempo real dos jovens e detectar emoções dos jovens. Segundo o relatório, o Facebook tem informações detalhadas sobre as mudanças de humor dos usuários jovens com base em “dados internos do Facebook” que não estão disponíveis ao público (LEVIN, 2017). O outro caso citado foi o da Cambridge Analytica, empresa de mineração e análise de dados que atuava estrategicamente no processo eleitoral norte americano. Em 2016 ela utilizou, sem o consentimento dos usuários, dados milhões de perfis do Facebook que foram coletados de testes de personalidades (“*thisisyourdigitallife*”). Esses dados foram correlacionados com outros perfis e foram criados perfis psicográficos, o que tornou possível fazer predições em larga escala quanto aos resultados das eleições norte-americanas, e por consequência realizar o direcionamento de propagandas políticas aos eleitores indecisos (BRUNO, 2018).

Em síntese são elementos-chave para delinear a manipulação: personalização, capacidades tecnológicas e adaptabilidade dinâmica, e exploração de vulnerabilidades individuais.

Java et al. (2022, p. 593, 595) denominam essa manipulação como *hacking* cognitivo, na medida em que se trata de uma forma caracterizada de influência que não se pauta na persuasão racional e nem coerção, mas é capaz de alterar a percepção, o comportamento e as emoções da pessoa, em nível amplo e coletivo. Afirmam os autores que, no caso do espaço *on-line*, o caráter aberto da internet e a facilidade que os conteúdos são compartilhados nas redes sociais, facilita a ocorrência de manipulações, sem o conhecimento de seus usuários, por meio de influência sob a cognição, opiniões, emoções e perspectivas (JAVA; et al., 2022, p. 593).

Susser et. al. (2019, p. 6) desenvolvem as condições que tornam possível a manipulação *on-line*. O primeiro deles seria a vigilância digital generalizada - tal como desenvolvido por Zuboff (2020) na tese do capitalismo de vigilância - que coloca as vulnerabilidades de tomada de decisão em exibição permanente e as torna fáceis de detectar, na medida em que quase tudo o que se faz hoje, digitalmente, deixa rastros em perfis extremamente detalhados. Além da vigilância que torna as vulnerabilidades de tomada de decisão fáceis de detectar e das plataformas digitais que as tornam fáceis de explorar, as tecnologias se tornaram invisíveis para os usuários devido ao uso frequente e habituação (SUSSER, et al., 2019, p. 7). Esses fatores, alinhados, possibilitam a manipulação *on-line* dos usuários.

Alinhado aos estudos dos vieses cognitivos e de vulnerabilidades, Malgieri (2021) alerta que a construção de perfis psicométricos tem possibilitado a exploração das limitações cognitivas inatas humanas por serviços *on-line* para direcionar os usuários para escolhas das quais podem se arrepender. E, também, em virtude da estrutura dinâmica e interativa, as plataformas digitais são capazes de se adaptar a cada usuário individual, e criar ambientes de escolha personalizados, isto é, contextos de tomada de decisão nos quais as vulnerabilidades catalogadas por meio de vigilância digital são colocadas em funcionamento em um esforço para influenciar as escolhas das pessoas (YEUNG, 2017, p. 122).

Diante destas considerações, os textos localizados indicam que o primeiro passo em direção à manipulação *on-line* tem início na coleta e tratamento de dados pessoais e em seguida, perfilização e personalização. Sobre isso, Peters (2022) analisa o rastreamento algorítmico das “pegadas digitais”, isto é, dados dos usuários como histórico de navegação e pesquisa, cliques,

tempo de visita ao site, perfis pessoais, curtidas nas mídias sociais e assim por diante. Esses dados são coletados pelas plataformas como Google Amazon, Facebook, e por meio de sistemas de inteligência artificial (IA) como algoritmos de aprendizado de máquina são identificados padrões neles para inferir as preferências, interesses e objetivos desses mesmos usuários. Esse processo é denominado de rastreamento algorítmico e existem dois tipos de rastreamento algorítmico envolvidos no processo de monitoramento dos rastros digitais: o rastreamento algorítmico simples e o rastreamento psicométrico (PETERS, 2022, p. 267, 269).

Segundo Peters (2022, p. 269-270), o rastreamento simples é aquele que se baseia em sistemas de recomendação - como utilizado pela Amazon e Netflix - para produzir sugestões de conteúdos que um usuário pode querer comprar, assistir ou ler. Comumente estão envolvidos o (1) rastreio de outras atividades do usuário (compras anteriores, avaliações, itens visualizados ou cliques no site), (2) construção de um modelo do usuário com base no rastreio e (3) procura de grupos de outros usuários do site a que as atividades se sobrepõem. Em seguida, os algoritmos (4) agregam itens de usuários semelhantes, (5) excluem itens que o usuário individual já comprou, avaliou ou visualizou e (6) recomenda os restantes (PETERS, 2022, p. 269).

Esse processo é considerado simples porque os algoritmos vinculam determinados perfis de usuário a recomendações expressas que não necessariamente representam os itens de preferência dos usuários. Os algoritmos apenas preveem que, com base no comportamento *on-line* anterior, determinados usuários do site provavelmente terão outros tipos de comportamentos *on-line* que os algoritmos foram projetados para maximizar. Trata-se de uma probabilidade, a partir dos conteúdos com que o usuário interagiu, e não há uma categorização explícita de pessoas em termos de aspectos de sua personalidade, preferências ou interesse e estado mental (PETERS, 2022).

Existem tipos mais sofisticados de rastreamento algorítmico, como o utilizado pelo Facebook no *feed* de notícias de cada usuário que é individualizado para destacar o conteúdo que o mantém mais envolvido e engajado (PETERS, 2022). Isso é possível com base nos variados dados de comportamento *on-line* coletados (curtidas dos usuários, perfis visitados, com quem interage, o que especificam sobre si mesmos em seus perfis etc.). Alguns desses cálculos envolvem rastreamento psicométrico, ou seja, processamento no qual os sistemas de

IA medem e atribuem explicitamente aos usuários do site recursos psicológicos, incluindo traços de personalidade com base em seu comportamento *on-line* ou outros dados do usuário⁷ (PETERS, 2022, p. 269). Esse rastreamento psicométrico tem sido empregado por, por exemplo, empresas de mídia social e firmas de consultoria para segmentar os usuários do site em grupos de personalidade para publicidade e mensagens personalizadas (PETERS, 2022, p. 269).

A perfilização seria então uma segunda etapa. As plataformas de mídias sociais utilizam os dados dos usuários coletados muitas vezes sem consentimento, para desenvolver estruturas de perfis psicográficos individuais e classificar os usuários em categorias específicas (JAVA, et al., 2022, p. 594-595). Büchi et al. (2019, p. 2) definem o perfil como o registro e classificação sistemáticos e propositais de dados relacionados ao indivíduo, a partir de um processo de mineração (HILDEBRANDT, 2018) e explicam que a era digital transformou a criação de perfis em perfis algorítmicos automatizados, e o *big data* permitiu a criação de perfis a partir de fontes de dados muito mais extensas. A preocupação está no fato de que embora os perfis sejam alimentados por dados pessoais fornecidos pelos próprios usuários, as inferências automatizadas extraídas desses dados, podem se desviar das possíveis inferências imaginadas pelo usuário que forneceu seus dados (BÜCHI, et al., 2019, p. 3).

A perfilização tem por objetivo final a adaptação e personalização de conteúdo para manter os usuários cada vez mais engajados. Pela personalização de conteúdos, busca-se atingir efetivamente o usuário com informações e anúncios personalizados, contornando a tomada de decisão racional por meio de estratégias que se utilizem das inferências e das vulnerabilidades. E essa situação entende-se resultar na violação da liberdade, ao explorar o comportamento do usuário e inconsciente (JAVA, et al., 2022, p. 594-595).

Peters (2022) explica que muitos pesquisadores⁸ defendem que a partir do rastreamento algorítmico, os sistemas de computador são capazes de fazer inferências psicológicas,

⁷ Youyou, Kosinski e Stillwell (2015) coletaram dados de curtidas dos perfis do Facebook de mais de 86.000 voluntários. Esses perfis foram obtidos com pesquisas que capturaram as atitudes políticas dos entrevistados e os traços de personalidade. Um sistema de *machine learning* foi utilizado para treinar o algoritmo para encontrar padrões nos dados e conectar com precisão as curtidas dos indivíduos no Facebook com as pontuações de personalidade. Após, quando analisou outras curtidas de outros usuários, o algoritmo pôde prever muitas das características psicológicas dos usuários com mais precisão do que até mesmo cônjuges desses indivíduos.

⁸ Peters (2022) cita as pesquisas de YOUYOU; KOSINSKI; STILLWELL, 2015, ZANKER; ROOK; JANNACH, 2019 e BURR; CRISTIANNI, 2019.

julgamentos e suposições sobre os objetivos, interesses e preferências dos indivíduos. Essas inferências sobre indivíduos ou grupos são feitas com base nos perfis, e podem abranger previsões sobre ações ou inações futuras, características gerais e preferências específicas (BÜCHI, et al., 2019, p. 3).

Segundo Peters (2022), ao inferirem e predizer algumas informações pertencentes a construções psicológicas (estados mentais) de usuários individuais, com base na amostra do comportamento observável do sujeito, seria como se os sistemas pudessem “ler as mentes” dos usuários. Os algoritmos podem descobrir, incentivar, moldar ou até mesmo criar as preferências dos usuários (FRISCHMANN; SELINGER, 2018). Afinal, se eles são capazes de identificar, por exemplo, as preferências atuais dos usuários, também podem influenciar de forma mais eficaz e adequar melhor os conteúdos a eles, por meio da personalização *on-line*. Essa visão do rastreamento algoritmos pode ajudar a conscientizar as pessoas sobre as consequências potencialmente prejudiciais de seu uso da Internet, como a manipulação *on-line*, e contribuir para a reflexão acerca de caminhos para reivindicar a autonomia diante de formas de controle computacional e invasões de privacidade (PETERS, 2022, p. 278).

À vista dessas noções, o texto de Kim (2020, p. 868) explica que a personalização *on-line* é impulsionada por complexos algoritmos de aprendizado de máquina criados para discernir as preferências e antecipar o comportamento dos usuários. Essa personalização de fato oferece benefícios, pois as empresas podem oferecer aos consumidores os produtos e serviços com mais eficiência, mas o perigo encontra-se no fato de que não é todo tipo de inferência que é comunicada aos usuários (BÜCHI, et al., 2019, p. 3). A personalização e as inferências resultantes do processo de rastreamento algorítmico possibilitam práticas manipulativas em grande escala para a manipulação de mercado (SUSSER, et al., 2019), na medida em que empresas privadas aplicam os *insights* da ciência comportamental para manipular os consumidores, explorando suas vulnerabilidades psicológicas ou emocionais, conhecidas pelas inferências (CALO, 2014; ZARSKY, 2019).

Nesse contexto, a personalização e os algoritmos preditivos têm levantado discussões sobre a discriminação, na medida em que são utilizados nos mercados (moradia, emprego)⁹,

⁹ A questão pode ser ilustrada pelas ferramentas de segmentação de anúncios de redes sociais como o Facebook que pode distribuir informações sobre oportunidades de maneira tendenciosa e a apenas determinadas pessoas, ainda que o anunciante use critérios de segmentação neutros e pretenda atingir um público diversificado. Esse,

crédito etc. - que fornecem acesso a recursos essenciais ao desenvolvimento da pessoa humana e o exercício de uma vida digna) para segmentar as pessoas e determinar com precisão quais informações serão entregues a quais usuários. Esses algoritmos podem reproduzir ou reforçar formas históricas de discriminação, pois são construídos a partir dos padrões de comportamento na sociedade (KIM, 2020, p. 869-870). Além disso, no âmbito público e político, têm sido levantadas preocupações sobre a manipulação, com advertências de que a personalização de notícias está criando “bolhas de filtro” e aumentando a polarização, e como as técnicas de vigilância comportamental e micro direcionamento contribuem para danos sociais, como polarização e extremismo (KIM, 2020, p. 869).

A extensa crítica da personalização é motivada especialmente pela preocupação de que a manipulação *on-line* prejudica a autonomia pessoal e compromete a tomada de decisões racionais (KIM, 2020, p. 869). Nessa perspectiva, Java et al. (2022, p. 594) afirmam que as manipulações de indivíduos com a ajuda de estratégias de desinformação, desempenharam um papel vital no declínio da liberdade *on-line* para seus usuários. Assim, os dados que são coletados (etapa um) dos usuários passam por uma metodologia sistemática de agregação, filtragem e organização (etapa dois) para fins de manipulação *on-line*, como anúncios personalizados, alteração de opiniões políticas, fraudes comerciais, vitimização emocional e cognitiva (etapa três) (JAVA; et al., 2022, p. 593).

O ecossistema da Internet fornece uma vantagem aos manipuladores para espalhar notícias falsas, percepções de propaganda e divulgar agendas de interesses específicos, com a ajuda de mídias sociais, memes, *bots* ou *clickbots*, análises e métricas, táticas de desinformação para espalhar preconceito político, discurso de ódio, falso comentário de ativismo e até mesmo tentar influenciar debates de interesse público como saúde, política e eleições e meio ambiente (JAVA, et al., 2022, p. 594). O objetivo é sensacionalizar as notícias e obter cada vez mais cliques que resultarão em mais receita ou lucros, na medida em que os direitos e vulnerabilidades do usuário são explorados (JAVA, et al. 2022).

segundo o autor, é um exemplo de uma preocupação muito mais ampla que diz respeito a uma ameaça à igualdade (KIM 2020, p. 871). Segundo Kim (2020, p. 873) essas tecnologias moldam como os participantes do mercado (trabalhadores e empregadores) percebem suas opções disponíveis e, portanto, também influenciam seu comportamento.

Além da personalização, Bongard-Blanchy et al. (2021) chamam a atenção para o domínio do design de interface/experiência do usuário e as estratégias de design das plataformas que têm sido utilizadas para explorar vulnerabilidades de tomada de decisão dos usuários para induzi-los a agir contra seus interesses (SUSSER, et al. 2019, p. 7). Os autores discutem a manipulação *on-line* a partir dos padrões obscuros ou *dark patterns*, isto é, escolhas de design que beneficiam um serviço *on-line* por meio da coação, direcionamento ou engano dos usuários para tomarem decisões que, se totalmente informados e capazes de selecionar alternativas, provavelmente eles não tomariam (BONGARD-BLANCHY, et al., 2021, p. 763).

As possibilidades de implementações de *dark patterns* é ampla e pode variar desde *designs* coercitivos que restringem as opções do usuário, à mecanismos de incentivos (*nudges*) que sutilmente usam da proeminência visual de uma escolha em detrimento de outra (BONGARD-BLANCHY, et al., 2021, p. 765). Os *dark patterns* são efetivos porque exploram vieses cognitivos e a racionalidade humana limitada. Exemplificando, alguns exemplos de práticas de *dark patterns*, são: mensagem de alta demanda, mensagem de tempo limitado, pré-seleção de informações, hierarquia falsa, informações ocultas, reprodução automática, consentimento agrupado, consentimento forçado, *confirmshaming*, mensagem de perda-ganho e pergunta capciosa (BONGARD-BLANCHY, et al., 2021, p. 768).

Bongard-Blanchy et al. (2021, p. 763), por meio de uma pesquisa empírica, analisaram a conscientização e a falta de consciência ou preocupação dos usuários quanto aos *dark patterns*; a (in)capacidade dos usuários de reconhecê-los; e a (in)capacidade dos usuários de resisti-los. Os autores identificaram que os usuários são capazes de reconhecer alguns dos padrões obscuros capazes de influenciar suas escolhas e comportamentos e reconheceram que esses padrões podem moldar o comportamento de gastos, consumo de conteúdos e escolha de serviços, principalmente por meio de conteúdos e recomendações personalizados e ofertas especiais. Inclusive, os respondentes associaram os *dark patterns* às plataformas como Amazon, Netflix, Facebook, Instagram, eBay, Twitter e Youtube. Mas, não conseguiram visualizar como esses padrões poderiam prejudicá-los concretamente (BONGARD-BLANCHY, et al., 2021, p. 764, 768-769).

Quanto aos danos, alguns citaram exemplos específicos de danos como de natureza psicológica (frustração, ansiedade, perda de autoconfiança), física e financeira. inclusive, em

relação aos danos causados pela manipulação *on-line* em geral, especialmente aos danos psíquicos e físicos, Lee, Qiu e Whinston (2015, p. 4864) alertam que plataformas populares são propensas a abuso e manipulação de partes estratégicas, e essas manipulações podem causar consequências terríveis.

Outros mencionaram os perigos relacionados a informações enganosas e pré-filtradas que podem influenciar as opiniões, valores e atitudes das pessoas e causar danos à sociedade como um todo. Suscitaram apreensão quanto aos danos às pessoas vulneráveis, como idosos e crianças. Mas, de um modo geral, mostraram tendência a não se preocuparem em serem manipulados por *designs on-line* (BONGARD-BLANCHY, et al., 2021, p. 768-769). E, aos que consideraram a manipulação por *dark patterns* como um risco, não tinham certeza se poderiam ser prejudicados pessoalmente (BONGARD-BLANCHY, et al., 2021, p. 768-769).

Em outro viés, Dorofeeva et al. (2022, p. 66), analisou a relação entre manipulação *on-line* de adolescentes, vício em Internet e comportamento suicida. Os autores demonstraram que existe uma relação entre a conduta suicida e o vício na internet, que determina o efeito da manipulação *on-line* na intenção suicida dos adolescentes, por meio do envolvimento em comunidades *on-line* de “grupos de morte”, alinhado ao aumento da popularidade das mídias sociais e a dependência da Internet (DOROFEEVA; et al., 2022, p. 66, 70-72).

Bongard-Blanchy et al. (2021) constataram que os mais jovens conseguiram identificar um número maior de padrões escuros que outras gerações; e aqueles com ensino médio ou inferior detectaram menos padrões que participantes com graduação ou formação profissional¹⁰. Em geral, muitos participantes ficaram surpresos por não conseguirem reconhecer certos designs manipulativos, o que indica uma variação entre os tipos de padrões detectáveis (BONGARD-BLANCHY, et al., 2021, p. 769-770). Por fim, os autores mostraram uma pequena correlação inversa entre a capacidade de detecção dos participantes e sua classificação de probabilidade de influência, o que indica que os usuários que reconhecem designs manipulativos com mais facilidade se consideram menos propensos a serem influenciados (BONGARD-BLANCHY, et al., 2021, p. 771).

¹⁰ Mas, segundo os autores, a diferença não foi tão grande como esperada pelos autores, o que sugere que o nível de licenciatura/formação profissional é um limiar abaixo do qual as taxas de reconhecimento são mais baixas (BONGARD-BLANCHY, et al., 2021, p. 769).

Além dos *dark patterns*, há outros mecanismos de manipulação de comportamentos online. Cresci et al. (2021) atentam ao fato de que a manipulação muitas vezes é realizada por meio de *fake news* e *bots* sociais. As notícias falsas estão presentes nos mais diversos contextos como na seara política, em questões de saúde e no mercado financeiro; e se trata de “informações fabricadas que imitam o conteúdo da mídia jornalística na forma, mas não no processo organizacional ou na intenção” (CRESCI; et al., 2021, p. 48). Elas são publicadas em veículos pouco conhecidos e são amplificadas nas postagens nas redes sociais, muitas vezes com o uso de *bots* sociais, que são algoritmos de *software* que imitam o comportamento de uma conta genuína para criar uma ênfase artificial na notícia falsa, de forma maliciosa (CRESCI, et al, 2021, p. 48-49). Pennekamp et al., 2019, p. 197) alertam que as notícias falsas e os *bots* e *trolls*¹¹, acarretam riscos às democracias estabelecidas ao suscitar a manipulação da opinião pública, o que pode ser explorado por governos, organizações e empresas para manipular as opiniões dos usuários a seu favor.

O problema das *fake news* e dos *bots* está relacionado principalmente à dificuldade de detecção. As *fakes news* atuais são mais difíceis de serem detectadas em razão dos modelos de linguagem capazes de gerar parágrafos de texto coerentes e de qualidade. Embora, ainda, a maior parte das *fake news* ainda seja escrita manualmente, à medida que o progresso tecnológico avança para a geração de textos em linguagem natural, a potencialidade de criação de notícias falsas e desinformação com aparência realista crescerá (CRESCI, et al., 2021, p. 49-50). Segundo os autores, os algoritmos de aprendizado têm sido utilizados para detectar notícias falsas, mas esses algoritmos ainda assim podem ser enganados por meio da adição ou remoção de determinadas palavras no texto, adição de comentários falsos¹² (CRESCI, et al., 2021, p. 49).

Os *bots* sociais também se tornaram mais sofisticados e hoje são quase indistinguíveis das contas genuínas, e são utilizados para representar falsamente o envolvimento e engajamento dos usuários em determinados conteúdos nas mídias sociais, até mesmo de conteúdos e notícias falsas (SIGI, et al., 2021, p. 384). A evolução dos *bots* sociais continua, especialmente pelos

¹¹ Os *bots* são usuários artificiais, automatizados, que não existem no espaço *off-line*, enquanto os *trolls* é um usuário real.

¹² Indica-se a leitura do texto de WANG; LEE, 2020, p. 282-291, que consta nas referências de CRESCI; et al., 2021.

avanços em técnicas computacionais que permitem imitar o comportamento humano (CRESCI, et al., 2021, p. 49-50).

Outra perspectiva de manipulação de comportamentos *on-line* é discutida por Malgieri (2021) ao trabalhar o *marketing on-line* ilícito intrusivo como instrumento manipulador de consumidores. No *marketing on-line*, a manipulação comercial é uma realidade crescente e uma ameaça concreta à privacidade no mercado digital (MALGIERI, 2021). Nesse sentido, o Conselho da Europa destacou que as ferramentas contemporâneas de aprendizado de máquina têm capacidade crescente de não só prever escolhas, mas também de “influenciar emoções e pensamentos e alterar um curso de ação antecipado, às vezes de forma subliminar” (COUNCIL OF EUROPE, 2019, p. 2). Malgieri (2021) ressalta o fato de que na sociedade atual, pós-pandêmica, os riscos de manipulação *on-line* se amplificaram na medida em que houve aumento da exposição digital das pessoas (e consumidores), combinado com estados psicoemocionais mais vulneráveis e o aperfeiçoamento das capacidades computacionais na área do *marketing*.

Embora as novas potencialidades tecnológicas tenham aumentado a eficiência das práticas de *marketing* e consolidado serviços digitais aos usuários e consumidores, o autor salienta que as técnicas de *marketing on-line*, especialmente as não transparentes, levantam preocupações quanto à integridade, privacidade e liberdade de escolha do consumidor, na medida em que o *marketing* manipulador pode explorar vulnerabilidades permanentes ou temporárias dos usuários enquanto consumidores, de ordem interna/pessoal e externas. Isso torna-se preocupante se consideradas as noções sobre os vieses cognitivos e perfis psicométricos e o desenvolvimento da tomada de decisão algorítmica que possibilita manipulação, o que repercute significativamente na autonomia dos indivíduos e no direito de agir e tomar decisões independentes (MALGIERI, 2021).

Neste contexto, Malgieri (2021) reflete sobre o *marketing* ilícito à luz do Regulamento Geral sobre a Proteção de Dados da União Europeia, e explica que para considerar um *marketing on-line* lícito, o controlador de dados (no caso, o profissional do *marketing*) deve passar por quatro testes, estabelecidos no Regulamento, que devem ser considerados em um fluxo contínuo: teste de imparcialidade/equidade, teste de legalidade, teste de efeito significativo e teste de alto risco. Apenas se cumprindo as quatro etapas, é que se pode considerar que a conduta do profissional do *marketing* é lícita e cumpre com os direitos dos

titulares de dados. Caso contrário, corre-se o risco de existir manipulação ilícita, logo, *marketing* ilícito e violador do direito à privacidade e a proteção de dados dos titulares/consumidores (MALGIERI, 2021). Embora sua pesquisa enfoque sobre o viés consumerista e na publicidade comportamental para ilustrar a manipulação, a partir da revisão realizada, é possível vislumbrar que estas não sejam as únicas práticas manipulativas (SUSSER, et al. 2019, p. 7).

Sobre a problemática, Lee, Qiu e Whinston (2015, p. 4864, 4872) enfatizam a importância de reconhecer a existência de uma manipulação estratégica realizada por meio da coleta de análise de dados por pesquisadores e profissionais para realizar análises de sentimentos, muitas vezes sem ajustar explicitamente os sentimentos manipulados. E nesse contexto, afirmam que a manipulação *on-line* é resultado da falta de conscientização dos usuários, ausência de mecanismos de verificação, incentivo das plataformas ou da natureza do modelo de negócios escolhido.

Sobre a relação entre manipulação *on-line* e liberdade e autonomia, Klenk (2022, p. 90), explica que a manipulação, assim como a coerção, envolve influência e um certo grau de controle por parte do manipulador, de modo que o manipulado seja direcionado para os objetivos do manipulador. Mas, as pessoas manipuladas ainda agiriam de forma autônoma ou com livre arbítrio, pois haveria uma área de liberdade, ainda que mínima, mesmo que sua agência seja diminuída por causa da influência manipuladora. Se o manipulado deixar de agir voluntariamente, não se trataria de manipulação, mas sim coerção (WOOD, 2014). Por esse sentido, só haveria manipulação quando houver um mínimo de voluntariedade.

Não se concorda com essa concepção. Em semelhança à Klenk (2022, p. 90), entende-se que o comportamento manipulado ainda é um comportamento menos livre, pois a liberdade não se satisfaz apenas com a decisão voluntária. Para ser livre, os dois sentidos de liberdade discutidos (positivo - autonomia; e negativo, de não obstrução, coação ou interferência) devem ser resguardados. Entende-se que a manipulação atinge esses dois sentidos, não existindo uma voluntariedade genuína daquele que é manipulado. Assim, concorda-se com Susser, et al. (2019, p. 3) ao afirmar que quando os dados sobre as pessoas são usados para influenciar a tomada de decisão, eles fazem mais do que diminuir seus interesses. Na verdade, ameaçam a autonomia.

Conclui-se a partir da revisão sistemática realizada que a manipulação *on-line* ameaça o direito de personalidade à liberdade humana, na medida em que prejudica a autonomia por meio da exploração de vulnerabilidades. Além disso, ameaça o direito de personalidade à privacidade, na medida que os dados dos usuários são coletados sem conhecimento e para fins (inferências comportamentais) desconhecidos.

Ademais, quando se discute a manipulação *on-line* na seara pública e os efeitos na disseminação de desinformação, a manipulação prejudica a deliberação e o exercício da liberdade democrática. Diante destas considerações, entende-se que a manipulação prejudica a dignidade da pessoa humana ao tratá-la como sujeito “experimental” e mero meio para um fim.

3 CONCLUSÃO

Esta pesquisa problematizou a ideia de que na contemporaneidade as ferramentas disponíveis para influenciar as decisões das pessoas foram ampliadas por meio das tecnologias. Constatou-se que há fundamentos teóricos de que a era digital acarreta riscos à autonomia humana, existindo um espaço de tensão entre novas tecnologias de processamento de dados e liberdade humana.

Por meio da técnica de revisão sistemática da literatura estrangeira, na base de dados *Web of Science*, constatou-se que a manipulação *on-line* se vale de algumas técnicas, como o rastreamento algorítmico, a perfilização e a personalização de conteúdo. Nesse contexto, constata-se que a manipulação *on-line* usa os próprios dados comportamentais dos usuários contra ele para contornar seu processo racional de tomada de decisão. Os autores analisados vislumbram que surgiram novos mecanismos manipulatórios que tornam possível a manipulação *on-line* dos indivíduos por meio da exploração de suas vulnerabilidades. Além disso, tem destaque na literatura a manipulação por meio do design de interface/experiência do usuário e as estratégias de *dark patterns*, o *marketing on-line* ilícito, as *fakes news* e os *bots* sociais.

Reconhece-se que nem todas essas práticas necessariamente manipulam as pessoas. Mas, a pesquisa evidenciou o grande risco existente, na medida em que muitos usuários de mídias sociais provavelmente não compreendem o funcionamento que embasa essas mídias ou

os riscos que essas estratégias representam à sua liberdade e autonomia. Somando à isso, vislumbra-se, na contemporaneidade, a crescente dependência de ferramentas digitais em todas as áreas da vida – ferramentas que constantemente registram, agregam e analisam informações sobre as pessoas – significa que as pessoas estão revelando cada vez mais sobre suas vulnerabilidades individuais e compartilhadas. Nesse contexto, visualiza-se na pesquisa que as plataformas digitais são cada vez mais capazes de explorar essas vulnerabilidades para estimular e moldar as escolhas na esfera privada ou pública.

Pelas perspectivas analisadas na revisão sistemática, é possível constatar que o *big data* e as tecnologias das mídias instrumentalizam a pessoa humana, ao invés de conceber o reconhecimento daquele indivíduo, estabelecem espaços nos quais se suprime a liberdade do sujeito, subjuga-se sua individualidade pela exploração de suas vulnerabilidades, furta-lhe possibilidades de exercício de sua personalidade, retira-lhe a condição de humano, na medida em que a pessoa é impedida de agir autonomamente e de forma livre.

Por meio do método hipotético-dedutivo e da análise da revisão sistemática realizada, conclui-se confirmando a hipótese inicialmente lançada de que há um contexto de manipulação *on-line* dos comportamentos que acarreta tensões aos direitos de personalidade, como o direito de personalidade à liberdade e a autonomia humana. Ademais, infere-se que essa influência também se espalha para o mundo *off-line* na medida na contemporaneidade os espaços de vivência digital e real se confundem, e digital e real constituem ambientes de formação da personalidade individual e de exercícios de direitos da personalidade. Neste contexto, entende-se necessário refletir, em novas pesquisas, sobre as perspectivas emancipatórias e respostas de regulação à manipulação *on-line* – como a investigação do tema à luz da Lei Geral de Proteção de Dados (LGPD) – para a fim de se efetivar amplamente os direitos da personalidade, em especial, o direito à liberdade humana.

169

REFERÊNCIAS

ALLMER, Thomas. *Towards a critical theory of surveillance in informational capitalism*. Frankfurt: Peter Lang, 2012.

ALVES, Marco Antônio Sousa. A resistência à governamentalidade algorítmica: condutas e contracondutas na era da informação. In MATOS, Andityas Soares de Moura Costa. (Org.)

Ensaio de Desobediência Epistemocrítica: dimensões antagonistas na era das sujeições bio-político-cibernéticas. Série: Desobediências E Democracias Radicais: A potência comum dos direitos que vêm. Belo Horizonte: Initia Via, 2019.

ALVES, Marco Antonio Souza Alves; ANDRADE, Otávio Morato de. Autonomia individual em risco? Governamentalidade algorítmica e a constituição do sujeito. *Cad. Metropole*, São Paulo, v. 24, n. 55, pp. 1007-1023, set./dez. 2022.

BONGARD-BLANCHY, Kerstin; et all. "I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective. *Designing Interactive Systems Conference 2021*, EUA, jun./jul. 2021.

BRUNO, Fernanda. A economia psíquica dos algoritmos: quando o laboratório é o mundo. *MediaLab – UFRJ*. 14 de junho de 2018.

BÜCHI, Moritz; et al. The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, v. 36, p. 105367, 2020.

BURR, Christopher; CRISTIANNI, Nello. Can Machines Read our Minds? *Minds and Machines*, v. 29, p. 461-494, mar. 2019

CALO, Ryan. Digital Market Manipulation. *George Washington Law Review*. University of Washington School of Law. v. 82, n. 4, p. 994-1051, ago. 2014.

CAPELO DE SOUSA, Rabindranath Valentino Aleixo. *O direito geral de personalidade*. 1. ed. reimp. Coimbra: Coimbra, 2011.

COULDRY, Nick; MEJIAS, Ulises Ali. *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. California: Stanford University, 2019.

COUNCIL OF EUROPE. *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*. Adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies. Disponível em: <https://rm.coe.int/090000168092dd4b>. Acesso em: 13 dez. 2022.

CRESCI, Stefano et al. Adversarial machine learning for protecting against on-line manipulation. *IEEE Internet Computing*, v. 26, n. 2, p. 47-52, 2021.

DE CUPIS, Adriano. *Os direitos da personalidade*. Trad. Afonso Celso Furtado Rezende. São Paulo: Quorum, 2008.

DELLAROCAS, Chrysanthos. Strategic Manipulation of Internet Opinion Forums: Implications for Consumers and Firms. *Management Science*, v. 52, n. 10, p. 1577-1593, out. 2006.

DORNELAS, Felipe Müller. A proteção de dados pessoais na pandemia de covid-19: breves notas sobre contact tracing apps e o direito à privacidade na era da vigilância. *JSNELB*, ano 16, v. 6, n. 1, abr./jun. 2021.

DOROFEEVA, Julia; AKINFIEVA, Olga; SAKVARELIDZE, Eliza. Consideración de la influencia de la manipulación on-line en la intención suicida de los adolescentes. *Interacción y Perspectiva*, v. 12, n. 1, p. 63-45, maio, 2022.

FISCHER, Alexander. Manipulation and the Affective Realm of Social Media. In JONGEPIER, Fleur; KLENK, Michael. *The Philosophy of On-line Manipulation*. New York: Routledge, 2022.

FOUCAULT, Michel. *História da sexualidade: a vontade de saber*. Trad. Maria Thereza da Costa Albuquerque; J. A. Guilhon Albuquerque. Rio de Janeiro, São Paulo: Paz e Terra, 2014.

FOUCAULT, Michel. O sujeito e o poder. In: DREYFUS, Hubert; RABINOW, Paul. *Michel Foucault, uma trajetória filosófica: para além do estruturalismo e da hermenêutica*. Trad. Vera Porto Carrero. Rio de Janeiro: Forense Universitária, pp. 231-249, 1995.

FOUCAULT, Michel. *Segurança, território, população: curso dado no College de France (1977-1978)*. Trad. Eduardo Brandão. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Trad. Raquel Ramallete. 20. ed. Petrópolis: Vozes, 1999. Ebook.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

FRISCHMANN, Brett; SELINGER, Evan. *Re-engineering humanity*. Reino Unido: Cambridge University, 2018.

HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Coord). *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Alemanha: Springer, 2008, p. 17-30.

INSTITUTO TRICONTINENTAL DE PESQUISA SOCIAL. *Big Techs e os desafios atuais para a luta de classes*. Dossiê 46, novembro de 2021. Disponível em: <https://thetricontinental.org/pt-pt/dossier-46-big-tech/>. Acesso em: 21 dez. 2022.

KAUFMAN, Dora. *Os Meandros da Inteligência Artificial: Conceitos-chave para Leigos*. Estado da Arte, 1 de fevereiro de 2018. Disponível em: <https://estadodaarte.estadao.com.br/os-meandros-da-inteligencia-artificial-conceitos-chave-para-leigos/>. Acesso em: 19 maio 2022.

KIM, Pauline T. Manipulating Opportunity. *Virginia Law Review*, v. 106, n. 4, p. 867-935, jun. 2020.

KLENK, Michael. (On-line) manipulation: sometimes hidden, always careless. *Review of Social Economy*, v. 80, n. 1, p. 85-105, 2022.

LEE, Shun-Yang; QIU, Liangfei; WHINSTON, Andrew. The Perils of On-line Manipulation. *48° Hawaii International Conference on System Sciences (HICSS)*, 2015.

LESSIG, Lawrence. *Code: version 2.0*. New York, USA: Basic Books, 2006.

LEVIN, Sam. Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'. *The Guardian*, San Francisco, 1 may, 2017. Disponível em: <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>. Acesso em: 21 dez. 2022.

MARTINS, Leonardo. Direito geral de liberdade. In CANOTILHO, J. J. Gomes; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz; et al. *Comentários à Constituição do Brasil*. 2. ed. São Paulo: Saraiva, 2018.

MENCZER, Filippo. 4 Reasons Why Social Media Make Us Vulnerable to Manipulation. *RecSys '20*, Brasil, set. 2020.

MONTEAGUDO, Ricardo. Democracia em tempos de vigilância ubíqua. *Revista Quaestio Iuris*, Rio de Janeiro, v. 14, n. 4, p. 1727-1743, dez. 2021.

PENNEKAMP, Jan; HENZE, Martin; HOHLFELD, Oliver; PANCHENKO, Andriy. Hi Doppelgänger: Towards Detecting Manipulation in News Comments. *WWW'19 Companion*, São Francisco, EUA, p. 197-205, maio, 2019.

PETERS, Uwe. Reclaiming Control: Extended Mindreading and the Tracking of Digital Footprints. *Social Epistemology*, v. 36, n. 3, p. 267-282, 2022.

RICHARDS, Neil M. The Dangers of Surveillance. *Harvard Law Review*, v. 126, n. 7, p. 1934-1965, 2013.

ROUVROY, Antoinette; BERNS, Thomas. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? *Revista Eco Póis*, v. 18, n. 2, p. 35-56, 2015.

ROUVROY, Antoinette; STIEGLER, Bernard. Le régime de vérité numérique: de la gouvernementalité algorithmique à un nouvel État de droit. *Socio: La nouvelle revue des sciences sociales*, n. 4, p. 113-140, 2015.



SIGI, Lee; et al. The Impact of Social Endorsement Cues and Manipulability Concerns on Perceptions of News Credibility. *Cyberpsychology, Behavior, and Social Networking*. v. 24, n. 6, p. 384-389, jun. 2021.

SPENCER, Shaun B. The Problem of On-line Manipulation. *University of Illinois Law Review*, v. 2020, n. 3, p. 959-1006, jul. 2020.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. On-line Manipulation: Hidden Influences in a Digital World. *Georgetown Law Technology Review*, v. 4, n. 1, p. 1-45, 2018.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy, and manipulation. *Internet Policy Review*, v. 8, n. 2, p. 1-22, 2019.

WANG, T. Le, S.; LEE, D. MALCOM: Generating Malicious comments to attack neural fake news detection models. *Proc. IEEE Int. Conf. Data Mining*, p. 282-291, 2020.

WOOD, Allen W. Coercion, manipulation, exploitation, p. 17–50. In COONS, Christian; WEBER, Michael (Coord). *Manipulation: Theory and practice*. Reino Unido: Oxford University, 2014.

YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences of the United States of America*, v. 112, n. 4, p. 1036-1040, jan. 2015.

ZANKER, Markus; ROOK, Laurens; JANNACH, Dietmar. Measuring the impact of on-line personalisation: Past, present and future. *International Journal of Human-Computer Studies*, v. 131, p. 160-168, nov. 2019.

ZARSKY, Tal Z. Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law*, v. 20, n. 1, p. 157-188, 2019.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder*. Trad: George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

Submissão: 14/03/2023

Aceito para Publicação: 16/05/2023

DOI: 10.22456/2317-8558.130117