UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

RAFAEL DA SILVA ALVIM

Proteção de dados pessoais sob o paradigma da confiança: uma defesa da autonomia humana na era da manipulação movida a dados

Brasília

2025

RAFAEL DA SILVA ALVIM

Proteção de dados pessoais sob o paradigma da confiança: uma defesa da autonomia humana na era da manipulação movida a dados

Dissertação apresentada ao Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de Brasília (área de concentração "Direito, Estado e Constituição"), como requisito parcial à obtenção do título de Mestre em Direito.

Orientadora: Profa. Dra. Fernanda de Carvalho Lage

Brasília

2025

RAFAEL DA SILVA ALVIM

Proteção de dados pessoais sob o paradigma da confiança: uma defesa da autonomia humana na era da manipulação movida a dados

Dissertação apresentada ao Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de Brasília (área de concentração "Direito, Estado e Constituição"), como requisito parcial à obtenção do título de Mestre em Direito.

Aprovado em 19 de fevereiro de 2025.

BANCA EXAMINADORA

_____

Profa. Dra. Fernanda de Carvalho Lage (Orientadora)

_____

Profa. Dra. Ana de Oliveira Frazão (Avaliadora Interna)

_____

Prof. Dr. Leonardo de Andrade Mattietto (Avaliador Externo)

Para o Heitor, na esperança de que cresça e viva em um mundo melhor.

Para a Ritta de Cássia, *in memoriam*, sempre.

AGRADECIMENTOS

A jornada que culmina na elaboração e na apresentação desse trabalho teria sido uma tarefa impossível caso me faltasse a dedicação, o apoio, a compreensão e a paciência de diversas pessoas que caminharam ao meu lado nos momentos em que eu mais precisei ao longo desses dois anos. Essa dissertação, portanto, não só apresenta uma resposta a um problema científico, mas materializa o valor fundamental da amizade e do acolhimento, sem os quais eu não teria conseguido escrever nem ao menos uma das mais de oitenta mil palavras nesse documento.

É justo e necessário, portanto, registrar o meu reconhecimento e o meu profundo agradecimento às pessoas que me cercaram e preencheram meus dias – e ainda, felizmente, o fazem – com a sua presença, estendendo-me a mão amiga, mesmo que virtualmente. Preciso, da mesma forma, agradecer às pessoas que me deram o privilégio de sua presença, que deixaram uma marca indelével na construção da minha própria história. Inspirar os outros é uma das mais belas formas de se tornar imortal. Essas pessoas são imortais, porque vivem em mim.

Minha avó e mãe, Ritta de Cássia Alvim, foi a maior incentivadora dos meus estudos. Demonstrava um entusiasmo sincero e uma indisfarçável alegria diante das minhas conquistas acadêmicas, mesmo que singelas. Ela, que adoraria saber que eu cheguei ao Mestrado, sempre me deu muito e me exigiu muito pouco: que eu estudasse. Em troca, me deu teto, comida, educação – quando nenhuma outra pessoa seria capaz de o fazer –, pelo simples fato de me amar. Está aqui, vó. A gente venceu mais uma etapa. Eu sei que isso só foi possível porque, além de plantar a semente no meu coração, você esteve ao meu lado o tempo todo. E eu vou continuar a fazer o que você me ensinou a fazer: estudar e ensinar. Obrigado.

À minha irmã Amanda Alvim e ao meu sobrinho Heitor Alvim. Mesmo longe, meu amor por vocês foi (e é) o sentimento que me impulsionou a escrever esse trabalho. Obrigado por serem o meu laço mais forte e profundo, por tentarem se fazer presentes apesar do oceano que nos separa e por estarem ao meu lado, em coração e pensamento. Heitor, quando tiver esse "livro" nas mãos, saiba que ele foi escrito para você. Eu escrevi esse trabalho pensando no que será do mundo em que você vai crescer, quando eu já não estiver mais por aqui. Quero que você tenha uma vida livre e feliz, que você possa conversar com seus amigos, ir para as festas da escola (e, depois, da faculdade) e andar pelas ruas sem ser observado, sem sofrer preconceitos pelas suas escolhas, sem que coisas importantes para você dependam de uma máquina que te vigia e sabe tudo sobre você. Quero que você viva num mundo em que você possa se expressar

livremente, descobrir e criar coisas novas e empolgantes, que tornarão melhor a vida de outras pessoas. Espero, com esse trabalho, te dar o exemplo disso. Use todo o seu talento e potencial para fazer do mundo um lugar um pouquinho melhor para todos, sempre.

Essa jornada também foi desafiadora do ponto de vista da saúde mental. Aqui, eu tive a oportunidade de vivenciar e de compreender, em todo o seu potencial, a importância do olhar fraterno e da escuta atenta revelados na figura de amigos e profissionais que fizeram por mim o melhor que poderiam ter feito, sem pensar duas vezes. Aos meus amigos – dentre os quais cito, mesmo correndo o risco de ser injusto, Amanda Nunes, Larissa Camargo, Thalita Callegaro, Olga Pinheiro, Marina Aguileras e João Felipe Galvão –, agradeço por terem sempre me oferecido o melhor de si próprios, por terem permanecido ao meu lado, por terem compreendido as minhas falhas, por terem me incentivado e me emprestado, generosamente, a sua atenção. Obrigado, aliás, por terem sempre acreditado em mim mais do que eu mesmo.

Aos profissionais que estiveram ao meu lado nessa jornada, colocando o melhor de suas habilidades em meu benefício, agradeço por terem contribuído decisivamente com o sucesso dessa invulgar missão. Menciono, como melhor expressão da minha gratidão e reconhecimento, as. Dras. Juliana Ferreira e Flávia Onishi. Da mesma forma, agradeço, pelo impacto positivo que produziram na minha vida, ao longo desses dois anos, aos profissionais da educação física que (às vezes literalmente) caminharam ao meu lado nessa jornada. Por todos, agradeço ao Prof. Marcus Gabriel, pelo trabalho sério e dedicado.

Pela inspiração responsável por me trazer à pós-graduação *stricto sensu*, pela confiança no meu potencial para conduzir uma investigação científica e oferecer alguma contribuição significativa à comunidade acadêmica – e à sociedade, de modo mais amplo –, e pelas generosas palavras de incentivo e encorajamento que sempre me levaram adiante, agradeço aos professores que tive a sorte e o privilégio de encontrar durante a minha (sempre inacabada) jornada intelectual. Agradeço, em particular, à minha orientadora, Profa. Dra. Fernanda Lage, por ter me conduzido, com seu olhar atento e com contribuições sempre valiosas, que muito me ensinaram e enriqueceram o presente trabalho, pela árdua e apaixonante jornada da pesquisa científica.

Agradeço, por fim, a Deus e aos trabalhadores fraternos da seara do mestre Jesus, que, como expressão sublime do dever maior de caridade, se mantiveram silenciosamente ao meu lado, intuindo-me a persistir, por entre as dificuldades, no caminho edificante do Evangelho.

“Eu lhes digo que a palavra ‘busca’ significava uma jornada existencial ousada, não o toque do dedo para acessar respostas já existentes; que ‘amigo’ é um mistério personificado que pode ser forjado cara a cara e coração a coração; e que ‘reconhecimento’ é o lampejo de acolhimento que vivenciamos no rosto da pessoa amada, não ‘reconhecimento facial’. Digo que não está nada certo ter nossos melhores instintos de conexão, empatia e informação explorados por uma compensação draconiana que mantém esses bens como reféns para uma varredura completa de nossa vida. Não está nada certo que cada movimento, emoção, fala e desejo seja catalogado, manipulado e então usado para nos pastorear sub-repticiamente através do tempo futuro em nome do lucro de terceiros. ‘Essas coisas são muito recentes’, digo a eles. ‘Elas não têm precedentes. Vocês não deveriam aceitá-las sem questionar porque elas não estão nada certas’.” (ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. 1. ed. Rio de Janeiro: Intrínseca, 2019, p. 584)

RESUMO

A presente investigação se ocupa de avaliar as potencialidades de uma epistemologia do regime jurídico de proteção de dados pessoais pautada no conceito de confiança para reforçar a proteção à autonomia individual no contexto das plataformas digitais. Ao situar o problema de pesquisa por meio do exame das principais características das relações informacionais no contexto do capitalismo de vigilância (extração massiva de dados pessoais, dependência, hipervulnerabilidade e assimetrias de poder e informacionais), o trabalho discute figura dos padrões obscuros (*dark patterns*) – técnicas de *design* enganoso que exploram vulnerabilidades e vieses cognitivos dos usuários para instrumentalizar a agência humana – enquanto exemplos eloquentes das ameaças à autonomia individual nos ambientes *online* não adequadamente endereçados pelas leis de proteção de dados estruturadas sobre a ideia de controle e de legitimidade do tratamento (*paradigma do controle*). Investigam-se, portanto, as efetivas potencialidades da proteção de dados pessoais pautada na noção de controle individual na perspectiva da proteção da autonomia individual, considerado o fenômeno dos padrões obscuros. À luz do contexto brasileiro, evidencia-se a insuficiência do paradigma do controle como mecanismo de proteção da autonomia individual no uso de plataformas digitais, sobretudo em se considerando o uso de técnicas de *design* enganoso. Problematiza-se o marco teórico, de sorte a explicitar e discutir seus postulados dogmáticos, concluindo-se que uma epistemologia pautada na noção de confiança é compatível com o regime jurídico brasileiro, e que se apresenta como acréscimo substancial ao regime de proteção das liberdades fundamentais que a Lei Geral de Proteção de Dados Pessoais (LGPD) buscou resguardar, notadamente a autonomia individual, ao trazer para o centro do debate a respeito da regulação dos fluxos informacionais o dever de lealdade (noção que desborda dos estreitos limites procedimentais empregados pela LGPD para se avaliar a legitimidade das atividades de tratamento) como aspecto fundacional de uma compreensão da proteção de dados pessoais atenta às dinâmicas de poder – materializadas nas técnicas de manipulação por meio do uso de padrões obscuros – entre usuários e empresas cuja atividade econômica se estruture sobre a extração massiva de dados pessoais a partir do uso de plataformas digitais.

Palavras-chave: autonomia; privacidade; controle; confiança; proteção de dados.

ABSTRACT

The present research is concerned with assessing the potentialities of an epistemology of the personal data protection legal regime based on the concept of trust in order to strengthen the protection of individual autonomy in the context of the digital platforms. In locating the research problem through the examination of the main characteristics of informational relationships in the context of surveillance capitalism (mass extraction of personal data, dependence, hypervulnerability and asymmetries of power and information), the work discusses the figures of dark patterns – deceptive design techniques that exploit users' vulnerabilities and cognitive biases to instrumentalize human agency – while eloquent examples of the threats to individual autonomy in online environments inadequately addressed by data protection laws focused on the idea of control and processing legitimacy (*control paradigm*). It thus investigates the effective potentialities of personal data protection based on the notion of individual control from the perspective of the protection of individual autonomy, considering the dark patterns phenomenon. In light of the Brazilian context, the insufficiency of the control paradigm as a mechanism for protecting individual autonomy in the use of digital platforms becomes evident, especially when considering the use of deceptive design techniques. The theoretical framework is problematized, in order to explicate and discuss its dogmatic postulates, concluding that an epistemology based on the notion of trust is compatible with the brazilian legal regime, and that it presents itself as a substantial addition to the protection of fundamental freedoms regime that the Lei Geral de Proteção de Dados Pessoais (LGPD) sought to watch, notably individual autonomy, by bringing to the center of the debate concerning the regulation of information flows the duty of loyalty (a notion that goes beyond the narrow procedural limits employed by the LGPD to assess the legitimacy of processing activities) as a foundational aspect of a personal data protection comprehension that is mindful to the power dynamics – materialized in manipulation techniques through the use of dark patterns – between users and companies whose economic activity is structured on the mass extraction of personal data from the use of digital platforms.

Keywords: autonomy; privacy; trust; control; data protection.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
AI Act	Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho
CCPA	California Consumer Privacy Act
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CNIL	Commission Nationale de l'Informatique et des Libertés
DCA	Data Care Act
DETOUR Act	Deceptive Experiences to Online Users Reduction Act
DESI	Digital Economy and Society Index
DMA	Digital Markets Act
DSA	Digital Services Act
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
FIP	Fair Information Practices
FTC	Federal Trade Commission
LCP	Lei do Cadastro Positivo
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
MJ	Ministério da Justiça
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PNID	Plano Nacional de Inclusão Digital
PL	Projeto de Lei
RGPD	Regulamento Geral de Proteção de Dados
ROSCA	Restore Online Shoppers' Confidence Act

SUMÁRIO

INTRODUÇÃO

Do despertar ao adormecer, plataformas digitais[1] são corriqueiramente utilizadas pelos indivíduos como meios – por vezes únicos – de acesso a diversos bens e serviços. Do monitoramento de sinais vitais à mobilidade urbana; do entretenimento à busca por relacionamentos amorosos; da hospedagem à lista de espera em restaurantes, a figura ubíqua de tais interfaces representa a epítome do modo de vida contemporâneo[2]. Qualquer que seja a atividade mediada pelas plataformas digitais, em todas elas o *dado pessoal* representa o insumo fundamental do modelo econômico em que se inserem, baseado na *comodificação* das informações a respeito de seres humanos[3].

É importante, nesse modelo, assegurar a perenidade do fluxo informacional, de forma a abastecer vastos repositórios de dados pessoais (*Big Data*)[4], possibilitando-se não apenas a sua comercialização, mas também análises, inferências e predições cada vez mais precisas (*Big Analytics*) sobre o comportamento de indivíduos ou de grupos que possam ser identificados e classificados por denominadores comuns. No contexto dessas novas atividades[5] envolvendo dados pessoais – sobre as quais se projeta uma regulação ainda incipiente no Brasil –, técnicas que viabilizem a sua extração em massa oferecem grandes vantagens competitivas. A partir dessa perspectiva, poderíamos reformular a afirmação inicial desse trabalho, para dizer que *do despertar ao amanhecer, plataformas digitais são utilizadas como meios de conversão das*

---

[1] No presente trabalho, utilizar-se-á a definição de plataformas digitais dada por Srnicek (2017, p. 254): "Essencialmente, elas [as plataformas] são um novo tipo predominante de modelo de negócio baseado em reunir diferentes grupos. Facebook e Google conectam anunciantes, empresas e usuários cotidianos; a Uber conecta passageiros e motoristas; e Amazon e Siemens estão construindo e alugando as infraestruturas de plataforma que sustentam a economia contemporânea. Essencial para todos esses negócios de plataforma – e indicativo de uma mudança mais ampla no capitalismo – é a centralidade dos dados. Dados são o recurso básico que impulsiona essas empresas, e são os dados que lhes dão vantagem sobre os concorrentes." (Tradução nossa)

[2] De acordo com a pesquisa TIC Domicílios 2023, "89% da população brasileira com 10 anos ou mais já utilizou a Internet, proporção superior à observada em 2022, quando 86% mencionaram já terem utilizado a rede" (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 27). Adiante, a mesma pesquisa revela: "Cerca de nove entre cada dez usuários de Internet enviaram mensagens nos três meses anteriores à pesquisa (92%). Destacam-se, também, entre as atividades de comunicação, a conversa por chamada de voz ou vídeo (81%) e o uso das redes sociais (80%)" (*Idem*, p. 28).

[3] "A violação da privacidade e dos dados pessoais torna-se, portanto, um lucrativo negócio que, baseado na extração e na monetização de dados, possibilita a acumulação de um grande poder que se retroalimenta indefinidamente [...]." (Frazão, 2019a, p. 29)

[4] "[...] com a possibilidade de organizar tais dados de maneira mais escalável (*e.g.*, *Big Data*), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma 'economia de vigilância' que tende a posicionar o cidadão como um mero expectador das suas informações." (Bioni, 2020, p. 12)

[5] As atividades comerciais das cinco maiores empresas de tecnologia do mundo (Alphabet, Amazon, Apple, Meta e Microsoft, denominadas *Big Techs*) se estruturam essencialmente sobre a operação de plataformas digitais, e movimentam um pujante mercado mundial. Em 2023, o lucro registrado foi de US$ 311 bilhões. Disponível em: https://www.poder360.com.br/economia/big-techs-batem-recorde-em-2023-com-lucro-de-us-327-bilhoes/. Acesso em: 10 nov. 2024.

experiências humanas em dados pessoais. Como se vê, o lugar reservado aos usuários em tal dinâmica – sem que sequer se deem conta disso, no mais das vezes – é o de *produção* dessa valiosa matéria-prima.

Apresentam-se, nesse complexo cenário, dois grandes desafios à proteção da autonomia individual. De um lado, o uso, nas plataformas, de técnicas de engano e manipulação dos usuários para maximizar a extração[6] de dados pessoais (*padrões obscuros*), dar-lhes a *impressão* do controle sobre seus dados, ou dificultar o exercício de direitos. De outro, um regime protetivo erigido sobre o *paradigma do controle*, que se ampara na racionalidade dos indivíduos (pretensamente capazes de fazer escolhas autônomas sobre o fluxo de seus próprios dados) e em uma ótica da *legitimidade* do tratamento a partir da demonstração do cumprimento de requisitos procedimentais, que promove um *descolamento* entre a relação *informacional* e a relação *substancial* entre usuários e plataformas digitais.

É a partir de tais desafios, considerando-se relevantes formulações doutrinárias acerca do papel da confiança como vetor axiológico de uma abordagem regulatória *substancial* do fluxo informacional, que buscaremos propor uma resposta ao nosso problema de pesquisa: *em que medida uma epistemologia da proteção de dados pessoais baseada no paradigma da confiança poderia reforçar a proteção da autonomia individual no uso de plataformas digitais?*

É objetivo da presente pesquisa investigar, a partir de perspectiva ainda pouco explorada pela doutrina nacional, as potencialidades de uma nova forma de compreender a proteção de dados pessoais, no sentido de ampliar-se a defesa da autonomia individual, considerada a ameaça representada pela manipulação por padrões obscuros. Nesse contexto, a importância do estudo do tema está na **proposição de uma mudança de paradigma** na epistemologia da proteção de dados pessoais, que dá amparo a novas abordagens regulatórias, centradas na relação *substancial* subjacente ao fluxo informacional.

Sem desconsiderar a importância do paradigma do controle, constrói-se o argumento no sentido de sua insuficiência para a proteção da autonomia individual frente à ameaça de manipulação por padrões obscuros. Como se verá, cuida-se de modelo protetivo gestado e implementado no contexto europeu, em que se consolidou uma tradição jurídica (e, inclusive, cultural) no sentido da proteção de dados pessoais, e cuja transposição para o contexto brasileiro

---

[6] "Embora as plataformas digitais possam dar ensejo a diferentes tipos de interações, com distintos propósitos, é inequívoco que têm sido reiteradamente utilizadas por poderosos agentes econômicos que operacionalizam grandes empreendimentos, a partir dos dados coletados dos seus usuários, os quais são utilizados para os mais diversos fins. Daí a ideia de uma economia movida a dados (*data driven economy*), já que estes são hoje o novo 'petróleo' ou o principal insumo das atividades econômicas." (Frazão, 2019b, p. 333).

deve ocorrer de modo cauteloso, sob pena de total inefetividade do regime jurídico. Afinal, em um país marcado por extrema desigualdade (não apenas informacional, mas também social, econômica e educacional), pretender implementar um regime protetivo eficaz baseado na atribuição, aos indivíduos, do controle sobre o fluxo de seus dados pessoais é, no mínimo, um objetivo audacioso.

Com efeito, no contexto brasileiro, a proteção de dados pessoais pautada no controle individual pode não ser suficiente. Como a presente pesquisa revela, uma epistemologia escorada no paradigma da confiança se mostra mais consentânea com a perspectiva de um Estado Social compromissado com a mitigação de desigualdades extremas, inclusive no ambiente digital. Tal paradigma, antecipe-se, leva em consideração o papel primordial dos conceitos de confiança, vulnerabilidade e lealdade na regulação do fluxo informacional. Para essa nova visão, são relevantes os contornos da *relação substancial* entre as empresas que operam as plataformas e seus usuários. De fato, se o fluxo informacional importa para fins de proteção dos fundamentos que a Lei Federal n. 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD") buscou promover, há também importância em trazer-se ao centro do debate a natureza (e as características[7]) da dinâmica substancial havida entre as partes envolvidas nesse fluxo, na qual se revelam a hipervulnerabilidade e as assimetrias de poder.

No **primeiro capítulo** deste trabalho, descreveremos com maior detalhamento o contexto da sociedade algorítmica, marcada pela intermediação do uso de funcionalidades essenciais à vida moderna – como a comunicação, o acesso à informação ou transações bancárias – por plataformas digitais[8], que operacionalizam a extração massiva de dados pessoais de seus usuários e interferem diretamente em aspectos existenciais por meio de decisões algorítmicas. Como brevemente já mencionamos, dados pessoais são a matéria-prima necessária à *retroalimentação* de um vantajoso modelo econômico que envolve práticas que se estendem do treinamento de sistemas de inteligência artificial[9] ao desenho de *interfaces* digitais

---

[7] "Em vez de tratar todos os tipos de relações de informação como iguais e fungíveis, [o dever de lealdade] aumentaria as obrigações e restrições sobre as partes dominantes à medida que acumulam poder. Quanto mais poder uma empresa tem em um relacionamento, mais protetora e leal ela deve ser. Um dever de lealdade adicionaria uma camada adicional ao direito da privacidade de dados. A privacidade não seria mais principalmente sobre os dados; em vez disso, teria que considerar as relações entre as pessoas e as empresas às quais elas estão expostas." (Richards; Hartzog, 2022b, p. 995, tradução nossa)

[8] Aliás, cumpre também lembrar do uso crescente de dispositivos inteligentes (como *smartphones*, *smart TVs* e *smartwatches*, por exemplo), cujo funcionamento depende da conexão à *Internet* e, invariavelmente, do emprego de plataformas digitais. De acordo com notícia do periódico Forbes Tech, "até 2025, mais de 27 bilhões de dispositivos estarão conectados". Disponível em https://forbes.com.br/forbes-tech/2022/08/iot-ate-2025-mais-de-27-bilhoes-de-dispositivos-estarao-conectados/. Acesso em: 20 out. 2024

[9] Vale citar, a propósito, trecho de decisão cautelar proferida pela Autoridade Nacional de Proteção de Dados (ANPD), em que se determinou a suspensão, no Brasil, da vigência da nova política de privacidade da empresa

que induzam o vício (*addictive behavior*) e capturem, ao máximo possível, a atenção dos usuários[10], instrumentalizando a própria agência humana.

Do contexto a ser aprofundado emergem novos problemas que deverão ser debatidos e compreendidos pela ciência jurídica, a reforçar a importância do tema da pesquisa ora apresentada. Em primeiro lugar, o crescente fenômeno de *dataficação* da vida é observável por uma relação cada vez mais estreita entre seres humanos e interfaces digitais, a descortinar um cenário de *dependência* com relação ao uso das plataformas[11], que se intensifica à medida que cada vez mais aspectos da vida passam envolver a intermediação por alguma plataforma digital[12] (e, bem assim, a sua conversão em dados pessoais).

Em segundo lugar, a extração massiva de dados pessoais via plataformas, enquanto fenômeno da economia movida a dados (ou "economia de plataformas", na denominação utilizada por Julie Cohen[13]), faz surgir *assimetrias informacionais*[14] – e, consequentemente, de poder – como subprodutos. Nesse particular, Pasquale (2016, p. 9) se utiliza da metáfora do "espelho de um lado só" (*one-way mirror*), como representação de uma lógica de *hipervigilância* que decorre da intensificação do poder de coleta e de concentração de informações em apenas um dos polos da relação informacional. De acordo com o autor,

> Nós não vivemos em um reino pacífico de jardins privados e murados; o mundo contemporâneo lembra mais um espelho de um lado só. Importantes atores corporativos têm conhecimento sem precedentes sobre as minúcias de nossas vidas cotidianas, enquanto nós sabemos pouco ou nada sobre como eles

---

Meta: "a empresa expõe que informações publicamente disponíveis e informações compartilhadas em produtos e serviços da Meta, incluindo dados pessoais, podem ser utilizadas para treinamento de seus sistemas de IA generativa" (Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta. Acesso em: 20 out. 2024).

[10] "[...] com o novo horizonte de possibilidades também veio a erosão do perímetro da vida privada. Então, é tanto quanto um paradoxo que em tendo individualizado tão completamente a nossa atenção, nós acabemos sendo menos nós mesmos e mais escravos de nossas várias mídias e dispositivos. Sem consentimento expresso, a maioria de nós se abriu passivamente à exploração comercial de nossa atenção praticamente em qualquer lugar e a qualquer tempo." (Wu, 2017, p. 350, tradução nossa)

[11] "Em termos econômicos, as plataformas representam estratégias horizontais e verticais para extrair o valor excedente dos dados de usuários. Porque esse objetivo requer grandes números de usuários gerando grandes quantidades de dados, o objetivo do provedor da plataforma é se tornar e permanecer o ponto de intermediação indispensável para as partes em seus mercados-alvo." (Cohen, 2017, p. 9, tradução nossa)

[12] "São interações recíprocas: relações online modificam relações offline e vice-versa, fazendo com que o ambiente digital e o 'real' tenham a si atribuída certa simbiose, que pode ser identificada a partir dos objetivos (produtos/serviços inteligentes), dos sujeitos (perfis de consumo e de trabalho), da estrutura (virtual) e das relações ali estabelecidas." (Marques; Mucelin, 2022, p. 5)

[13] Segundo a autora, "as vidas cotidianas de usuários da rede tornaram-se cada vez mais 'dataficadas' – convertidas em fluxos estruturados de dados apropriados para a coleção e análise contínuas no nível de plataforma" (2017, p. 5, tradução nossa).

[14] Embora empresas digitais saibam muito sobre nós, não sabemos muito sobre elas – suas operações, que tipos de dados coletam, como usam esses dados, e com quem os compartilham. Graças a essa assimetria de informação, estamos especialmente vulneráveis a elas, e devemos confiar que elas não vão trair nossa confiança ou nos manipular." (Balkin, 2020, p. 11, tradução nossa).

> usam esse conhecimento para influenciar as importantes decisões que nós – e eles – tomamos. (Tradução nossa)

Em terceiro lugar, a *vulnerabilidade* dos indivíduos diante das empresas que titularizam, desenham, operam e modificam unilateralmente as plataformas digitais. Trata-se de decorrência lógica do cenário de dependência e de assimetrias que mencionamos; no entanto, no contexto das plataformas, tal vulnerabilidade se agrava pelo fato de que os usuários não têm qualquer ingerência ou poder de barganha com relação à definição de sua arquitetura[15] ou mesmo quanto à possibilidade de utilizá-las *ou não* para obter determinado bem ou serviço. Daí porque Bioni (2020, p. 157) identifica, nesse contexto, uma *hipervulnerabilidade*, caracterizada por uma "sobreposição de fraquezas" do cidadão no mercado informacional, que decorre "da situação objetiva pertinente a sua inserção no mercado informacional, cujos traços de vulneração são peculiares e se sobrepõem ao ordinário das relações de consumo".

Diante dos novos desafios impostos pela *revolução da informação*[16], incumbe ao Direito salvaguardar direitos fundamentais dos indivíduos hipervulneráveis (como a autonomia, a privacidade e, ao fim e ao cabo, a própria dignidade), submetidos à coleta massiva de dados pessoais, à vigilância, e a decisões algorítmicas sobre questões existenciais[17], baseadas na formação de um perfil biopsicossocial sobre o qual não têm qualquer ingerência (ou sequer conhecimento). São superlativos os riscos que se apresentam à humanidade, na atual quadra da História, produzidos pela utilização disseminada e constante de tecnologias da informação e comunicação e suas interfaces digitais, mesmo porque não se restringem à esfera individual; no limite, pode-se cogitar de potenciais danos à própria democracia[18], a nível mundial.

---

[15] "As pessoas extraem diferentes conclusões da mesma informação dependendo de como ela é apresentada ('*framing effects*'), e assim em diante. Porque esses vieses cognitivos são difundidos e previsíveis, manipuladores podem facilmente tratá-los como vulnerabilidades a serem exploradas. Manipuladores podem lembrar seus alvos de fatos não importantes para que deem a eles peso indevido. Eles podem indicar que os amigos de seus alvos acreditam em certas coisas na esperança de que eles também irão acreditar. Eles podem enquadrar a informação de maneiras errôneas. A manipulação, portanto, não precisa envolver o total engano; a verdade também pode ser usada para controlar nossa tomada de decisões." (Susser; Roessler; Nissenbaum, 2019a, p. 22, tradução nossa)

[16] "Estamos no meio de uma revolução da informação, e estamos apenas começando a entender suas implicações. As últimas décadas testemunharam uma transformação dramática na maneira como compramos, utilizamos serviços bancários, e conduzimos nossas tarefas diárias – mudanças que resultaram em uma proliferação sem precedentes de registros e dados." (Solove, 2004, p. 1, tradução nossa)

[17] "[...] algoritmos vêm sendo utilizados para análises complexas, que abarcam as respostas para nossas perguntas mais difíceis, como decisões e diagnósticos que, além de representarem uma verdadeira devassa na intimidade das pessoas, ainda terão impactos nas possibilidades e no acesso destas a uma série de direitos e oportunidades." (Frazão, 2019a, p. 32)

[18] "Se, como eu argumentei, a capacidade de subjetividade crítica encolhe em condições de privacidade reduzida, o que acontece com a capacidade de autogoverno democrático? Condições de privacidade mitigada reduzem a mencionada capacidade também, porque elas prejudicam tanto a capacidade quanto o escopo da prática da cidadania. Mas uma sociedade democrática liberal não pode se sustentar sem cidadãos que possuam a capacidade de autogoverno democrático. Uma sociedade que permita a ascendência não contida de infraestruturas de vigilância não pode esperar continuar sendo uma democracia liberal." (Cohen, 2012, p. 7, tradução nossa)

Com essa perspectiva, no **segundo capítulo**, cabe-nos incursionar na dimensão dos riscos à *autonomia individual*, para refletir sobre a *manipulação*[19] dos usuários de plataformas digitais. Considerada a delimitação do problema de pesquisa, interessa-nos, em especial, compreender o fenômeno dos padrões obscuros (ou *dark patterns*), que são "interfaces de usuário cujos designers intencionalmente confundem os usuários, dificultam que eles expressem suas verdadeiras preferências, ou os manipulam para que pratiquem certas ações" (Luguri; Strahilevitz, p. 43, 2019, tradução nossa)[20].

Com efeito, uma das manifestações mais eloquentes da assimetria de poderes – e, bem assim, da vulnerabilidade dos usuários – no contexto ora delineado, é a definição unilateral de aspectos estruturantes (*design*) da arquitetura das interfaces digitais, que podem ser concebidos de forma a instrumentalizar a manifestação da vontade humana no ambiente virtual[21] a partir da exploração de vieses cognitivos, para que sejam atendidos os interesses de quem detenha o poder de controlar as características da arquitetura digital. Vale, nesse aspecto, citar a lição de Véliz (2021, p. 108):

> Outros utilizarem suas informações pessoais para manipular seus desejos também é uma forma de interferir em sua autonomia, principalmente quando tal influência é encoberta. Se você não percebe que o conteúdo que você está acessando online é mais um reflexo da forma de como publicitários ou cientistas de dados pensam que você é, em vez de um reflexo do mundo exterior, será mais difícil para você agir racionalmente e de acordo com seus próprios valores. Autonomia requer que você esteja relativamente bem-informado sobre o contexto em que você vive. Quando outros manipulam suas crenças sobre o mundo e o fazem acreditar em algo falso que influencia como você se sente e vive, eles estão interferindo em sua autonomia.

O emprego de arquiteturas enganosas para manipular os usuários de plataformas digitais transcende o mero objetivo de maximização de lucros. Na *economia da atenção*[22], o *design* das

---

[19] De acordo com Calo (2014, p. 1031), "[...] na medida em que a manipulação de mercados digitais influencia os indivíduos subliminarmente, ou então esgota os recursos limitados da força de vontade, nossos instintos ainda podem levar as pessoas a falar em termos de danos à autonomia individual ou coletiva" (tradução nossa).

[20] Em sentido análogo, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) registra que o termo se aplica "a uma grande variedade de práticas online em interfaces de usuário que guiam, enganam, coagem ou manipulam consumidores a fazer escolhas, incluindo em relação a compras, seus dados pessoas ou tempo de atenção, que podem não ser em seus melhores interesses" (OCDE, 2022, p. 8, tradução nossa).

[21] Como explicam Susser, Roessler e Nissenbaum (2019a, p. 13), manipulação "é um tipo de influência – uma tentativa de modificar a forma como alguém se comportaria se ausentes as intervenções do manipulador" (tradução nossa).

[22] Na ilustrativa lição de Wu (2019, p. 788): "[...] podemos pensar no gastador de atenção como um homem com um grande suprimento de pó de ouro vazando do bolso a uma frequência constante. Este é o consumidor, o gastador de atenção, cuja própria presença é valiosa. Enquanto ele anda pela rua, os comerciantes (os Corretores de Atenção) podem oferecer-lhe comida, bebidas ou outros atrativos de graça para atraí-lo e então podem cobrar dos outros clientes (os anunciantes) um valor extra pela oportunidade de pegar um pouco do pó que cai enquanto o homem aprecia suas bebidas. Esse, em poucas palavras, é o modelo de negócios do Corretor de Atenção." (tradução nossa)

plataformas serve a manter os usuários conectados pelo máximo de tempo possível, estimulando-se a sensação de prazer[23] e a adicção[24]; além disso, objetiva incitar – sem que os indivíduos se deem conta – o fornecimento de dados pessoais, que robustecerão sistemas de perfilamento e aperfeiçoarão algoritmos utilizados para predições e inferências a respeito do comportamento individual, com reflexos, inclusive, sobre processos eleitorais.

Nesse mesmo sentido, em suas *guidelines* sobre padrões obscuros em plataformas de redes sociais, o European Data Protection Board (EDPB) destaca que as *dark patterns* "visam a influenciar o comportamento dos usuários e podem impedir sua capacidade de proteger efetivamente seus dados pessoais e fazer escolhas conscientes" (EDPB, 2022, p. 3, tradução nossa). De fato, tem-se na manipulação um elemento-chave de perpetuação de uma lógica não só econômica, mas também de *poder*, pautada pela extração massiva de dados pessoais[25] (e, bem assim, pela hipervigilância).

Compreender os contornos dessa complexa discussão à luz do ordenamento jurídico brasileiro é tarefa que não prescinde de uma reflexão acerca dos pressupostos e características do regime jurídico incidente sobre o uso de dados pessoais por entidades privadas e públicas, de que trataremos no **terceiro capítulo**. No Brasil, embora o tema tenha sido, em alguma medida, alvo de tutela jurídica pelo Código de Defesa do Consumidor (CDC), na década de 1990, a sistematização e a centralização da disciplina do uso de dados pessoais só foram concebidas com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais[26].

---

[23] "Como é que o desejo induzido pela sugestão se traduz em nossa balança prazer-sofrimento? A balança inclina-se para o lado do prazer (um minipico de dopamina) em antecipação a uma recompensa futura, imediatamente seguida por uma inclinação para o lado do sofrimento (um minidéficit de dopamina) após a sugestão. O déficit de dopamina é um anseio e leva ao comportamento que busca a droga." (Lembke, 2024, p. 63)

[24] "É o mesmo mecanismo dos caça-níqueis: ganhar produz uma sensação boa, mas não do tipo que faz os viciados em jogo pegar o dinheiro e ir embora satisfeitos. O prazer na verdade os motiva a buscar mais. Isso também acontece com jogos on-line, redes sociais, sites de compras e outros aplicativos em que as pessoas gastam muito mais tempo ou dinheiro do que pretendiam, e de maneira rotineira. [...]. Os desenvolvedores desses aplicativos usam todos os truques da caixa de ferramentas dos psicólogos para prender os usuários tanto quanto os viciados em caça-níqueis." (Haidt, 2024, p. 156)

[25] Na precisa observação de Calo (2014, p. 1042): "[...] as tendências que constituem a manipulação no mercado digital dependem, para a sua vitalidade, de informações individuais sobre os consumidores. A produção massiva de vieses [...], perfilamento de persuasão [...], tudo isso requer acesso a grandes conjuntos de dados do consumidor ou a detalhes específicos do consumidor. A informação tem que vir de algum lugar (ou de alguém)." (tradução nossa)

[26] Entre a entrada em vigor do CDC e a aprovação da LGPD, contudo, outras normas de relevo para o microssistema de tutela jurídica dos dados pessoais passaram a viger em nosso ordenamento jurídico. Nesse sentido, mencione-se a Lei Federal n. 12.414/2011 (Lei do Cadastro Positivo), a Lei Federal n. 12.527/2011 (Lei de Acesso à Informação) e a Lei Federal n. 12.965/2014 (Marco Civil da Internet).

A LGPD, de aberta inspiração no modelo europeu[27], tem por norte axiológico o princípio da *autodeterminação informativa* dos titulares[28] de dados pessoais, de que decorre a atribuição de direitos inerentes ao *controle* sobre as informações que lhes digam respeito[29]. Nesse sentido, a norma, fundada em um paradigma marcadamente liberal[30], compreende o titular como indivíduo dotado de racionalidade e, bem assim, da capacidade de conduzir-se e de expressar sua vontade de modo consentâneo com seus próprios interesses, uma vez que tenha acesso à informação – apresentada de modo claro, preciso e acessível – a respeito dos usos que serão feitos de seus dados pessoais.

Não por outra razão, nota-se no texto legal a prevalência de referências à manifestação formal de vontade pelos titulares de dados pessoais, como ocorre no caso da hipótese legal do *consentimento* e dos deveres a ele associados[31], e de princípios específicos consentâneos com o modelo de aviso-e-escolha[32] (*notice-and-choice*). Mendes e Fonseca (2020, p. 509) observam, com acerto, que "não é exagero afirmar que o consentimento tem figurado como instrumento regulatório central e núcleo de legitimidade prática" do regime de proteção de dados pessoais. No mesmo diapasão, Bioni (2020, p. 130) nota a existência de uma espécie de *veneração* ao consentimento do titular de dados pessoais, uma vez que

> [e]m que pese sempre ter havido dúvidas em torno da racionalidade e do poder de barganha dos titulares de dados pessoais para que eles empreendessem um controle efetivo sobre seus dados pessoais, o consentimento permaneceu sendo o elemento nuclear da estratégia regulatória da privacidade informacional.

Se, por um lado, o regime jurídico de proteção de dados pessoais busca empoderar os indivíduos por meio da atribuição de controles, por outro, ele se baseia em uma abordagem

---

[27] "Os dois sistemas encontram-se fortemente alinhados, como desejou o legislador brasileiro, para que a norma nacional, nos próximos anos, seja reconhecida como adequada ao sistema europeu, uma vez que isso facilitará a realização de transações e cooperações com países do bloco." (Tepedino; Teffé, 2019, p. 293)

[28] De acordo com o art. 5º, V, da LGPD, titular é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

[29] "O controle dos seus dados pessoais pelo indivíduo compõe um aspecto essencial da dimensão subjetiva do direito à proteção de dados pessoais. O conceito geral é o de que, a princípio, o titular dos dados deve ter o controle da coleta, processamento, utilização e circulação dos seus dados pessoais. Afinal, tendo em vista que os dados se referem a ele e influenciam a sua esfera de direitos, somente o titular pode determinar a extensão da circulação de seus dados na sociedade." (Mendes, 2018, p. 206)

[30] "O conceito liberal-clássico de direitos fundamentais também caracteriza a forma pela qual os bens a serem protegidos pela proteção de dados são descritos. Isso se aplica de modo especificamente claro ao direito à autodeterminação informativa. Esse direito é o direito fundamental decisivo nos domínios da proteção de dados na Alemanha. Entretanto, também está sendo mencionado com maior frequência no debate transnacional e Europeu como um direito central digno de proteção." (Albers, 2014, p. 217, tradução nossa)

[31] Citem-se, como exemplos dos deveres relacionados ao emprego da hipótese legal do consentimento, o art. 7º, § 5º, o art. 8º e o art. 9º, § 1º, todos da Lei Geral de Proteção de Dados Pessoais.

[32] Nesse sentido, a LGPD prevê, em seu art. 6º, VI, o princípio da transparência, consubstanciado na "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

baseada no risco para impor limites e parâmetros aos agentes de tratamento. Assim, busca-se regular as atividades de tratamento[33] de dados pessoais, necessárias ao desenvolvimento de atividades econômicas, a partir de critérios que pretensamente as compatibilizem com os fundamentos da norma (tais como o respeito à privacidade e o livre desenvolvimento da personalidade – art. 2º, I e VII). Nessa perspectiva, a *legitimidade* das atividades de tratamento se revela a partir de demonstrações objetivas – relatórios, testes de proporcionalidade e políticas internas, por exemplo – do cumprimento dos requisitos formais e procedimentais da LGPD[34].

Embora reconheça a vulnerabilidade dos indivíduos, bem como a existência de assimetrias de poder entre esses e os agentes de tratamento de dados pessoais, o desenho regulatório de regimes jurídicos pautados no *paradigma do controle* erige-se em torno de uma lógica marcadamente *procedimental*, que remetem à figura das *Fair Information Practices* (FIPs), concebidas na década de 1970. É dizer: a mitigação das assimetrias e a tutela da vulnerabilidade dão-se pela observância de restrições legais e pelo atendimento a princípios, exigências demonstráveis objetivamente a partir do cumprimento de deveres relacionados à *licitude* do tratamento de dados pessoais, como a implementação de canais para o exercício de direitos previstos em favor dos titulares.

No paradigma do controle, mais importa a avaliação da adequação formal da *relação informacional* do que a consideração das características da *relação subjacente* à atividade de tratamento. Não por outra razão, o mesmo plexo de parâmetros e regras limitadoras do tratamento de dados pessoais aplica-se à *ByteDance* (empresa que opera a plataforma "TikTok"[35]) e a um varejista local[36].

---

[33] A LGPD utiliza o termo *tratamento* para se referir a, basicamente, qualquer atividade que possa ser realizada com dados pessoais. Confira-se a definição trazida pelo art. 5º, X, da Lei: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

[34] "As regras sob o modelo de proteção de dados são amplamente procedimentais, com algumas exceções importantes. Essas disposições são combinadas com direitos do titular dos dados contra todos que tratam seus dados [...], sob a ideia de que o tratamento justo é, por si só, uma maneira de mitigar o poder. Mas essas estruturas não têm como objetivo principal restringir o tratamento, e sim garantir que o tratamento aconteça de forma legítima." (Richards; Hartzog, 2020, p. 4, tradução nossa)

[35] De acordo com notícia veiculada em abril de 2024 no portal "Correio do Povo", o Brasil é o terceiro país do mundo em número de usuários ativos da plataforma TikTok. Com 98,6 milhões de usuários ativos, o Brasil fica atrás, apenas, da Indonésia e dos Estados Unidos. Disponível em: https://www.correiodopovo.com.br/jornal-com-tecnologia/brasil-%C3%A9-o-terceiro-pa%C3%ADs-com-mais-usu%C3%A1rios-ativos-do-tiktok-no-mundo-veja-ranking-1.1488377. Acesso em: 21 out. 2024.

[36] Necessário consignar, todavia, que a Resolução CD/ANPD n. 2/2022 flexibilizou algumas das obrigações constantes da LGPD para agentes de tratamento de pequeno porte, assim consideradas as "microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador" (art. 2º, I).

O art. 1º da LGPD evidencia o desiderato de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Nesse diapasão, a extensa carta principiológica da norma revela preocupação com a adoção de práticas adequadas ou desejáveis que, idealmente, seriam suficientes à proteção de liberdades e garantias fundamentais do indivíduo. Entretanto, por mais amplo que seja seu conjunto de parâmetros, requisitos e limites, o modelo de proteção de dados pautado no paradigma do controle não é capaz de endereçar adequadamente o problema da manipulação no contexto do uso de plataformas digitais[37] e suas consequências lesivas para as liberdades fundamentais que o regime de proteção de dados pessoais buscou proteger.

Em primeiro lugar, ao pressupor que os usuários têm capacidade de tomar decisões racionais[38] sobre o fluxo informacional, desde que sejam adequadamente informados sobre as atividades de tratamento, o paradigma do controle atribui peso significativo à declaração formal de anuência com o tratamento, sem considerar a exploração "de *limitações* cognitivas, como vieses e heurísticas, que podem dificultar a avaliação dos elementos necessários 'para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais'" (Mendes; Fonseca, 2020, p. 514). Nesse cenário, o ônus de compreender, avaliar e concordar com o tratamento (assim como de reagir e exercer seus direitos diante de violações) recai sobre o titular de dados pessoais. Cabe acrescentar que, não raro, o consentimento é condição inafastável para o acesso às funcionalidades viabilizadas pelas plataformas digitais, o que remete o usuário a uma lógica de "pegar ou largar" (*take-it-or-leave-it choice*)[39].

Em segundo lugar, como já antecipamos, o paradigma do controle se estrutura sobre uma lógica procedimental, em que a legitimidade do tratamento de dados pessoais prepondera sobre a avaliação das dinâmicas de poder da relação subjacente (entende-se, em síntese, que o

---

[37] "[...] o controle que as leis de privacidade dão às pessoas é, em geral, voltado contra elas, e [...] as pessoas prontamente renunciam a qualquer controle que lhes possa ter sido dado. As pessoas ansiosamente abraçam as tecnologias que as machucam e fazem escolhas em seu detrimento. Embora a lei certamente deva fazer com que as empresas parem de explorar e manipular as pessoas, simplesmente restringir essas práticas não é suficiente." (Solove; Hartzog, 2024, p. 1024, tradução nossa)

[38] Entretanto, Solove e Hartzog (2024, p. 1034) argumentam: "Os estudos do psicólogo Stanley Milgram demonstraram que as pessoas prontamente se submetem à autoridade. As pessoas podem desenvolver dependências tecnológicas danosas. As pessoas frequentemente agem contra seus próprios interesses, às vezes de modos altamente autodestrutivos. Não apenas as pessoas falham em agir racionalmente, mas também agem de modos absurdamente improdutivos." (Tradução nossa)

[39] Ao examinar as causas da vulnerabilidade dos consumidores no contexto das plataformas digitais, Marques e Mucelin (2022, p. 18) notam que a complexidade do modelo de consentimento se agrava "quando o consentimento é mais aparente que real, haja vista o consumidor ver-se, no mais das vezes, constrangido ou pressionado a consentir para que o produto ou serviço acessado não lhe seja negado, já que resiste com certa normalidade a base do *take it or leave it* (pegar ou largar), fazendo com que a liberdade de consentir reste prejudicada, bem como sua autodeterminação informativa".

cumprimento dos requisitos procedimentais, *per se*, já reduz assimetrias e protege os titulares). Nesse sentido, não há vedações substanciais ou peremptórias com relação a determinadas práticas de tratamento de dados: toda atividade de tratamento é válida (ou *validável*), desde que demonstrada a sua adequação procedimental.

Essa lógica faz com que os mecanismos regulatórios estabelecidos pelo regime jurídico de proteção de dados pessoais baseado no paradigma do controle gravitem em torno da *licitude* do tratamento. Assim, a verificação da adequação das operações de tratamento envolvendo dados pessoais prestigia o cumprimento de exigências formais relacionados ao dado pessoal, excluindo-se, em princípio, a avaliação das dinâmicas de poder da relação jurídica subjacente.

A propósito, Richards e Hartzog (2020a, p. 5), ao examinarem criticamente os modelos de proteção de dados pessoais pautados no paradigma do controle, fazem referência à busca por uma "higiene de dados" (*data hygiene*), asseverando que a abordagem da proteção de dados pessoais a partir de um paradigma *relacional* enfocaria "o verdadeiro problema que a privacidade e a proteção de dados deveriam enfrentar – as consequências do poder nas relações informacionais, tornando a legitimidade do tratamento uma questão de justiça fundamental" (tradução nossa), ao invés da constatação da adequação entre as atividades de tratamento e os requisitos formais.

Como o paradigma do controle envolve a demonstração da licitude por meio da apresentação de relatórios, análises e outros documentos, há risco de que agentes de tratamento produzam simples declarações vazias do atendimento à lei. No ponto, aliás, Waldman (2021, p. 101) afirma que normas sobre proteção de dados são vítimas "da conformidade simbólica – empresas estão criando sistemas que têm a aparência e dão a sensação de verdadeira conformidade, mas são, na verdade, meros enfeites" (tradução nossa).

Sendo a relação entre usuários e plataformas digitais marcada por assimetrias informacionais, pela vulnerabilidade dos indivíduos e pela dependência destes com relação àquelas, o exame da licitude das atividades de tratamento de dados pessoais ocorridas em tal contexto deve remeter não apenas ao cumprimento de requisitos procedimentais, como políticas de privacidade claras e transparentes, ou canais de atendimento às requisições de titulares. Mais do que isso, numa perspectiva *substancial*, deve ser considerada a relação de *confiança*[40] que

[40] "Na era digital, as pessoas estão cada vez mais dependentes e vulneráveis a empresas digitais que coletam dados delas e usam dados sobre elas. Essas empresas usam dados para prever e controlar o que os usuários finais fazem e para vender acesso de consultores a esses usuários finais. As empresas digitais convidam os usuários a confiar nelas com seus dados. Quando as pessoas aceitam essa oferta de confiança, elas se tornam vulneráveis: à forma

se estabelece entre os (hiper)vulneráveis e as grandes empresas que exploram as plataformas digitais, a justificar o reconhecimento de deveres substanciais no âmbito das relações jurídicas informacionais (notadamente, o de *lealdade*), decorrências de uma conduta substancialmente protetiva.

Como destacado, o objetivo típico dos padrões obscuros é "enganar as pessoas para que paguem por algo que elas de outro modo não comprariam ou entregar informações pessoais que de outro modo elas manteriam confidenciais" (Luguri; Strahilevitz, 2021, p. 59, tradução nossa). Nada obstante, na perspectiva do *paradigma do controle*, é possível que uma empresa empregue padrões obscuros e, ainda assim, seja capaz de demonstrar conformidade com as exigências formais do regime jurídico de proteção de dados pessoais, como diz Waldman (2021, p. 101):

> No ambiente da privacidade, a União Europeia, o Congresso dos Estados Unidos e vários estados podem aprovar todas as leis de privacidade que quiserem, mas essas leis serão mobilizadas pela indústria da informação para atingir seus objetivos de lucro. Uma forma pela qual as empresas fazem isso é criando um ambiente organizacional onde as pessoas responsáveis por implementar as leis que aprovamos – advogados e profissionais de privacidade – criam estruturas, sistemas, protocolos, políticas e procedimentos que fazem parecer com que elas cumprem a lei, mas na verdade servem para minar a efetividade da lei. (Tradução nossa)

No **quarto capítulo** do presente trabalho, buscaremos enfrentar o problema de pesquisa com o auxílio do marco teórico haurido das formulações de Neil Richards e Woodrow Hartzog, que, atentos à dimensão *substancial* da relação entre usuários e plataformas digitais, sugerem uma abordagem epistemológica centralizada na vulnerabilidade identificada no contexto subjacente às relações informacionais, intimamente relacionada com a proteção da confiança. De acordo com os autores (2016, p. 459), tal enfoque recai sobre "os valores substantivos que o direito da privacidade deve acolher se for para promover a confiança que é essencial a relações informacionais sustentáveis" (tradução nossa).

Propõem os autores (2016, p. 431; 452), nesse sentido, que o paradigma da privacidade enquanto confiança erige-se sobre o pressuposto dogmático fundamental de que as relações informacionais – nas quais o uso do dado pessoal é necessário para que se atinja um certo objetivo (como as relações entre indivíduos e comerciantes, médicos, empregadores, amigos, cônjuges, etc.) – envolvem uma propensão do titular *a se tornar vulnerável* à ação de outrem, ou seja, pressupõem *confiança*.

---

como as empresas usam seus dados, à segurança dos dados das empresas (ou à falta dela) e à escolha das empresas de compartilhar ou vender os dados a terceiros." (Balkin, 2020, p. 11, tradução nossa)

Confiança e vulnerabilidade, portanto, são conceitos-chave para que se compreenda a proposta epistemológica de que ora se cogita. A partir dessa perspectiva, buscaremos, na presente investigação, testar a higidez de nossa hipótese preliminar: a de que *uma epistemologia da proteção de dados pessoais baseada no paradigma da confiança pode prestar uma contribuição decisiva para a proteção substancial da autonomia dos titulares de dados pessoais no contexto do uso das plataformas digitais.*

Para tanto, desenvolveremos o estudo do tema de pesquisa a partir da vertente jurídico-dogmática, articulando elementos internos ao próprio ordenamento jurídico, sendo necessário investigar em que medida os postulados teórico-dogmáticos que sustentam o paradigma da confiança são compatíveis com o quadro normativo delimitado pelo regime jurídico da proteção de dados pessoais centralizado pela LGPD. Antes, contudo, importa problematizar a atual perspectiva epistemológica do modelo de proteção de dados pessoais pautada no controle do titular, para aferir em que extensão se sustenta a proposta de abordagem baseada no marco teórico empregado, enquanto possível resposta ao problema de pesquisa.

Embora ao longo do trabalho tenhamos colhido elementos empíricos que buscam auxiliar o leitor na compreensão e contextualização da dimensão prática do tema delimitado – como, por exemplo, notícias, pesquisas, pronunciamentos formais de órgãos dos Poderes Judiciário e de Autoridades de Proteção de Dados, legislação nacional e estrangeira correlata ao campo de investigação –, a pesquisa que ora se apresenta é essencialmente teórica, na medida em que seus resultados se restringem aos domínios da epistemologia do regime jurídico de proteção de dados pessoais. Em arremate, discutem-se possíveis reflexos da confirmação da hipótese preliminar sobre o âmbito prático de aplicação da LGPD.

1 ENTRE ORWELL E KAFKA: O "CIDADÃO DIGITAL" NA SOCIEDADE ALGORÍTMICA

O romance distópico *1984*, de autoria de George Orwell (pseudônimo de Eric Arthur Blair), narra a história de Winston Smith, um funcionário da burocracia estatal de Oceânia, país em que um governo totalitário exerce profundo controle sobre a população por meio de seus agentes – que podem ser, inclusive, infiltrados –, integrantes da *Polícia das Ideias*, e também por tecnologias de vigilância ostensiva instaladas dentro das próprias residências.

Sempre ligadas, as *teletelas* servem não apenas à transmissão de comunicados oficiais do Partido (como é comumente denominado o governo), mas como instrumentos de dominação[41] e de demonstração de poder. Nunca se sabe quando alguém a serviço do Partido estará do outro lado do monitor observando, ouvindo, interpretando e registrando o que se passa nas casas em que vivem os habitantes de Oceânia, como Winston. Mesmo uma leve expressão facial de descontentamento ou gesto de insubordinação diante da figura onipresente do Grande Irmão pode levantar suspeitas sobre o alinhamento aos ideais do Partido.

No regime totalitário de Oceânia, sobrevivem por mais tempo aqueles que saibam dominar suas emoções, controlar suas expressões, calcular suas falas e transitar pelos locais certos. Afinal, *o Grande Irmão está de olho em você*. Ao menor sinal de subversão, qualquer cidadão pode ser *vaporizado*. Por outro lado, o Partido busca construir e apresentar – pela manipulação da narrativa oficial – uma figura protetora e carismática do Grande Irmão como parte de um projeto de docilização dos habitantes de Oceânia, para que percebam as decisões institucionais como intrinsecamente boas e corretas.

Aos poucos, Winston, responsável por reescrever notícias e declarações do Partido que já não estejam em conformidade com os atuais interesses da cúpula política – uma das estratégias de manipulação utilizadas para evitar sejam percebidas possíveis incoerências no discurso institucional –, passa a conspirar contra o governo. Descoberto, Winston é preso e torturado, e acaba por delatar sua parceira – Julia – para manter-se vivo. Submetido à força e à brutalidade do Grande Irmão, o protagonista volta a se comportar como um cidadão *normal* de

[41] "A eficiência do panóptico disciplinar consiste em que os reclusos se sintam constantemente vigiados. Eles interiorizam a vigilância. É essencial para o poder disciplinar 'a criação de um estado de visibilidade consciente e permanente'. No Estado da vigilância de George Orwell, o Big Brother cuida da visibilidade constante [...]. No regime disciplinar, medidas espaciais, como inclusão e isolamento, garantem a visibilidade dos submissos. [...]. A mobilidade é restringida de modo massivo, fazendo com que não sejam capazes de se livrar do acesso panóptico." (Han, 2022, p. 12)

Oceânia, submetendo-se sem questionamentos à intensa vigilância que ceifa, por completo, o desenvolvimento de uma sociedade plural e democrática. Em uma das mais célebres frases do livro, Orwell (2009, p. 311) escreve: "Poder é estraçalhar a mente humana e depois juntar outra vez os pedaços, dando-lhes a forma que você quiser".

A *magnum opus* de George Orwell é amiúde lembrada – e citada – como ilustração das repercussões e perigos da vigilância sobre a vida privada. O livro, cuja primeira edição fora publicada em 1949 – ano em que *smartphones* e *apps* não passavam de ficção científica –, concebe a figura das teletelas como representações futuristas de um cenário distópico em que os indivíduos são constantemente observados e movidos pelo temor de sofrer as duras penas reservadas a quem cometesse um *pensamento-crime*.

Com nítida inspiração na figura do panóptico, concebida por Jeremy Bentham[42], a tecnologia de constante vigilância retratada em *1984* convida o leitor a refletir sobre a privacidade como aspecto fundamental da liberdade individual, esfera de proteção contra interferências exteriores dentro da qual pode florescer a subjetividade humana (que, nessa acepção, guarda intrínseca relação com o que Zuboff, com arrimo na lição de Gaston Bachelard, chama de "direito a santuário"[43]).

Se, no contexto histórico em que foi publicada, a distopia de *1984* se apresentava como uma metáfora apropriada dos perigos (e consequências) da hipervigilância de governos autoritários sobre as liberdades individuais, atualmente, contudo, a obra já não mais ilustra adequadamente as preocupações que vêm pautando a discussão sobre a proteção da vida privada e suas repercussões sobre o exercício de outros direitos fundamentais (muito embora os problemas havidos no cenário narrado por George Orwell não tenham sido abandonados ou substituídos[44]). Como bem observa Frazão (2024, p. 17), ao comentar sobre o desenvolvimento

---

[42] Kietzmann e Angell (2010, p. 136) observam que, após uma "primeira geração de panópticos", que teve ênfase no condicionamento de comportamentos em localidades específicas, estamos agora diante de uma segunda geração, implementada sobretudo pelo comércio. Segundo os autores: "O comércio, através da mineração de dados e do perfilamento, foi rápido ao implementar a segunda geração, tentando superar as limitações da primeira. Vigilância baseada em computação (a indústria da aposta conduziu os rumos aqui), cartões de fidelidade, compras com cartão de crédito, celulares etc. permitem a coleta de dados pessoais de todos, incluindo não apenas aqueles suspeitos de atividades ilegais, mas também apostadores, viajantes frequentes, compradores atuais e potenciais clientes em quaisquer localidades lucrativas". (Tradução nossa)

[43] Diz Zuboff (2020, p. 538) que, no capitalismo de vigilância, as paredes das casas – entre as quais os indivíduos encontram refúgio e proteção contra interferências externas, podendo comportar-se de modo autêntico – tornaram-se permeadas por "coordenadas de termostatos, câmeras de segurança, alto-falantes e interruptores de luz 'inteligentes' que extraem e renderizam a nossa experiência para atuar sobre o nosso comportamento".

[44] "[...] o advento do computador, a proliferação de bases de dados, e o nascimento da Internet criaram uma nova espécie de problemas de privacidade. Os perigos Orwellianos certamente não desapareceram; nem tampouco os danos criados pela mídia sensacionalista. Mas o surgimento de dossiês digitais criou problemas novos e diferentes. Novas leis de privacidade foram criadas em resposta." (Solove, 2004, p. 74, tradução nossa)

da *neurotecnologia*, "o contexto atual mostra o quão desatualizada está a ideia defendida por George Orwell [...], de que, no contexto de vigilância, a única coisa que continuaria pertencendo verdadeiramente aos cidadãos seriam os poucos centímetros cúbicos dentro de seus crânios".

Com o avançar do tempo (e da tecnologia), a dogmática da privacidade sofreu mutações. A forma como as pessoas compreendem a privacidade, também. Na síntese de Rodotà (2008, p. 23), "novas dimensões da coleta e do tratamento de informações provocaram a multiplicação de apelos à privacidade". Embora uma narrativa pormenorizada das transformações dogmáticas do direito à privacidade ao longo da história não se insira no escopo investigativo desse trabalho, podemos, ilustrativamente, identificar ao menos três momentos paradigmáticos nos quais revoluções tecnológicas impuseram a ressignificação epistemológica do conteúdo normativo (e a remodelagem do âmbito protetivo) do direito à privacidade.

Na segunda metade do século XIX, a câmera fotográfica portátil e os tabloides de fofocas (a chamada *Yellow Press*) passaram a expor, de forma jamais concebida, fatos por vezes insólitos da vida cotidiana, ganhando a atenção e o entretenimento populares. Samuel Warren, advogado egresso da *Harvard Law School*, incomodado pela circulação pública de notícias sobre sua vida pessoal[45], envolveu Louis Brandeis (que, mais tarde, tornar-se-ia Juiz da Suprema Corte norte-americana) na elaboração do seminal artigo *The Right to Privacy*, advogando em favor do reconhecimento da privacidade como bem jurídico a ser protegido pelo Direito norte-americano. De acordo com Doneda (2021, p. 30), o trabalho representa o marco fundacional da doutrina moderna do direito à privacidade.

Referiam Warren e Brandeis (1890, p. 196) que "iniciativas e invenções modernas, através de invasões de sua privacidade, sujeitaram-no [o homem] a dor e sofrimento mentais, muito maiores do que aqueles que poderiam ser infligidos pela mera lesão corporal" (tradução nossa). Ao delimitar-se um âmbito indevassável da vida particular, decorrente de um princípio geral do *common law*[46], os autores atribuíam ao conteúdo dogmático da privacidade um aspecto

[45] "A gênese do projeto parece ter vindo, em vez disso, da 'profunda aversão' de Warren por fofocas nas páginas sociais dos jornais de Boston sobre sua vida social, particularmente relacionadas à sua esposa e compromissos sociais domésticos. Essas fofocas podem parecer brandas pelos padrões modernos, mas feriram as sensibilidades de Warren o suficiente para que ele alistasse Brandeis no projeto, que eles concluíram durante o outono." (Richards, 2010, p. 1302, tradução nossa)

[46] "O *common law* assegura a cada indivíduo o direito de determinar, ordinariamente, em que extensão seus pensamentos, sentimentos e emoções devem ser comunicadas a outros. Sob nosso sistema de governo, ele nunca pode ser compelido a expressá-los (exceto quando no banco das testemunhas); e mesmo se ele tiver escolhido expressá-los, ele geralmente retém o poder para fixar os limites da publicidade que deverá ser dada a eles." (Warren; Brandeis, 1890, p. 198, tradução nossa)

essencialmente excludente[47]: o direito a ser deixado só (*the right to be let alone*). Ademais, propunham, como mecanismo de tutela jurídica da privacidade, a possibilidade de responsabilização civil de veículos de imprensa visando à reparação por danos emocionais e psicológicos causados pela divulgação indevida de informações privadas.

Evidentemente, a circulação de notícias não era novidade; todavia, a publicação de aspectos da vida privada e o registro fotográfico instantâneo, por meio do qual se poderia – com facilidade sem precedentes – captar e fazer circular imagens do cotidiano da vida burguesa nas mais diversas situações, redimensionaram as fronteiras entre os acontecimentos públicos e privados[48], a ensejar a necessidade de se definir, à luz do Direito, o que constitui a vida privada (e, portanto, o âmbito de proteção do direito à privacidade). Como observa Richards (2010, p. 1304), "[a]s velhas normas de deferência e respeito pareciam estar sob ataque, e havia grande ansiedade entre as elites interessadas em proteger seu status, autoridade e privacidade" (tradução nossa).

Entretanto, "por mais que a imprensa ainda imponha uma ameaça à privacidade, e a fotografia tenha se tornado uma ferramenta indispensável do jornalismo [...] existem agora muitas ameaças adicionais à privacidade [...]" (Solove, 2004, p. 58, tradução nossa). De fato, em meados do século XX (no pós-Segunda Guerra Mundial), o advento da computação viabilizou a digitalização da informação[49] – que passou a ser acessada, organizada e armazenada em bancos de dados (*databases*) – e, com isso, estabeleceu um novo limiar a respeito da proteção ao direito à privacidade[50].

---

[47] "Em seus primórdios, marcada por um individualismo exacerbado e até mesmo egoísta, [a doutrina do direito à privacidade] portava a feição do direito a ser deixado só. A esse período remonta o paradigma da privacidade como uma *zero-relationship*, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais." (Doneda, 2021, p. 30)

[48] "Embora a discussão que eles [Warren e Brandeis] provocaram na comunidade jurídica tenha sido e continue sendo importante, seu aviso ressoa aqui não tanto por suas ramificações legais, mas por sua percepção aguda sobre as maneiras como as novas tecnologias podem perturbar a vida e as práticas sociais a ponto de ameaçar valores morais e políticos. Na época de Warren e Brandeis, os avanços técnicos disruptivos estavam na fotografia, que permitia a captura de imagens de pessoas à distância e sem sua permissão. Combinado com máquinas de impressão eficientes, isso permitiu uma publicação barata e ampla disseminação dessas imagens." (Nissenbaum, 2010, p. 19, tradução nossa)

[49] "O advento de uma sociedade em rede, entretanto, trouxe consigo intensa preocupação sobre as implicações pessoais e sociais de tais bancos de dados – agora, em formato digital, capazes de serem rapidamente procurados, instantaneamente distribuídos e perfeitamente combinados com outras fontes de dados para gerar registros ainda mais abrangentes de atributos e atividades individuais." (Cohen, 2000, p. 1374, tradução nossa)

[50] Como observam Frazão, Carvalho e Milanez (2022, p. 18): "Foi exatamente em virtude dessa preocupação, incrementada pelo crescimento exponencial dos bancos de dados e processos automatizados de tratamento de dados pessoais à época, nos Estados Unidos, que o Congresso americano, em 1960, deixou de aprovar um projeto de lei cujo objetivo principal seria a construção de uma base de dados centralizada no país, o *National Data Center*, sob o fundamento de que a proposta apresentava sérios riscos à privacidade dos cidadãos [...]."

As novas preocupações concentravam-se, sobretudo, no papel dos governos enquanto detentores de vastos repositórios de dados a respeito dos indivíduos, e dos riscos atrelados à vigilância e ao controle estatais narrados no romance de George Orwell. Houve, diante desse cenário, o advento do que a literatura especializada denomina de uma *primeira geração* de leis cujo escopo era o de conter e regular o emprego das novas tecnologias de gerenciamento da informação, evitando-se o acúmulo de dados pessoais e, consequentemente, a concentração desproporcional de poderes nas mãos do Estado. Como refere Bioni (2020, p. 110),

> Naquela época, a saída regulatória foi focar na própria tecnologia que deveria ser domesticada e orientada pelos valores democráticos. Temia-se a emergência da figura orwelliana do Grande Irmão, que poderia sufocar a liberdade do cidadão com uma vigilância ostensiva. Optou-se, então, por controlar a criação desses bancos de dados por meio da concessão de autorizações para o seu funcionamento.

Nessa mesma perspectiva, e de acordo com a observação de Mendes (2020, p. 11), considerando-se o incremento exponencial da capacidade de armazenamento e transmissão de dados pessoais pela tecnologia dos bancos de dados[51], já não "mais importava se as informações coletadas dos cidadãos eram íntimas, privadas ou públicas; tratava-se, antes, dos riscos para a personalidade que poderiam surgir do processamento eletrônico de dados".

A dogmática da privacidade, portanto, já não se estrutura mais sobre a exposição ou o sigilo de aspectos da vida privada e sobre um direito à reparação pecuniária pela intromissão indevida de veículos de imprensa. O âmbito protetivo reclama alargamento, para que se compreendam o acúmulo e o acesso irrestrito aos dados pessoais como perigosos componentes de um grave risco de lesão à própria *personalidade*.

Nesse contexto, no final do ano de 1983, paradigmática sentença proferida pela Corte Constitucional Alemã[52] (*Bundesverfassungsgericht*) anunciava uma virada epistemológica no conteúdo jurídico do direito à privacidade, associando-o fortemente às noções de transparência e de controle individual sobre o fluxo informacional. Cunhou-se, assim, o direito à *autodeterminação informativa*[53] – extraído de uma base normativa que, no Direito alemão,

---

[51] "O advento do computador *mainframe* em 1946 revolucionou a coleta de informações. O computador e a fita magnética permitiram o armazenamento sistemático de dados. À medida que as velocidades de processamento do computador aceleravam e a memória do computador aumentava, os computadores forneciam uma capacidade muito maior de coletar, pesquisar, analisar, copiar e transferir registros." (Solove, 2001, p. 1402, tradução nossa)

[52] Como esclarece Doneda (2021, p. 170): "O estopim da sentença foi a própria lei que organizava o censo, aprovada em 1982. Esta lei previa que cada cidadão deveria responder a 160 perguntas, a serem posteriormente submetidas a tratamento informatizado."

[53] "O direito à autodeterminação informativa confere ao indivíduo o poder de, em princípio, determinar por si próprio a revelação e o uso de seus dados pessoais. Indivíduos têm o direito de decidir, eles próprios, se e como seus dados pessoais deverão ser divulgados e usados, em outras palavras: um direito à autodeterminação sobre o processamento de dados referentes a eles." (Albers, 2014, p. 218, tradução nossa)

dava sustentação ao direito geral da personalidade (*allgemeines Persönlichtkeitsrecht*) –, atribuindo-se aos cidadãos o protagonismo na contenção do uso abusivo de dados pessoais. Com isso, foram concebidos direitos e garantias específicas de controle como mecanismos de defesa de liberdades individuais contra as assimetrias informacionais (e, bem assim, de poderes) entre os cidadãos e o Estado, que havia se tornado capaz de compilar informações e formar *dossiês* sobre qualquer indivíduo. Na síntese de Mendes a respeito da sentença (2020, p. 11),

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

Nessa perspectiva, os *dados pessoais* ganhariam centralidade na discussão a respeito da tutela jurídica da privacidade[54]. O vetor hermenêutico da proteção da privacidade não reside mais (apenas) na corporeidade do indivíduo, no binômio segredo-exposição, relacionando-se agora aos próprios dados a seu respeito, enquanto expressões virtuais de sua subjetividade que passam a ser *coletáveis*, *processáveis* (para que gerem informações[55]) e *armazenáveis* em grandes bancos de dados. O âmbito de proteção do direito à privacidade se dilata ao se reconhecer a capacidade de controle do sujeito sobre o *fluxo de informações* atinentes a si próprio[56].

Mais do que isso, estabelece-se uma cisão hermenêutica entre o direito à privacidade e o direito à proteção de dados pessoais (e não uma *evolução* de um rumo a outro[57]). A privacidade, decorrente de um direito fundamental à personalidade, ganha uma *dimensão dinâmica*, passando a ser vista como "um espaço a ser construído *a posteriori* e dinamicamente

---

[54] "A temática da privacidade passou a se estruturar em torno da informação e, especificamente, dos dados pessoais. Esta guinada, que plasmou o próprio conteúdo do termo privacidade, pode ser verificada com clareza nas construções legislativas e jurisprudenciais sobre o tema nos últimos 40 anos [...], assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional Alemão e a Diretiva 95/46/CE da União Europeia, com todas as suas consequências." (Doneda, 2021, p. 177)

[55] Dado pessoal e informação são conceitos intimamente relacionados e, muito embora utilizados como sinônimos pela LGPD (art. 5º, I), não têm o mesmo significado. De modo simples, dado pessoal é o elemento primordial necessário para a geração da informação. Como leciona Frazão (2019, p. 336), "os dados importam, do ponto de vista econômico, na medida em que podem ser convertidos em informações necessárias ou úteis para a atividade econômica". Dado pessoal, portanto, é a partícula fundamental a partir da qual se gera informação sobre alguém, por meio de técnicas como análise e agregação.

[56] "Talvez seja possível traçar um esquema deste processo, ressaltando que parece cada vez mais frágil a definição de 'privacidade' como 'o direito a ser deixado só', que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito." (Rodotà, 2008, p. 24)

[57] Bioni (2020, p. 95) aponta, com acerto, que defender a ideia de "que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma construção dogmática falha que dificulta a sua compreensão".

mediante o controle das informações pessoais" (Bioni, 2020, p. 94). A proteção de dados pessoais, por outro lado, autonomiza-se e assume expressão mais ampla[58], dissociada da liberdade negativa que se pauta pela dicotomia *público versus privado*, extraindo-se de seu conteúdo jurídico-dogmático salvaguardas do indivíduo contra danos[59] e ameaças decorrentes do autoritarismo estatal, que põem em risco a autonomia, a liberdade e a igualdade[60]. Na conhecida síntese de Rodotà (2008, p. 93), "pode-se dizer que hoje a sequência quantitativamente mais relevante é 'pessoa-informação-circulação-controle', e não mais apenas 'pessoa-informação-sigilo', em torno da qual foi construída a noção clássica de privacidade".

O terceiro momento paradigmático em que a inovação tecnológica impôs novas reflexões sobre a dogmática da proteção à privacidade é o que Zuboff (2015, p. 75) identifica como a gênese do *capitalismo de vigilância* (*surveillance capitalism*), advindo da disseminação do acesso às tecnologias de informação e comunicação – e, com elas, as plataformas digitais – , num contexto em que agentes econômicos passaram a se orientar por uma lógica de mercado pautada na extração massiva de dados pessoais dos usuários das interfaces digitais.

Foi a lógica econômica desenvolvida pelo *Google* que inaugurou esse novo modelo comercial baseado na extração e comercialização de informações a respeito do comportamento dos indivíduos. Tal processo de criação é bem sintetizado por Zuboff (2015, p. 85):

> O Google entendeu que se fosse para capturar mais desses dados [pessoais], armazená-los, e analisá-los, eles poderiam afetar substancialmente o valor dos anúncios. Conforme as capacidades do Google nessa arena se desenvolveram e atraíram níveis históricos de lucro, ele produziu práticas sucessivamente ambiciosas que expandiram a lente dos dados do comportamento virtual anterior para o comportamento atual e futuro. Novas oportunidades de monetização são então associadas a uma nova arquitetura global de captura e análise de dados que produz recompensas e punições voltadas a modificar e comodificar o comportamento por lucro.

---

[58] Discutindo a autonomização do direito à proteção de dados pessoais com relação à mera defesa da privacidade, no contexto da economia movida a dados, Frazão (2019b, p. 341) pondera que "[...] a utilização dos dados deixa de se restringir apenas à questão da privacidade e passa necessariamente a envolver outras discussões, como o direito de não ser julgado ou categorizado para determinados fins ou o direito de não ser julgado ou categorizado com base em determinados critérios."

[59] "O dano, aqui, não repousa na exposição de comportamentos anteriormente privados à observação pública, mas na dissolução dos limites que separam esferas de comportamento diferentes uma da outra. O universo de todas as informações sobre todos os comportamentos geradores de registros cria uma 'foto' que, em alguns sentidos, é mais detalhada e íntima do que a produzida pela observação visual, e aquela foto é acessível, em teoria e às vezes em realidade, a basicamente qualquer um que queira vê-la. Em tal mundo, devemos todos ser mais cautelosos." (Cohen, 2000, p. 1425, tradução nossa)

[60] "Há [...] uma série de liberdades individuais, atreladas ao direito à proteção dos dados pessoais, que não são abraçadas pelo direito à privacidade. Além disso, o centro gravitacional da proteção dos dados pessoais é diferente do direito à privacidade – *i.e*., a percepção de que a sua tutela jurídica opera fora da dicotomia do público e do privado." (Bioni, 2020, p. 96)

Efetivamente, ao final da segunda metade do século XX, os ganhos exponenciais de rapidez e eficiência na produção, transmissão e armazenamento de informações fez com que os computadores pessoais (a partir dos quais se seguiu, com o avançar dos anos, uma miríade de outros dispositivos, dos *pagers* aos *wearables*) assumissem função central na vida cotidiana e na exploração das atividades econômicas. A Internet reconfigurou as formas pelas quais o conhecimento é produzido, *indexado*[61], acessado e disseminado. O cotidiano dos usuários foi invadido pelas novas tecnologias de informação e comunicação, com seus inegáveis benefícios para a realização das mais diversas tarefas. Assim, no contexto do capitalismo de vigilância, redesenharam-se mais uma vez os contornos dogmáticos até então conhecidos e atribuídos ao direito à privacidade.

Nesse contexto, o uso massivo dessas novas tecnologias rendeu ensejo à concepção da lógica econômica pautada na comodificação dos dados pessoais dos usuários das interfaces digitais surgidas com o acesso à Internet. Formulários de inscrição, históricos de navegação, registros de buscas, endereços *IP*, taxas de cliques, tempo de visualização, todos são exemplos de dados aparentemente irrelevantes, mas, na verdade, valiosos sobre o comportamento individual (ou, como denominadas por Zuboff, excedente comportamental – *behavioral surplus*) no ciberespaço. Como ensina Frazão (2019, p. 30), cuida-se da exploração ilícita de um ativo que, contudo, veio justificada de uma lógica de *trade-off* entre novas funcionalidades e inovação, de um lado, e acesso aos dados pessoais, de outro:

> [...] tal modo de proceder sempre foi acompanhado de justificativas relacionadas às eficiências geradas e aos benefícios e vantagens que, de maneira 'gratuita' ou acessível, são disponibilizados aos usuários, os quais muitas vezes não percebem que, ao 'pagarem' pelos serviços com seus dados pessoais, são o verdadeiro produto nesse tipo de negócio.

Esse, portanto, o desenho geral – em que iremos nos aprofundar adiante – do paradigma vigente na atual quadra da História, em que o uso das interfaces digitais se tornou essencial à vida moderna. Na precisa síntese de Véliz (2021, p. 61), "[u]ma vez que as plataformas digitais se tornaram indispensáveis para nós, um imperativo para ser um participante pleno em nossa sociedade, não havia chance alguma de optar pela não coleta de dados".

---

[61] A lógica de funcionamento do Google revolucionou, à época, o modo de organização e pesquisa de informações na Internet. Como narra Lastowka (2008, p. 1337), a partir do PageRank, o buscador passou a classificar os resultados de busca de acordo com sua relevância (considerada, para tanto, a quantidade de acessos à página). Diz o autor: "A aplicação do PageRank aos resultados de busca permitiu que as páginas da Web mais populares flutuassem ao topo dos resultados de busca do Google. Combinado com técnicas de análise de links, o PageRank tornou os resultados de busca do Google perceptivelmente melhores e permitiu que os usuários obtivessem resultados mais relevantes em resposta aos seus termos de busca." (tradução nossa)

A sofisticação das técnicas de tratamento das informações no ambiente digital atingiu um novo patamar com o emprego disseminado do algoritmo, definido por Lage (2021, p. 37) como "o processo ou conjunto de regras a serem seguidas em cálculos ou outras operações de solução de problemas, especialmente, por um computador". O aperfeiçoamento da solução de problemas por algoritmos, intrinsecamente relacionado ao desenvolvimento da inteligência artificial, viabilizou o surgimento de um cenário em que, cada vez mais, o poder e a autoridade vêm se expressando por meio do uso dos ditos algoritmos (que, por sua vez, se utilizam dos dados pessoais para cálculos e predições). Como leciona Pasquale (2016, p. 21),

> [...] não podemos nos esquecer de que o acesso aos dados é apenas o pequeno e o menor passo em direção à justiça em um mundo de pontuações digitais invasivas, em que muitas de nossas atividades diárias são processadas como 'sinais' de recompensas ou penalidades, benefícios ou ônus. Decisões críticas não são tomadas com base nos dados *per se*, mas com base nos dados analisados *algoritmicamente*: isto é, em cálculos codificados em softwares de computador." (Tradução nossa)

É nessa perspectiva que Balkin (2017, p. 11) cogita da formação de uma *sociedade algorítmica*, "organizada em torno de tomadas de decisões sociais e econômicas por algoritmos, robôs e agentes de IA; que não apenas tomam as decisões, mas também, em alguns casos, as cumprem" (tradução nossa). A sociedade algorítmica é marcada pelo emprego disseminado e cotidiano de tecnologias de informação e comunicação pelos indivíduos, como estruturas essenciais[62] a uma lógica econômica amparada na *extração massiva* de dados pessoais (na expressão de Zuboff[63]), necessária ao abastecimento de sofisticados sistemas automatizados de tomada de decisões que podem, inclusive, referir-se a aspectos existenciais da vida humana[64].

Considerado o cenário atual, vê-se que o mundo retratado em *1984* de fato não se amolda tão adequadamente aos desafios à privacidade – e, para além disso, à liberdade humana – havidos na sociedade algorítmica. Ao contrário do que se passava com Winston Smith, o quadro

---

[62] "[...] está-se diante de um novo ambiente de mercado, caracterizado pela 'digitalização de praticamente tudo', no qual a informação constitui um dos bens mais valiosos para a agregação de valor a produtos e serviços, o que vem dispensando estruturas, empregados e procedimentos burocráticos que outrora eram o cerne da organização empresarial." (Frazão, 2018, p. 651)

[63] "O capitalismo industrial transformava as matérias-primas da natureza em mercadorias, já o capitalismo de vigilância reivindica o material da natureza humana para a feitura de uma mercadoria nova. Agora é a natureza humana que é raspada, arrancada e tomada para o projeto de mercado de um novo século. É ofensivo supor que esse dano possa ser reduzido ao fato óbvio de que usuários não recebem pagamento algum pela matéria-prima que fornecem. Essa análise é uma façanha de má orientação usada para institucionalizar um mecanismo de precificação, e, portanto, legitimar a extração do comportamento humano para fins de manufatura e venda. Ela ignora o ponto-chave de que a essência da exploração, aqui, é a utilização de nossa vida como dados comportamentais para o aperfeiçoamento do controle de outros sobre nós." (Zuboff, 2020, p. 115)

[64] "Com efeito, os perfis são utilizados para decisões que, para a maioria dos cidadãos, são mais frequentes e, no mais das vezes, mais significativas do que as judiciais ou administrativas, e que são aquelas que dizem respeito ao cidadão consumidor ou usuário de serviços (comerciais, bancários, e assim por diante): tal preocupação aliás encontra-se na lei francesa, que amplia a proibição também às decisões 'privadas'." (Rodotà, 2008, p. 115)

atual é marcado por uma hipervigilância velada e encoberta pelo discurso a respeito dos benefícios e das funcionalidades proporcionadas pelas diversas interfaces digitais (ao contrário da figura centralizadora do Grande Irmão). Tecnologias que envolvem a extração massiva de dados pessoais não são temidas, mas desejadas pelos usuários. Como bem observa Camargo (2021, p. 1), a *teletela* dos dias atuais é por nós carregada "em nossos bolsos de forma deliberada, consentida e até mesmo alegre e divertida".

No romance de Orwell, as ameaças à privacidade e à liberdade são essencialmente representadas pela vigilância, que envolve o *risco* de que informações e opiniões pessoais dissidentes dos interesses do Partido sejam conhecidas por seus integrantes (do que poderão advir, como consequências individuais, a tortura, a prisão, ou mesmo a morte).

Além disso, em *1984*, "o protagonista Winston conseguia escapar, em certos momentos, da vigilância operada pelo Grande Irmão" (Bioni, 2020, p. 133). Na sociedade algorítmica, contudo, não lidamos com apenas *uma* tecnologia ou dispositivo (em *1984*, a *teletela*), mas com uma miríade de recursos utilizados para captar (ou disputar) a atenção e armazenar a informação humana relacionada às mais diversas situações do cotidiano. Como vimos, dados são os *inputs* empregados no aperfeiçoamento de algoritmos; são a matéria-prima indispensável às inúmeras tomadas de decisões automatizadas a que nos sujeitamos, que vão do próximo conteúdo a ser visualizado ao acesso ao crédito, a uma vaga de emprego ou a um seguro de vida.

Daí porque o contexto da sociedade algorítmica mais bem se assemelha à narrativa de Franz Kafka em O Processo. Como argumenta Solove (2001, p. 1399), o romance kafkiano "retrata uma burocracia indiferente em que indivíduos são peões, sem saber o que está acontecendo, sem ter voz ou capacidade de exercer controle significativo sobre o processo" (tradução nossa). Em O Processo, narra-se a história de Josef K., subitamente acusado de ter cometido um crime sobre o qual os agentes da burocracia estatal nada sabem. Tampouco o protagonista compreende a natureza e a razão de sua acusação. Diante disso, Josef K. se vê desorientado frente à burocracia do Estado e progressivamente angustiado em razão da tramitação de um processo desconhecido e da potencial aplicação de uma pena que se aproxima. Nada se sabe, exceto pela existência de um dossiê a respeito de K. e de um tribunal que profere decisões que poderão repercutir gravemente sobre a sua própria vida.

O cenário retratado por Franz Kafka revela a completa falta de capacidade e de poder de K. de interferir no processo em que é acusado, e de compreender as razões por trás das decisões tomadas a seu respeito. Revela, também, a opacidade representada por uma burocracia labiríntica que agrava, ainda mais, a vulnerabilidade do sujeito da ação estatal, interditando por

completo o acesso à informação (K. desconhece *o que* se sabe a seu respeito, assim como *quem* sabe). Nessa perspectiva, Kafka nos demonstra como a informação está intrinsecamente associada ao exercício do poder.

As diferenças entre os cenários distópicos criados por Orwell e Kafka nos ajudam a notar que a dimensão das ameaças a que hoje estão sujeitos os indivíduos é muito maior do que as que decorrem da vigilância estatal percebida por Winston. Em *1984*, o Grande Irmão é o claro opositor dos ideais de liberdade que o protagonista passa a nutrir, ao passo que em O Processo sequer se sabe quem decide e o que se decide. Em *1984*, Winston compreende que seu encarceramento e tortura se devem à sua subversão. Em O Processo, Josef K. apenas se sujeita aos efeitos da sentença, sem sequer saber que crime cometera.

A partir da sujeição de Josef K.[65], presente na obra de Kafka, podemos traçar um paralelo para compreender que regimes jurídicos de proteção de dados pessoais baseados na atribuição do poder de controle aos indivíduos podem produzir efeitos contrários ao esperado empoderamento frente às assimetrias informacionais e de poder com relação a empresas e governos (de que trataremos no Capítulo 3), colocando-se em xeque o paradigma da racionalidade da conduta humana. Segundo Hartzog e Solove (2024, p. 1034):

> Dar mais controle aos personagens de Kafka não os salvará. Eles não são forçados a seus destinos; eles frequentemente participam ativamente de sua própria ruína. Para a privacidade, os mesmos fenômenos estão ocorrendo. As pessoas prontamente "consentem" com a coleta e uso indiscriminado e generalizado de seus dados. Às vezes, isso ocorre porque as empresas exploram e enganam as pessoas para que se submetam. Mas, muitas vezes, as empresas podem simplesmente induzir, instigar ou seduzir as pessoas para os comportamentos que geram lucro, o que frequentemente envolve pessoas expondo seus dados ao máximo. As histórias de Kafka dão a lição de que as pessoas ainda podem ser destituídas de poder mesmo quando as empresas não ajam maliciosamente. Quando recebem poder, as pessoas frequentemente o devolvem imediatamente. [...]. Se as pessoas recebem direitos de propriedade sobre seus dados, as empresas as induzem a negociar esses direitos em troca de bugigangas. (Tradução nossa)

A sociedade algorítmica se caracteriza, também, pela opacidade existente entre os intrincados mecanismos subjacentes à tomada de decisões e os usuários das plataformas digitais que, involuntariamente, se sujeitam a tais decisões (daí por que Pasquale emprega a metáfora

[65] "[...] em O Processo, Josef K. acredita na legitimidade do sistema de justiça apesar de incontáveis sinais de que ele é ilegítimo – os gabinetes ficam em sótãos em prédios decadentes; os atos judiciais ocorrem em salas de estar decrépitas; o que parecem ser livros de direito não são. A todo momento, o sistema é pouco profissional e até mesmo sucateado. No entanto, Josef K. aceita sua autoridade e se submete voluntariamente ao seu poder – até mesmo a sua própria execução." (Solove; Hartzog, 2024, p. 1033)

da caixa-preta, ou *black box*[66]). O exercício dos direitos atribuídos pelo regime jurídico de proteção de dados pessoais fundado no paradigma do controle pode ser sobremaneira dificultado diante do desenho labiríntico das arquiteturas das plataformas digitais. Aliás, não raro os indivíduos sequer sabem que têm direitos[67]. Mesmo assim, encontram-se sujeitos à autoridade privada exercida pelas plataformas e a decisões cujos fundamentos se desconhecem. Motivados pelo acesso fácil ao entretenimento ou pelas comodidades viabilizadas pelas plataformas, os usuários, no mais das vezes, confiam em que seus dados não venham a ser utilizados em seu próprio detrimento, o que se reforça pelo discurso das empresas.

De todo modo, a participação da vida em sociedade já não dispensa o acesso a tais interfaces e, assim, não há saída que envolva a interrupção do fornecimento (voluntário ou não) de dados pessoais sobre os quais o controle individual é, de várias formas, limitado (retomaremos esse assunto com maior detalhamento no Capítulo 3). Para melhor compreendermos o quadro que caracteriza os desafios impostos à privacidade e à proteção dos dados pessoais na sociedade algorítmica, é oportuno verticalizarmos nossa análise sobre alguns aspectos fundamentais desse contexto, porque fornecem o *pano de fundo* sobre o qual será problematizado o paradigma do controle como aspecto fundante de nosso regime jurídico de proteção de dados pessoais.

1.1 O fenômeno da "dataficação" da vida

O advento da sociedade algorítmica guarda intrínseca relação com a expansão e a disseminação das plataformas digitais. Não se limitando à função de mediadoras do *acesso* a bens e serviços, ditas plataformas são imprescindíveis ao próprio uso de uma miríade de novos dispositivos que, sempre *conectados*, progressivamente vêm substituindo seus equivalentes analógicos[68]. Os *smartwatches* substituem, aos poucos, os relógios analógicos; as *smart TVs* (e

---

[66] "O termo 'caixa-preta' é uma metáfora útil [...], dado o seu significado ambíguo. Ele pode se referir a um dispositivo de gravação, como os sistemas de monitoramento de dados em aviões, trens e carros. Ou pode significar um sistema cujo funcionamento seja misterioso; podemos observar seus inputs e outputs, mas não podemos dizer como um se torna o outro. Nós nos deparamos com esses dois significados diariamente: rastreados cada vez mais de perto por empresas e governo, não temos uma ideia clara do para quão longe essa informação pode viajar, como ela é usada, ou suas consequências." (Pasquale, 2016, p. 3, tradução nossa)

[67] Nesse sentido, a pesquisa Privacidade e proteção de dados pessoais 2023 revela que, em 2023, apenas "24% dos usuários de Internet com 16 anos ou mais buscaram algum canal de atendimento para fazer solicitações, reclamações ou denúncias relacionadas aos seus dados pessoais, resultado igual ao observado na edição de 2021" (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 53). Os resultados sugerem que, mesmo passados alguns anos da entrada em vigor da LGPD, os titulares de dados pessoais ainda não têm dimensão adequada de seus direitos nem tampouco das formas de os exercer.

[68] Matéria veiculada no Jornal O Globo em junho de 2024 repercutiu resultados da Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad) Tecnologia da Informação e Comunicação, realizada pelo IBGE. De acordo com

os serviços de *streaming*) tomam o lugar dos televisores sem conexão à Internet e dos serviços de TV a cabo; *smartphones*, da mesma forma, praticamente transformaram os antigos telefones celulares em peças de antiquário.

De fato, há muito a relação – direta ou indireta – dos indivíduos com interfaces virtuais não mais se limita ao uso do computador pessoal. Os *smartphones*, cujos sistemas operacionais – ao menos os mais largamente utilizados – são desenvolvidos, atualizados e comercializados por grandes corporações do setor tecnológico, tornaram-se verdadeiros computadores de bolso, alterando drasticamente os limites até então conhecidos a respeito do acesso à informação, à comunicação interpessoal, e a bens e serviços, que passa a ocorrer de modo praticamente instantâneo. Como um dos efeitos dessa nova forma de viver, novas gerações colhem as consequências de uma *infância baseada no celular* (Haidt, 2024, p. 139), com suas repercussões sobre o desenvolvimento de habilidades sociais, sobre as formas de se comunicar e de exprimir a sua própria individualidade e, ainda, sobre a saúde mental[69].

Novas modalidades de exploração de atividades econômicas há muito conhecidas – como o transporte individual de pessoas – estruturam-se exclusivamente sobre a lógica do uso das plataformas digitais, por meio das quais são feitas todas as solicitações relacionadas ao oferecimento do serviço. Outras atividades, a seu turno, incorporam tais interfaces como mecanismos aptos ao robustecimento de seus sistemas de segurança, mitigando a falibilidade humana, por exemplo, com o registro e o armazenamento dos dados pessoais em bancos de dados muito mais poderosos do que nossa limitada memória[70]. Nesse sentido, a verificação de identidades, a consulta a registros de eventos passados, a identificação de condutas suspeitas – a partir do confronto com padrões anteriores de comportamento – são possibilidades inerentes a um novo limiar aberto pelo uso de tecnologias digitais.

---

o estudo, houve um crescimento de 17% no número de lares com dispositivos inteligentes em um ano, atingindo-se o patamar de 11,6 milhões de lares com aparelhos *smart*. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2024/08/16/quase-12-milhoes-de-lares-brasileiros-tem-dispositivos-inteligentes-como-alexa-alta-de-17percent-em-um-ano.ghtml. Acesso em: 8 nov. 2024.

[69] "Quando demos smartphones a crianças e adolescentes no início da década de 2010, também demos às empresas a capacidade de aplicar neles esquemas de reforço de razão variável o dia todo, treinando-os como se fossem ratos de laboratório, nos anos mais sensíveis da reconfiguração cerebral. Essas empresas desenvolveram aplicativos viciantes que abriram caminhos muito profundos nos cérebros jovens." (Haidt, 2024, p. 163)

[70] Segundo Zuboff (2020, p. 219), "a capacidade do mundo de produzir informação excedeu de maneira substancial sua capacidade de processar e armazenar informação. Consideremos que a nossa memória tecnológica vem quase dobrando a cada três anos aproximadamente. Em 1986, apenas 1% da informação do mundo era digitalizada e 25% em 2000. Em 2013, o progresso de digitalização e dataficação (a aplicação de software que permite a computadores e algoritmos processar e analisar dados brutos), combinado a novas e mais baratas tecnologias de armazenamento, convertia 98% da informação mundial em formato digital".

Além disso, há novas atividades cujo próprio surgimento se deve ao advento das plataformas: mencionem-se, por exemplo, os aplicativos de relacionamento (*dating apps*), que reconfiguraram[71] o modo como indivíduos buscam (e se relacionam com) potenciais parceiros amorosos. Para além disso, não se pode deixar de mencionar as próprias redes sociais enquanto elementos centrais do convívio social, que, cada vez mais, passa a ocorrer no ambiente virtual[72]. A pandemia causada pelo vírus SARS-CoV-2, entre os anos de 2020 e 2023 (nos quais, respectivamente, a Organização Mundial da Saúde declarou a sua deflagração e o seu fim), catalisou decisivamente o emprego cotidiano de tecnologias da informação e comunicação como saída para a manutenção de atividades econômicas e para viabilizar o contato entre as pessoas durante as medidas de isolamento determinadas pelas autoridades sanitárias[73].

Com efeito, as plataformas digitais têm cada vez mais intensamente se integrado ao tecido social, sendo a *informação* a pedra angular[74] de uma verdadeira revolução cultural e comportamental que estrutura novos modos de vida no século XXI. Na ilustrativa síntese de Richards e Hartzog (2024, p. 1153), "a imagem definidora da nossa moderna sociedade da informação pode muito bem ser a de casais e grupos de amigos sentados a uma mesa de café, de restaurante ou de jantar 'sozinhos juntos', enquanto olham seus smartphones em um silêncio ensurdecedor" (tradução nossa).

---

[71] Interessante estudo de Büyükeren, Makarin e Xiong (2024, p. 1) analisou os impactos do uso do aplicativo Tinder sobre estudantes universitários, salientando que "a ascensão dos aplicativos de namoro foi acompanhada por crescente preocupação pública — vários artigos populares da imprensa vincularam os aplicativos de namoro à ascensão da cultura de pegação, declínio da saúde mental e atividade sexual entre jovens adultos e uma distribuição mais distorcida de correspondências de namoro" (tradução nossa). Dentre as conclusões do estudo, os pesquisadores referem que "as mudanças nas normas de namoro associadas à introdução do Tinder também levaram a maiores incidências de doenças sexualmente transmissíveis, bem como ao aumento da prevalência de agressão sexual" (*Idem*, p. 37, tradução nossa).

[72] Plataformas digitais fazem parte da rotina de grande parte da população brasileira. De acordo com a Pesquisa TIC Domicílios 2023, "84% dos brasileiros com 10 anos ou mais eram usuários da Internet em 2023, o que equivale a aproximadamente 156 milhões de pessoas" (Núcleo de Informação e Coordenação do Ponto BR, 2023, p. 69). Nesse enorme contingente de indivíduos, ainda conforme a pesquisa, nove em cada dez acessaram a Internet para enviar mensagens "por meio de plataformas como WhatsApp, Skype e Facebook Messenger" (2023, p. 81), ao passo que oito em cada dez usuários mais afirmaram utilizar redes sociais "como Facebook, Instagram ou TikTok" (*Idem*, 2023, p. 81).

[73] A pesquisa TIC Domicílios referente ao ano de 2020 revelou importante aumento no uso da internet pelos domicílios brasileiros com a chegada da pandemia. Conforme noticiado no portal Agência Brasil, o percentual de lares com acesso à internet passou, de 71% em 2019, "para 83% no ano passado [isto é, em 2020], o que corresponde a 61,8 milhões de domicílios com algum tipo de conexão à rede". Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais. Acesso em: 8 nov. 2024.

[74] Camargo (2021, p. 2), entretanto, observa: "[...] se a informação foi utilizada para caracterizar o novo contexto da teia social por meio da expressão 'sociedade da informação', hoje este elemento ressignificante tem sua centralidade nos dados. Efetivamente, os dados que circulam pelas redes da sociedade da informação são os grandes responsáveis por uma nova forma de organização econômica, política e social."

Se, por um lado, revelam-se inegáveis os ganhos de eficiência e conforto – de modo geral, um incremento na qualidade de vida – decorrentes da incorporação dessas novas tecnologias ao cotidiano dos indivíduos, por outro, as interações humanas com as interfaces digitais são a fonte primordial de extração do dado pessoal enquanto matéria-prima fundamental à manutenção e ao desenvolvimento do capitalismo de vigilância[75]. Essa matéria-prima constantemente produzida pela interação com as interfaces digitais é, de fato, o "combustível da economia da informação: assim como os motores da Era Industrial [...] funcionavam com óleo, os motores da Era da Informação [...] funcionam com dados" (Richards, 2022, p. 3, tradução nossa).

Assim, a vida humana passa a ser *dataficada*: plataformas digitais convertem toda a experiência individual (coletada inicialmente sob a forma de dados "crus", ou *raw data*) em informações que são lidas por algoritmos capazes de delimitar perfis pessoais e de interpretar, influenciar e predizer o comportamento humano com crescente precisão, gerando valiosos *inputs* que mantêm funcionando as engrenagens do capitalismo de vigilância. Ao definir a dataficação como a "aplicação de *software* que permite a computadores e algoritmos processar e analisar dados brutos", Zuboff (2020, p. 219) dá ênfase ao fato de que dados crus são refinados em informações[76] a partir de técnicas sofisticadas de processamento tornadas possíveis pelo emprego de algoritmos e sistemas de inteligência artificial.

Como se vê, a ocorrência do fenômeno da dataficação da vida relaciona-se intimamente com a percepção do valor comercial havido na coleta, processamento e compartilhamento de dados pessoais. Afinal, viabilizou-se o surgimento de um lucrativo mercado em que a mercadoria comercializada é a certeza sobre comportamentos humanos futuros.

Os dados pessoais ocupam posição de inequívoca centralidade nesse modelo porque são o insumo básico a ser utilizado "para tornar os comportamentos e preferências humanas calculáveis, previsíveis e lucrativos [...] com perfis de compra e de risco probabilisticamente determinados" (Cohen, 2017, p. 21, tradução nossa). Para muito além de informações voluntariamente inseridas em formulários de cadastro ou publicadas em redes sociais, as

---

[75] "À medida que a Internet das coisas conecta mais e mais dispositivos e aparelhos a redes digitais, a vigilância se espalha para cada vez mais recursos de interação diária. Em geral, quanto mais interativo e mais social o serviço, maiores as oportunidades para coleta de dados, análise de dados e tratamento individualizado." (Balkin, 2018, p. 2, tradução nossa)

[76] "Os dados precisam, portanto, ser processados e trabalhados para que possam gerar valor. Se tal constatação não afasta a importância em si dos dados isolados ou 'crus', tem o importante papel de realçar o fato de que o mero acesso a dados, sem a possibilidade efetiva e eficiente de transformá-los em informação, pode ser insuficiente para a obtenção dos respectivos benefícios econômicos." (Frazão, 2019b, p. 337)

plataformas nutrem-se da coleta incessante de dados sobre o próprio comportamento dos indivíduos nos mais diversos ambientes digitais. Segundo Cohen (2017, p. 16), os usuários

> buscam acesso à conectividade social, comercial e cultural que as plataformas fornecem, enquanto os provedores de plataformas buscam acesso aos dados necessários para criar e manter vantagem competitiva em seu(s) campo(s) de intermediação escolhido(s). (Tradução nossa)

De fato, não há informações inúteis no capitalismo de vigilância. Padrões de digitação, erros de grafia, movimentação do cursor, históricos de busca, anúncios visualizados, geolocalização, duração da bateria de dispositivos móveis, comentários, "curtidas", fotos, vídeos, compartilhamentos, dados de saúde (presentes no uso de dispositivos "vestíveis" – *wearables* – como *smartwatches* e medidores de glicemia), todos são dados pessoais gerados e coletados graças à mediação da agência humana no ciberespaço. Esses dados, a que o capitalismo de vigilância se refere como "migalhas digitais" (*digital breadcrumbs*) (Zuboff, 2020, p. 110), são extraídos pelas corporações que implementam e administram as plataformas digitais como matéria-prima gratuita e abundante para o desenvolvimento de seu modelo de negócios.

Acresce que o uso das plataformas digitais, bem como o próprio processo de dataficação da vida, são – como já mencionamos – permeados pelo discurso da modernidade e da inovação, tratando-se a privacidade e os dados pessoais como o preço a se pagar (*trade-off*) pelos inúmeros benefícios práticos (e supostamente gratuitos[77]) das novas tecnologias. Palavras, assim como dados, importam para esse modelo econômico.

O aparelhamento da retórica das *big techs* com eufemismos e neologismos ofusca, aos olhos dos indivíduos, a mecânica que põe em marcha o capitalismo de vigilância, ao passo que reforça os aspectos positivos das plataformas digitais. Na precisa observação de Camargo (2021, p. 86), a linguagem utilizada no contexto das plataformas serve não só "para dar contornos positivos para um sistema de apropriação de bens alheios, mas também como instrumento de afirmação". Como oportunamente observa Zuboff (2020, p. 110),

> [o] Google teve o cuidado de camuflar a importância das suas operações de superávit comportamental em jargão industrial. Dois termos populares — "data exhaust" e "digital breadcrumbs" [migalhas digitais] — aludem a

[77] Diz-se "supostamente gratuitos" com amparo na visão de Camargo (2021, p. 83), que, analisando a dinâmica de funcionamento das plataformas digitais disponibilizadas sem contrapartida financeira, destaca a alta capacidade de processamento de informação, os dados pessoais e a alocação de tempo dos usuários (como mão de obra não remunerada) como meios de produção. E conclui o autor: "Como resultado deste processo produtivo, do lado gratuito, a plataforma entrega conteúdo relevante para os usuários [...]. Já do lado pago, entrega anúncios a usuários mais propensos a converterem aquela exposição à mensagem publicitária em uma ação efetiva em favor do anunciante. [...]. Tudo isso, garantindo-se o rastreamento, ao menos nas ações realizadas na web, e, em alguns casos, por aplicações fornecidas pela própria plataforma."

> resíduos sem valor: restos espalhados que podem ser pegos. Por que permitir que os dados fiquem pairando na atmosfera quando podem ser reciclados e tornados úteis? Quem pensaria em chamar esse processo de reciclagem de exploração, expropriação ou pilhagem? Quem se atreveria a redefinir "data exhaust" como espólio ou contrabando, ou imaginaria que o Google aprendeu como formar de modo proposital a chamada "exaustão" com seus métodos, equipamentos ou estruturas de dados?

No mesmo sentido, Véliz (2021, p. 97), ao comentar os eufemismos disseminados na apologia das plataformas, aduz que "redes privadas de publicidade e vigilância são chamadas 'comunidades', os cidadãos são os 'usuários', o vício em telas é rotulado como 'engajamento', nossas informações mais sensíveis são consideradas 'poeira de dados' ou 'migalhas digitais' [...]". Com efeito, o adequado funcionamento dos modelos de negócio baseados na extração de dados pessoais, a partir da dataficação da vida, é dependente de uma estratégia discursiva capaz de justificar racionalmente (e de incentivar) o uso das plataformas digitais, em geral por seu potencial de simplificação de atividades humanas, de ganho de eficiência e tempo e, evidentemente, por seu apelo ao entretenimento, em suas mais variadas formas.

A lógica da dataficação é relacionada por Zuboff (2020, p. 269) ao fenômeno da "renderização", que designa, em síntese, as práticas operacionais que viabilizam a conversão da experiência humana em dados "crus", ao mesmo tempo em que significa "a forma pela qual a coisa permite se render ao longo do processo, sendo transformada". Esse segundo aspecto da renderização é diretamente associado à lógica discursiva que permeia o discurso da inovação viabilizada pelas plataformas digitais.

Afinal, o uso de plataformas digitais e dispositivos "inteligentes" – capazes de nos fornecer dados, análises e métricas sobre aspectos de nossas vidas que jamais monitoramos (como o tempo total de sono REM[78]) –, estimulado pelas vantagens práticas das novas tecnologias, faz com que os indivíduos voluntariamente entreguem informações cada vez mais detalhadas sobre suas vidas ao escrutínio do capitalismo de vigilância, dataficando-as. Nesse contexto, termos de uso e políticas de privacidade não passam de meros entraves burocráticos a serem vencidos pelos usuários com o apertar de um botão, ou com o preenchimento de um *checkbox*. O que se deseja, afinal, é o acesso à funcionalidade e à comodidade oferecidas pela plataforma. Aliás, a discordância com a forma de tratamento de dados pessoais, não raro, enseja a impossibilidade de uso do *app*. É pegar ou largar.

---

[78] Na definição constante do site do Observatório da Saúde da Criança e do Adolescente, da Faculdade de Medicina da Universidade Federal de Minas Gerais: "É o estágio do sono profundo, no qual corpo repõe as energias do desgaste diário. O organismo libera os hormônios ligados ao crescimento e executa o processo de recuperação de células e órgãos." Disponível em: https://www.medicina.ufmg.br/observaped/fases-do-sono/. Acesso em: 1 nov. 2024.

Essa lógica de funcionamento que dá sustentação e continuidade ao processo de dataficação da vida gera, como subproduto, um modelo que se vem denominando de *economia da atenção* (*economics of attention*), em que levam vantagem os agentes econômicos que sejam capazes de atrair a limitada atenção humana por mais tempo, na medida em que isso viabiliza o desenvolvimento de atividades econômicas baseadas na dataficação. Trataremos desse assunto no tópico seguinte.

1.2 "Queremos te conhecer melhor!": coleta massiva de dados pessoais e hipervigilância na economia da atenção

A limitada atenção humana[79] é um dos ativos mais valiosos para o capitalismo de vigilância. Afinal, o potencial de retenção da atenção dos indivíduos é um critério decisivo para os modelos de negócio baseados na extração massiva de dados pessoais[80]. No contexto do uso das plataformas de redes sociais, por exemplo, os usuários são constantemente bombardeados com conteúdos que podem ser do seu interesse, com convites e incentivos para que revelem mais sobre si próprios (e para que compartilhem suas opiniões), com testes de personalidade, *trends* e outras estratégias voltadas a aumentar o tempo durante o qual se mantêm *online*[81].

As redes sociais são poderosas ferramentas de atração e retenção da atenção individual porque emulam (ao mesmo tempo em que exploram) um dos aspectos mais essenciais da natureza humana: a propensão e a aptidão para formar conexões sociais[82]. O grande potencial de formação de ligações entre indivíduos – conhecidos ou não – que se relacionam entre si por perfis ou opiniões afins viabiliza a formação de grupos de interesses coesos e, consequentemente, o senso de pertencimento e aceitação causados pela ressonância de opiniões

---

[79] "O fato de que ignoramos quase tudo dá um sentido inicial do porquê a atenção é um recurso escasso. Também explica a importância da 'decisão atencional'. Para alocar a atenção, nosso cérebro tem meios pelos quais decide em que fluxos de informação, dentre as várias escolhas, vamos prestar atenção, ou processar. Cientistas descobriram ao menos dois mecanismos diferentes para tomar essas 'decisões atencionais'. Há um mecanismo involuntário, localizado nas partes inferiores do cérebro, e um mecanismo voluntário, cujo funcionamento depende das partes superiores do cérebro." (Wu, 2019, p. 781, tradução nossa)

[80] "[...] o apetite voraz do Facebook por dados não é saciado pelas informações que nós ativamente revelamos; ele também varre dados de nossos cliques, aplicativos de terceiros, comportamento de navegação na Internet, e nossas interações com seus parceiros e anunciantes." (Waldman, 2016, p. 194, tradução nossa)

[81] "Elas [as redes sociais] ganham seu dinheiro encorajando enormes números de pessoas a gastar tanto tempo quanto possível em suas plataformas e produzir enormes quantidades de conteúdo, mesmo que essa contribuição seja algo básico como comentar, curtir, ou repetir a contribuição de outra pessoa." (Balkin, 2018, p. 2, tradução nossa)

[82] Ao discutir as causas da Revolução Cognitiva, Harari (2020, p. 34) afirma que uma das teorias sobre o desenvolvimento da linguagem do *homo sapiens* se apoia na necessidade que a espécie tem de compartilhar informações sobre o mundo à sua volta. Segundo o autor: "[...] a informação mais importante que precisava ser transmitida era sobre humanos, e não sobre leões e bisões. Segundo essa teoria, o Homo Sapiens é em essência um animal social. A cooperação social é fundamental para a sobrevivência e a reprodução."

e por *feedbacks* positivos (como "curtidas" ou compartilhamentos) a respeito de experiências e relatos individuais[83].

Um dos principais elementos da discussão acerca da economia da atenção no contexto das plataformas digitais é o conceito de *engajamento*. Na compreensão de Richards e Hartzog (2024, p. 1155), trata-se de um conjunto de "ações que encorajam as pessoas a gastar mais tempo, atenção, ou esforço de uma forma que desproporcionalmente beneficia a parte que estimula o engajamento e onera o engajado" (tradução nossa). A definição dada pelos autores[84] coloca em evidência uma *assimetria* de poderes entre uma parte – as plataformas digitais, dito de modo amplo – que detém conhecimento para implementar estratégias capazes de capturar e reter a atenção humana, e outra, sobre quem se exerce o engajamento (o usuário), que reúne apenas uma quantidade limitada e valiosa de atenção.

Nesse contexto, é importante a referência à lição de Wu (2019, p. 784), ao ponderar que "uma das mais importantes, embora menos compreendidas mudanças [da última meia década] foi um melhor entendimento da ciência da atenção, junto com os modelos de negócio que não dependem da venda de bens ou serviços, mas da revenda da atenção" (tradução nossa). Como se pode perceber, a disputa pela atenção humana compõe parcela significativa dos interesses das empresas que exploram plataformas digitais, na medida em que a sua verdadeira clientela não são os usuários, mas, sim, os anunciantes interessados em trazer bens e serviços à atenção dos indivíduos. As plataformas digitais são a tecnologia utilizada pelos corretores de atenção[85].

A lógica da coleta massiva de dados pessoais se conecta com a dataficação – numa relação de causa e efeito – e, consequentemente, com o desenvolvimento de modelos de negócio estruturados sobre a atenção humana. Afinal, uma vez coletadas – pelos mais diversos

---

[83] "No início da década de 2010, os sistemas de 'networking' social que haviam sido (majoritariamente) estruturados para conectar pessoas se transformaram em 'plataformas' de rede social, repensadas (majoritariamente) para incentivar performances públicas de um para muitos em busca de validação não só de amigos, mas de desconhecidos. Até usuários que não publicam ativamente são afetados pelas estruturas de incentivo desses aplicativos." (Haidt, 2024, p. 142)

[84] Richards e Hartzog (2024, p. 1158), contudo, ressalvam outros dois usos correntes do termo engajamento: "O primeiro é como uma medida técnica da interação de uma pessoa com um serviço. O segundo é enquanto uma ideologia – um conjunto de objetivos e estratégias para aumentar a métrica técnica e para justificá-la como um bem virtuoso. A ideologia econômica do engajamento é o produto de um modelo de negócios que prioriza a extração e a exploração da informação, atenção e trabalho humanos para ganhos financeiros e outros." (tradução nossa)

[85] Ainda segundo Wu (2019, p. 787): "Em sua forma mais pura, esses negócios [da economia da atenção] dependem unicamente da revenda da informação para fazerem dinheiro. Exemplos de puros Corretores de Atenção incluem negócios como redes de TV aberta, jornais gratuitos, e muitas das companhias na World Wide Web, como Facebook ou Google. Em termos econômicos, o Corretor de Atenção pode ser descrito como uma versão especializada de um intermediário de plataforma em um mercado de dois lados. Na literatura em que são pioneiros os economistas Jean-Charles Rochet e Jean Tirole, um intermediário de plataforma é uma empresa que une compradores e vendedores de dois mercados separados e facilita as suas transações." (tradução nossa)

dispositivos e plataformas –, as experiências humanas não são apenas convertidas em dados pessoais (em sua forma "bruta"), mas refinadas e utilizadas na formação de perfis comportamentais que podem ser conhecidos, interpretados e manejados de forma a potencializar a efetividade da estratégia de engajamento[86]. Na oportuna síntese de Véliz (2021, p. 154): "Quanto mais comentários as pessoas fazem sobre o que os outros compartilham, mais cliques, mais anúncios, mais dinheiro, mais poder".

Na economia da atenção, tampouco se pode desprezar a importância da própria arquitetura das plataformas digitais, projetadas para serem viciantes. A partir de estudo empírico conduzido por Woolley e Sharif (2022), as pesquisadoras identificaram três fatores que influenciam a permanência das pessoas nas redes sociais: "a quantidade de conteúdo que a pessoa já viu, a similaridade do conteúdo que já viram, e a forma pela qual elas viram o conteúdo". No ponto que nos interessa, as autoras concluem:

> Esses resultados também esclarecem por que é tão fácil se distrair com aplicativos como Instagram ou YouTube no trabalho. Essas plataformas são projetadas para prender os espectadores em uma toca de coelho de mídia social: elas oferecem conteúdo do tamanho de uma mordida [*bite-sized*] que facilita o consumo rápido de vários vídeos ou postagens em sequência, geralmente sugerem conteúdo semelhante automaticamente e muitas delas até começam a reproduzir vídeos semelhantes automaticamente, reduzindo o potencial de interrupções. Embora apresentar aos usuários conteúdo envolvente não seja necessariamente algo ruim, a acessibilidade dessa mídia é exatamente o que torna tão difícil para os usuários se libertarem da toca de coelho e voltarem ao que estavam fazendo. (Tradução nossa)

Nesse contexto, a vulnerabilidade havida no engajamento não se revela apenas pela sujeição dos usuários às empresas que detêm aptidão para definir e implementar, unilateralmente, as técnicas de retenção da atenção humana. Mais do que isso, evidencia-se também a partir da potencial manipulação e instrumentalização da atenção, na medida em que o conhecimento pormenorizado sobre características, vieses, heurísticas, interesses, medos e aversões individuais viabiliza a implementação da estratégia de engajamento a partir de um juízo de *certeza*. A estreita relação entre atenção e poder é bem captada por Hawley (2023, p. 84), ao analisar o contexto norte-americano:

> Toda essa atenção e todo esse dinheiro deram a essas plataformas algo mais. Poder. Um poder inaudito na vida americana. Nenhuma outra corporação no mundo tinha sido capaz de controlar seus clientes como essas corporações, de

[86] "Frequentemente, o que mais envolve as pessoas é o material que produz fortes reações emocionais – mesmo que seja polarizador, falso ou demagógico. As empresas têm incentivos econômicos para expor as pessoas a esse material. E atores inescrupulosos, tanto nacionais quanto estrangeiros, aprenderam a tirar vantagem desse recurso das mídias sociais. Como resultado, o mesmo modelo de negócios que permite que as empresas maximizem as receitas de publicidade também as torna condutoras e amplificadoras de propaganda, de teorias da conspiração e de notícias falsas." (Balkin, 2018, p. 3, tradução nossa)

> invadir seus cérebros, observá-los, rastreá-los, predizer seu comportamento e moldá-lo. Isso era um poder sem precedentes conquistado sem consentimento ou permissão significativa de qualquer tipo. E estava nas mãos de alguns poucos – os fundadores, acima de tudo, os Zuckerbergs, Larry Pages e Sergey Brins deste mundo, e sua trupe de executivos.

Portanto, razão assiste a Frazão (2024, p. 9) ao notar que abordagens baseadas em um extremo conhecimento a respeito dos indivíduos "se aproveitam das vulnerabilidades e fragilidades dos usuários, muitas vezes os induzindo a estados mentais extremos, estimulando o vício na conectividade ou explorando suas fraquezas ou mesmo o seu subconsciente". De fato, os *corretores de atenção* da sociedade algorítmica são capazes de segmentar públicos de modo extremamente preciso e, a partir da coleta massiva de dados pessoais, direcionar a atenção para onde quiserem (inclusive para fins de produção e coleta de mais dados pessoais). Como bem observam Richards e Hartzog (2024, p. 1160),

> Outro motivo pelo qual as empresas podem querer aumentar as métricas de engajamento é que interagir com aplicativos, sites e dispositivos fornece uma rica fonte de informações pessoais a serem coletadas para criação de perfis e lucro. O Facebook costumava ter apenas uma opção "Curtir" se você quisesse interagir com uma publicação sem deixar um comentário. Então, ele lançou mais cinco opções, como "Amei", "Triste" e "Bravo". Esse ajuste de engenharia deu aos clientes humanos do Facebook mais cinco caminhos para engajamento, e cinco maneiras mais sutis de criar um perfil do que as pessoas gostam, do que não gostam e de que maneiras. Além de servir como um tempero adicional para a máquina de experiência viciante, essas técnicas são maneiras úteis de criar mais dados. (Tradução nossa)

Balkin (2018, p. 2) identifica uma "grande barganha" feita pelas redes sociais aos usuários, caracterizada essencialmente pela oferta *gratuita* de serviços de comunicação, e de suas vantagens, em troca da coleta e análise massivas de dados pessoais gerados pelo uso das plataformas. Nessa dinâmica, a conectividade ubíqua e o uso contínuo de plataformas digitais proveem um fluxo constante de informações sobre os usuários às empresas que exploram ditas plataformas, causando-se uma espécie de retroalimentação que gera, como subproduto, graves assimetrias informacionais (de que trataremos no tópico a seguir). Em suma, como bem nota Frazão (2018, p. 643), "qualquer que seja o objetivo principal de uma plataforma eletrônica [...] ela tem como negócio subjacente a coleta e a análise dos dados dos seus usuários, seja para utilizá-los em seu próprio favor [...], seja para negociá-los com outros parceiros comerciais".

Daí a se utilizar, mais recentemente, neologismo que designa a vigilância baseada na coleta massiva de dados pessoais: *dataveillance*. O incremento tecnológico que tornou possível a coleta e o armazenamento de informações em quantidades sem precedentes na história viabilizou o surgimento de um cenário de hipervigilância, justificada pela retórica que coloca em evidência as conveniências que as plataformas digitais podem oferecer a seus usuários, por

mais que a indústria de dados tenha "se alicerçado em um ativo que não é dela – os dados pessoais – e que, muitas vezes, tem sido explorado de forma ilícita" (Frazão, 2019, p. 40).

A *hipervigilância* se distancia da vigilância descrita em *1984* na medida em que já não mais se limita a um dispositivo identificável e situado em um espaço conhecido e determinado, como as *teletelas* (ou como as câmeras fotográficas portáteis, que motivaram o trabalho de Warren e Brandeis). A hipervigilância tem lugar a partir do uso das plataformas digitais, de dispositivos conectados à internet, das câmeras de reconhecimento facial em espaços públicos ou privados, e até mesmo de dispositivos capazes de coletar dados sobre a atividade cerebral[87].

Distingue-se, também, pelo fato de estar associada ao já mencionado discurso sobre a inovação, a disrupção e a eficiência gerada pelo uso de tecnologias digitais nos mais variados aspectos da vida humana, o que coloca sob penumbra os efeitos deletérios da extração massiva de dados pessoais, como a geração de assimetrias informacionais e o agravamento da vulnerabilidade dos indivíduos com relação às plataformas. Na interessante e ilustrativa síntese de Balkin (2018, p. 3), a relação entre plataformas digitais e usuários se estrutura sobre a seguinte dinâmica:

> Nós daremos a você habilidades milagrosas. Nós daremos a você redes sociais que permitem que você se conecte com qualquer pessoa, em qualquer lugar, a qualquer momento, em uma fração de segundo. Nós daremos a você mecanismos de busca que encontram qualquer coisa que você esteja procurando instantaneamente. Nós daremos a você novas formas de entretenimento que são imersivas, envolventes, ultrajantes e divertidas. Nós daremos a você ainda mais formas de se medir e se expressar para os outros.
>
> Nós daremos tudo isso a você, de graça! E em troca, você nos deixará te vigiar. Você nos deixará coletar e analisar seus hábitos, suas localizações, suas ligações, seus contatos com seus amigos, seus cliques, sua digitação, tudo o que pudermos medir. Nós alegremente vamos pegar tudo isso e estudar, e fazer inferências disso, e monetizar isso, para que possamos dar a você todas essas coisas milagrosas. E nós vamos usar esses dados para realizar experimentos com você para entender como te manter ainda mais focado em nossos sites e produtos, para que você possa produzir ainda mais dados para nós, que podemos monetizar. (tradução nossa)

Mais do que a oferta do acesso fácil, instantâneo e praticamente ilimitado ao entretenimento, à informação, e às interações sociais no ambiente digital, não se pode deixar de considerar o cenário de dependência que caracteriza a relação entre usuários e plataformas no capitalismo de vigilância. Cuida-se de elemento que aprofunda ainda mais as disparidades de

---

[87] Rieger (2022, p. 61), em importante Dissertação de Mestrado, desenvolve os conceitos de "privacidade mental" e "liberdade cognitiva" na perspectiva do desenvolvimento e da aplicação de neurotecnologias. Segundo a autora, "a privacidade mental é pressuposta para liberdade cognitiva, quando se compreende que qualquer intervenção a nível mental traz consequências a longo e curto prazo no livre desenvolvimento da personalidade, bem como intervenções abusivas nos padrões de escolhas, impedindo a autonomia do sujeito diante de sua realidade existencial".

poder no contexto do uso de plataformas digitais, na medida em que, considerada a sua incorporação às atividades cotidianas, a renúncia individual a tais tecnologias pode representar a própria interdição da vida em sociedade, ou mesmo a impossibilidade de vivenciar um espaço importante à formação e ao desenvolvimento da própria personalidade individual[88].

1.3 Assimetrias informacionais: o "espelho de um lado só" na sociedade algorítmica

A assimetria de informações representa outro subproduto da lógica de extração e acumulação de dados pessoais que permeia o modelo econômico predominante na sociedade algorítmica, com relação ao uso de plataformas digitais, e um dos principais desafios à proteção da autonomia individual nesse contexto[89]. Como vimos, o fenômeno da dataficação da vida integra uma dinâmica em que o desenvolvimento sem precedentes das capacidades de coleta e armazenamento permitiu a formação de imensos repositórios de dados pessoais (*Big Data*).

Todavia, não apenas o acúmulo desproporcional de dados pessoais em um dos polos da relação jurídica informacional caracteriza a assimetria de que aqui se cogita. Afinal, o conjunto de dados pessoais "crus", que não tenha sido submetido a um processo de agregação, organização, refinamento e análise, não tem grande utilidade para as empresas que operam plataformas digitais (e para seus parceiros comerciais), que estruturam sua lógica negocial a partir de inferências, predições e influências sobre o comportamento humano. Tão importante quanto os avanços tecnológicos na raiz do surgimento do *Big Data* é o desenvolvimento exponencial das tecnologias de processamento de dados pessoais, que permitiram um grande salto qualitativo na análise desses fragmentos da personalidade humana (*Big Analytics*).

A partir da sistemática do espelho de um lado só (*one-way mirror*) proposta por Frank Pasquale, de que já tratamos, a contínua vigilância do comportamento individual no ciberespaço oferece a matéria-prima que viabilizará a formação de inferências[90] e decisões a partir do perfil

---

[88] Na expressão de Zuboff, (2020, p. 159), a ubiquidade das tecnologias digitais nos relegou a um mundo sem fuga (*world of no escape*): "Com o capitalismo de vigilância migrando do Vale do Silício para uma gama de outras empresas e setores, aos poucos nos encontramos num mundo sem fuga, 'monopolizados' por operações de despossessão que vão convergindo, se sobrepondo e se expandindo sem piedade."

[89] "Muitos dos dados pessoais sobre os usuários de internet dos Estados Unidos decorrem de relacionamentos com seus fornecedores de internet e de serviços móveis, com sites que usam, ou com grandes plataformas de tecnologia como Google, Amazon, Apple, Facebook, e Microsoft. Isso significa que muitas, se não a maioria, das preocupações com a privacidade estão enraizadas em um relacionamento caracterizado por extremas assimetrias de informação e poder." (Richards; Hartzog, 2020b, p. 1745, tradução nossa)

[90] "Hoje, o sucesso de um modelo é muitas vezes medido em termos de lucros, eficiência ou taxas de inadimplência. É quase sempre algo que pode ser contado. Mas o que deveríamos estar contando? Considere o exemplo a seguir. Quando as pessoas fazem uma busca online por informações sobre vale-alimentação do governo, muitas vezes são confrontadas com anúncios de intermediários, como o FindFamilyResources, de Tempe, Arizona. Tais sites parecem oficiais e dão links para formulários verdadeiros do governo. Mas eles também coletam nomes e endereços de e-mail para anunciantes predatórios, incluindo universidades de fins lucrativos. Eles ganham

comportamental dos usuários. Assim, os dados pessoais em estado bruto são refinados, transformando-se em conhecimento sobre os indivíduos, de modo a que as empresas que operam as plataformas digitais (e os seus parceiros comerciais, aos quais interessa o acesso a verdadeiros *dossiês* acerca da identidade individual) sejam capazes de ter acesso a aspectos detalhados da individualidade humana ignorados pelos próprios titulares dos dados pessoais.

Basta verificar que a integração entre inúmeros dispositivos[91] que permeiam o cotidiano dos indivíduos na atualidade (sistemas operacionais, plataformas digitais, *wearables*, entre outros) torna possível a agregação dos dados pessoais coletados, formando-se, mesmo sem que seu usuário se dê conta, um retrato fidedigno de sua personalidade, disponível para ser acessada, comercializada, compartilhada e manipulada no capitalismo de vigilância.

Nesse contexto, um *smartwatch*, que periodicamente faz medições da frequência cardíaca, pode estar integrado à plataforma digital que apresente ao usuário determinado conteúdo de ódio (*hate speech*) ou de outra natureza, capaz de despertar estímulos emocionais de raiva ou medo. Pode, também, integrar-se à plataforma de *e-commerce*, de modo a informar se, exposto a este ou aquele produto, houve alteração na frequência cardíaca do usuário, ou em outro sinal vital indicativo de uma reação positiva ou negativa. Como se vê, tais associações, viabilizadas por algoritmos, permitem a criação de um perfil altamente refinado acerca da personalidade e do comportamento humanos, extrapolando a capacidade individual de perceber, registrar, analisar e compreender suas próprias reações a diferentes estímulos. Na síntese de Frazão (2019, p. 340), "os algoritmos estão adquirindo o poder de decodificar as pegadas digitais das pessoas, inferindo e predizendo até mesmo aquilo que ninguém revela e que muitas vezes não tem nem mesmo consciência".

Portanto, a assimetria informacional se revela tanto por uma dimensão *quantitativa*, relacionada à capacidade incomparável de coleta e armazenamento de dados pessoais de uma das partes, quanto, por outro lado, por uma dimensão *qualitativa*, na medida em que apenas as empresas detêm a capacidade de realizar sofisticados cruzamentos, análises e predições a respeito do comportamento humano, a partir do volume de informações coletadas de diversas

---

dinheiro com geração de leads ao fornecer um serviço supérfluo às pessoas, muitas das quais rapidamente se tornam alvo de serviços que não podem pagar." (O'Neil, 2017, p. 206, tradução nossa)

[91] De acordo com a 35ª edição da Pesquisa Anual do Centro de Tecnologia de Informação Aplicada (FGVcia) sobre o Mercado Brasileiro de TI e Uso nas Empresas, o Brasil tem 480 milhões de dispositivos digitais em uso, o que representa a distribuição média de 2,2 dispositivos digitais por habitante. Disponível em: https://portal.fgv.br/noticias/pesquisa-revela-brasil-tem-480-milhoes-dispositivos-digitais-uso-sendo-22-habitante (acesso em: 9 nov. 2024). Outra pesquisa, repercutida pelo portal Tudo Celular em abril de 2024, informa que, em média, brasileiros têm 4 dispositivos conectados à internet em casa. Disponível em: https://www.tudocelular.com/tech/noticias/n219704/brasileiros-tem-4-dispositivos-em-media-na-interne.html. Acesso em: 9 nov. 2024.

fontes. Tem-se, de fato, segundo Balkin (2018, p. 5), forte na proposta teórica de Pasquale, uma dinâmica em que "os comportamentos, crenças e atividades de uma parte são conhecidos pela outra enquanto a outra parte é essencialmente uma caixa preta" (tradução nossa).

Nesse contexto, as empresas que exploram plataformas digitais revelam aos usuários aquilo que desejam (e *do modo que* desejam), e aquilo que considerem suficiente à demonstração objetiva de cumprimento de deveres de transparência e boa-fé – dentre outros que sejam correlatos – determinados pela legislação de proteção de dados pessoais. Considerando-se a incapacidade de compreender ou interferir no conteúdo de termos de uso ou de políticas de privacidade, aos usuários resta *confiar* no teor das informações apresentadas, e esperar, razoavelmente, que o uso dos serviços oferecidos pelas plataformas digitais não lhes gere algum dano imediato ou futuro. Como lecionam Marques e Mucelin (2022, p. 14), na perspectiva consumerista:

> As informações, a marca e as comunicações despertam a confiança no consumidor, sujeito confiante passivo que, em princípio, não tem condições de atestar veracidade dos dados ou então a existência de informações outras que não foram fornecidas, mas que, outrossim, seriam de extremada importância. Miragem ensina 'nesta perspectiva, informação é um poder, e a imposição do dever de informação aos fornecedores visa, em última análise, promover a equidade informacional das partes'.

Há, contudo, uma terceira dimensão da assimetria informacional. Trata-se do desconhecimento – da perspectiva dos usuários – do funcionamento das técnicas de coleta e análise e dados pessoais[92], e dos pressupostos em que se baseiam os algoritmos utilizados nos processos de tomada de decisão (e, bem assim, do modo de funcionamento de tais algoritmos). Nessa dimensão, que podemos denominar de *funcional*, as assimetrias informacionais revelam a disparidade de poderes[93] havida no contexto da relação informacional, colocando em xeque as potencialidades da autodeterminação informativa enquanto mecanismo efetivo de empoderamento dos titulares de dados pessoais[94]. Nesse sentido, ao analisar criticamente a proteção de dados pessoais pautada no paradigma do controle (tema de que trataremos no Capítulo 3), Waldman (2021, p. 2) propõe que

---

[92] "[...] muitas vezes, o usuário não tem consciência plena dos diversos modos de coleta e categorias dos dados pessoais, muito menos consegue visualizar o tipo de utilização realizada pelos fornecedores, o que impede, na prática, um consentimento livre e informado sobre esta utilização." (Camargo, 2021, p. 89)

[93] "As *big tech* e os políticos nos tratam como marionetes e conseguem nos manipular porque sofremos de uma assimetria de conhecimento que levou a uma assimetria de poder. Até recentemente, sabíamos muito pouco sobre como as big tech e a propaganda política funcionam no reino digital. Suas táticas eram invisíveis para nós. Ao passo que eles sabem quase tudo sobre nós." (Véliz, 2021, p. 124)

[94] Como diz Bioni (2020, p. 191), "a diretriz normativa da autodeterminação informacional se perdeu em meio às assimetrias do mercado informacional [...] o cidadão-consumidor está exposto a uma (hiper)vulnerabilidade que mistifica a sua prometida capacidade de controle dos seus dados pessoais."

> ao invés de estabelecer as 'regras do jogo' que apenas legitimam a extração de dados pelas empresas, como fazem agora, leis sobre privacidade deveriam identificar assimetrias de poder estruturais que dão às empresas poder demasiado sobre os indivíduos e implantar ferramentas legais para combater esse poder. (Tradução nossa)

Afinal, se, por um lado, falta aos usuários das plataformas digitais o conhecimento técnico necessário para compreender os sofisticados mecanismos envolvidos na tomada de decisão algorítmica, por outro, mesmo que soubessem (a partir de uma exposição transparente das informações pelas empresas), não teriam qualquer influência apta a interferir em seu desenho ou modo de funcionamento. Como leciona Balkin (2020, p. 11),

> Nós confiamos em negócios digitais para realizarem diferentes tarefas para nós. No processo, esses negócios aprendem muito sobre nós – nossos gostos, nossas aversões, nossos hábitos, nossos movimentos, sites que visitamos, com quem nos comunicamos e quando o fazemos, detalhes de nossos corpos, e até mesmo como digitamos, clicamos e tocamos interfaces digitais. Embora empresas digitais saibam muito sobre nós, nós não sabemos muito sobre elas – suas operações, que tipos de dados elas coletam, como elas usam esses dados, e com quem elas os compartilham. Por causa dessa assimetria de informações, estamos especialmente vulneráveis a elas e temos que confiar que elas não vão trair nossa confiança ou nos manipular. (Tradução nossa)

Nesse quadro, são as empresas detentoras dos algoritmos que definem, livremente, as premissas e as inferências envolvidas na tomada de decisão automatizada. Tendo-se em vista as dimensões superlativas das disparidades de poder relacionadas à informação, é necessário refletir sobre a real aptidão dos usuários para tomarem decisões efetivamente livres no contexto do uso das plataformas digitais. Afinal, ignoram-se os pressupostos que dão amparo às inferências feitas pelos algoritmos[95], ao tempo em que não há poder de interferir ou influenciar em tal sistemática, ainda que houvesse, de fato, conhecimento sobre a mecânica decisória.

Nesse particular, a assimetria informacional desempenha papel fundamental na capacidade das empresas de interferir sobre o comportamento humano, na medida em que, conhecendo-se as reações do indivíduo a diferentes estímulos, há elementos suficientes para influenciar o processo decisório no ciberespaço[96]. Arquiteturas de escolha, assim, podem ser moldadas de acordo com o perfil individual, explorando-se vieses cognitivos, de modo a manipular (e, portanto, instrumentalizar) a agência do usuário nas plataformas digitais.

---

[95] "[...] é urgente a necessidade de se introduzir mecanismos de transparência e accountability nas decisões algorítmicas. Por mais que existam limitações naturais à transparência das decisões – que muitas vezes são baseadas em um número imenso de dados, processados por sistemas que adotam um número imenso de passos, de forma a tornar praticamente impossível uma regressão absoluta –, há que se buscar alternativas para lidar com essa realidade." (Frazão; Goettenauer, 2021, p. 31)

[96] "Ora, se a forma mais fundamental de poder em uma sociedade tecnológica e informacional é a capacidade de influenciar e manipular as pessoas, é fácil concluir que os principais riscos da nova economia vão muito além da violação à privacidade dos usuários, alcançando a própria liberdade e a identidade pessoal e, consequentemente, a cidadania e a democracia." (Frazão, 2018)

1.4 Dependência e (hiper)vulnerabilidade dos usuários de plataformas digitais

Plataformas digitais são tecnologias cada vez mais integradas ao cotidiano e ao tecido social. Segundo Marques e Mucelin (2022, p. 4), na sociedade atual, "a totalidade das relações são ou serão mediadas, viabilizadas ou concretizadas por intermédio de ou com plataformas, em cuja estrutura ressalta-se a importância dos códigos, compreendidos também os algoritmos".

Em se tratando, como elucida Han, de aspecto fundamental da dominação no regime de informação[97], cuida-se de tendência que tende a se ampliar, à medida que cada vez mais dispositivos se tornam *smart*, conectando-se à Internet e, portanto, sendo utilizados mediante o emprego de plataformas. Indivíduos tornam-se, nesse processo, progressivamente mais dependentes do uso das mencionadas tecnologias, ao passo que mais e mais aspectos de suas vidas passam a envolver o recurso ao ambiente digital. É exatamente nesse sentido o preciso diagnóstico de Balkin (2020, p. 13):

> Essas dependências só aumentarão com o tempo. Assistentes digitais pessoais como Alexa e Siri (que em breve serão seguidos por robôs pessoais) estão em nossas casas e escritórios esperando por nossos comandos, em troca de cada vez mais dados sobre nossos desejos e hábitos, até mesmo a inflexão emocional de nossas vozes. A internet das coisas em rápido crescimento promete fazer com que quase todos os aparelhos com os quais interagimos sejam um dispositivo de coleta de dados, melhor para nos servir — e nos monitorar. As empresas querem que dependamos cada vez mais dessas tecnologias; na verdade, elas querem que nossa dependência seja visceral, para que um dia nem pensemos em viver sem elas. (Tradução nossa)

A ubiquidade das plataformas digitais molda e condiciona o modo de vida na sociedade algorítmica, o que, segundo Zuboff (2020, p. 22), é parte de um "projeto de vigilância comercial, no qual as necessidades que sentimos por uma vida eficaz lutam contra a inclinação de resistir às audazes incursões do sistema". São, de fato, inegáveis as funcionalidades e comodidades oferecidas por tecnologias digitais para a realização de tarefas cotidianas.

Com poucos cliques (ou toques na tela), é possível estabelecer contato instantâneo com pessoas em qualquer lugar do mundo e acessar livremente um repositório virtualmente ilimitado de informações. O reconhecimento facial torna transações bancárias[98] (que, aliás, mediadas por

---

[97] "A dominação do regime de informação é ocultada, na medida em que se funde completamente com o cotidiano. É encoberta atrás da complacência das mídias sociais, da comodidade das máquinas de busca, das vozes embalantes das assistentes de voz ou da oficiosidade prestativa dos *smart apps*, os aplicativos inteligentes. O *smartphone* se revela como um *informante* eficiente, que nos submete a uma vigilância duradoura. A *Smart Hom*e, a casa inteligente, transfigura a casa toda em uma prisão digital que protocola minuciosamente nossa vida cotidiana. O robô-aspirador-de-pó *smart*, que nos poupa da limpeza cansativa, mapeia a casa toda. A *Smart Bed*, a cama inteligente, com seus sensores conectados, prolonga a vigilância também durante o sono. A vigilância infiltra-se no cotidiano na forma de *conveniência*." (Han, 2022, p. 16)

[98] Notícia veiculada no portal Agência Brasil em abril de 2024 informa que sete a cada dez bancos brasileiros utilizam a biometria facial na identificação de seus clientes, sendo essa uma das tecnologias mais adotadas pelas instituições financeiras no Brasil, de acordo com a primeira fase da Pesquisa Febraban de Tecnologia Bancária

plataformas digitais, reduziram drasticamente as enfadonhas filas dos caixas) mais seguras e ágeis. Os *smartwatches* fornecem dados e métricas cada vez mais precisos sobre a qualidade do sono, o gasto calórico, a frequência cardíaca, o nível de oxigênio no sangue. A lista continua.

Os usuários, no mais das vezes, são apresentados a apenas um dos lados da moeda. Tal é o entusiasmo com que são recebidos (e alardeados) novos aplicativos, novas tendências, novas facilidades, que a extração massiva de dados pessoais – e suas consequências a médio e longo prazo – é ignorada ou, na melhor das hipóteses, compreendida como um preço justo a ser pago pelos benefícios das novas tecnologias. A esse cenário somam-se declarações públicas das empresas que exploram as plataformas digitais, que convidam seus usuários a nelas depositarem sua confiança[99], porque, para elas, a privacidade é "algo importante"[100].

Não haveria, de acordo com esse discurso, nada com que se preocupar (lembremo-nos, como visto no subcapítulo 1.1, que a construção de uma *retórica da privacidade* é um dos aspectos fundamentais à manutenção das engrenagens do capitalismo de vigilância): dados pessoais seriam utilizados apenas "para te conhecer melhor", "para melhorar os serviços que prestamos a você", ou para "sugerir produtos que você possa se interessar". De todo modo, políticas de privacidade não são lidas[101]; se o são, não raro são evasivas, genéricas e incompreensíveis; e mesmo se não o forem, não há, afinal, nada a ser feito. O consentimento é a única saída possível para o uso das funcionalidades, facilidades e comodidades viabilizadas pelas plataformas. Sua lógica de uso estrutura-se, no mais das vezes, sobre a lógica do "pegar ou largar" (*take-it-or-leave-it choice*).

O uso das plataformas digitais como ferramentas predominantes para o acesso à informação, para a comunicação e para a aquisição de bens e serviços dá causa a uma relação

---

2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-04/sete-em-cada-dez-bancos-adotam-biometria-facial-0. Acesso em: 8 nov. 2024.

[99] "As empresas digitais convidam as pessoas a confiarem nelas com seus dados. Quando as pessoas aceitam essa oferta de confiança, elas se tornam vulneráveis: à forma como as empresas usam seus dados, à segurança dos dados das empresas (ou à falta dela) e à escolha das empresas de compartilhar ou vender os dados a terceiros." (Balkin, 2020, p. 11, tradução nossa)

[100] Aqui, faz-se referência a terminologia comumente utilizada em políticas de privacidade de agentes políticos e econômicos atuantes nos mais diversos setores, da Microsoft ao Tribunal de Contas do Estado de Goiás. Percebe-se, com a padronização (ou "copia e cola") do texto, que políticas de privacidade, em muitos casos, não passam de adornos ou de declarações vazias e descompromissadas com a adoção de cautelas e salvaguardas adequadas à proteção dos dados pessoais dos titulares. Essa tendência é reforçada com o modelo procedimental em que se fundamenta o regime de proteção de dados pessoais sistematizado pela LGPD.

[101] Além da falta de capacidade técnica, o usuário comum não dispõe de tempo suficiente para realizar a leitura das políticas de privacidade de todas as plataformas digitais que utiliza. De acordo com notícia veiculada na Folha de São Paulo, "[o]s brasileiros gastariam quase o tempo de uma semana de trabalho (39,5 horas) caso decidissem ler as políticas de privacidade dos 96 sites mais visitados do país". Disponível em: https://www1.folha.uol.com.br/tec/2023/10/brasileiro-perderia-40-horas-para-ler-politicas-de-privacidade-de-sites-mais-acessados.shtml. Acesso em: 9 nov. 2024.

de *dependência* dos usuários com relação àquelas. Essa ordem de coisas causa o acirramento das assimetrias entre indivíduos e empresas que exploram as plataformas, na medida em que são elas que franqueiam o acesso (*gatekeepers*) ao exercício de diversos direitos (e à própria participação social[102]) que, hoje, se apresentam sob roupagem essencialmente digital, e não mais analógica. Nesse contexto, a dependência – diretamente relacionada ao uso de mecanismos de extração massiva de dados pessoais – e o poder são grandezas diretamente proporcionais[103].

Para além disso, a dependência de que aqui se cogita é, quase sempre, psíquica. Como já referimos, o conhecimento pormenorizado sobre o perfil comportamental dos usuários permite o êxito de estratégias que, para além do engajamento, promovem o vício nas telas. Afinal, na economia da atenção, plataformas digitais viciantes têm o poder de reter os olhares de seus usuários por mais tempo[104] (no Brasil, em 2023, foram gastas em média 3,5 horas por dia com o uso de smartphones[105]).

Também em perspectiva ampla, o surgimento de um novo modo de viver, fortemente amparado na disponibilidade incessante (sobretudo no contexto das relações de trabalho) e no acesso imediato à informação, gerou o que se tem denominado *nomofobia* (neologismo derivado de *no mobile phone phobia*), que remete à ansiedade gerada pela falta dos *smartphones*, caracterizada por verificações constantes, preocupação excessiva e mesmo sintomas físicos[106]. Os efeitos da dependência psíquica causadas pelas plataformas digitais se

---

[102] "Cada vez mais, a participação social é dependente desse trânsito informacional. Na verdade, a lógica do mercado e da sociedade da informação arquitetam essa (falsa) escolha, já que, para fazer parte do jogo, deve-se aceitar o convite mediante o 'concordo' em compartilhar os 'meus' dados pessoais. Daí por que a proteção dos dados pessoais geraria um custo social, qual seja, a não fruição dessas oportunidades que resultaria em uma eremitania na sociedade da informação." (Bioni, 2020, p. 157)

[103] "Informação é poder, e informação sobre outras pessoas pode trazer poder sobre essas outras pessoas. [...]. Eu argumentei que é importante compreender a privacidade em termos de informação humana porque tecnologias de informação humana estão sendo usadas para predizer, influenciar e cada vez mais controlar o comportamento humano. Eu mostrei como termos antissépticos como 'dados' para descrever essas tecnologias são usados para nos distanciar do que realmente está em jogo em discussões sobre a privacidade – como o poder está sendo exercido sobre seres humanos de diversas formas. O poder é central à compreensão do que está sendo feito com a informação humana em nossas sociedades, e é a razão essencial pela qual a privacidade importa." (Richards, 2022, p. 40, tradução nossa)

[104] É nesse sentido a conclusão de Frazão (2018, p. 642): "Quanto mais tempo as pessoas passam em determinadas plataformas, mais intensamente estarão submetidas à publicidade e à coleta de seus dados, assim como mais suscetíveis estarão a estratégias que visam influenciar e alterar suas preferências e visões de mundo."

[105] É o que diz pesquisa divulgada na Folha de São Paulo em abril de 2024. Ainda de acordo com o levantamento, no mesmo período, aplicativos foram baixados 10 bilhões de vezes. Com isso, o Brasil ocupa o quarto lugar no *ranking* mundial de tempo de tela e de número de *downloads*. Disponível em: https://www1.folha.uol.com.br/tec/2024/04/brasileiros-gastaram-35-horas-por-dia-no-smartphone-em-2023.shtml. Acesso em: 9 nov. 2024.

[106] De acordo com notícia veiculada no Portal CNN, a nomofobia é causada, dentre outros fatores, pela "necessidade de estar sempre conectado e atualizado, a busca por validação social e o medo de perder informações importantes". Disponível em: https://www.cnnbrasil.com.br/saude/nomofobia-conheca-medo-irracional-de-ficar-sem-celular/. Acesso em: 9 nov. 2024.

fazem sentir, com especial gravidade, em crianças e adolescentes: dados da Rede de Atenção Psicossocial (RAPS) do SUS de 2013 a 2023 revelam que, pela primeira vez, o número de casos de ansiedade entre crianças e jovens *superou* o de adultos[107].

De todo modo, o discurso sedutor da inovação, da facilidade e do entretenimento catalisa a integração das plataformas digitais à vida humana, causando a formação de um estado de coisas irreversível, em que não mais se cogita de um modo de vida que prescinda do uso de referidas tecnologias[108]. Assim, quanto mais *dependentes* os usuários sejam das plataformas digitais, mais poder sobre eles terão as empresas que operacionalizam as plataformas. Na advertência de Véliz (2021, p. 251),

> Depender de qualquer empresa de tecnologia é perigoso. Isso significa que parte de sua identidade está nas mãos deles, e se eles cancelarem sua conta, ou apagarem seus e-mails (isso acontece), você pode ter muito a perder. As empresas de tecnologia querem que você dependa delas, por isso é muito difícil não depender. Às vezes é impossível. Mas tenha isso em mente. Há graus de dependência, e quanto menos você depender de qualquer plataforma ou aplicativo, menos poder eles terão sobre você.

As disparidades de poder entre titulares e plataformas digitais, como observa a literatura especializada, alcançam dimensões antes inimagináveis, sobretudo no cenário de um "mundo sem saída" (*world of no escape*), na expressão de Zuboff, já mencionada. Negar a coleta de dados pessoais significa, em tal contexto, tornar-se alheio ao convívio social que, em grande medida, migrou para o ciberespaço[109]. Significa, também, interditar importantes vias de acesso à informação e ao conhecimento, a relevantes instâncias de pluralização do debate democrático,

---

[107] "Com um crescimento expressivo nos últimos anos, a taxa de pacientes de dez a 14 anos atendidos pelo transtorno é de 125,8 a cada 100 mil, e a de adolescentes, de 157 a cada 100 mil. Já entre pessoas com mais de 20 anos, a taxa é de 112,5 a cada 100 mil, considerando dados de 2023. A situação dos mais jovens passou a ficar mais crítica do que a dos adultos em 2022." Disponível em: https://www1.folha.uol.com.br/folhateen/2024/05/registros-de-ansiedade-entre-criancas-e-jovens-superam-os-de-adultos-pela-1a-vez.shtml. Acesso em: 9 nov. 2024.

[108] Lembre-se, por exemplo, de recente episódio em que uma falha nos sistemas de segurança da empresa CloudStrike impactou diretamente a Microsoft, afetando, por consequência, usuários da plataforma Windows de todo o mundo. Chamado de "apagão cibernético", o evento ocorrido em julho de 2024 causou prejuízos da monta de 5,4 bilhões de dólares para as empresas afetadas. Disponível em: https://www.tecmundo.com.br/seguranca/287499-pane-crowdstrike-custou-us-5-4-bilhoes-empresas-afetadas.htm. Acesso em: 7 nov. 2024.

[109] À medida que as tecnologias digitais se integram à vida cotidiana, os indivíduos vão se tornando progressivamente mais dependentes de suas funcionalidades, que de fato racionalizam e atribuem eficiência ao exercício de atividades econômicas, profissionais, sociais e pessoais. Passa-se a integrar o acesso aos sistemas digitais à aquisição de bens e à utilização de serviços, de tal forma que o uso das plataformas digitais se torna verdadeira condição da participação no ambiente social. Segundo Balkin (2020, p. 12), "[é] cada vez mais difícil evitar lidar com empresas digitais que coletam e usam nossos dados. [...]. Viver sem interagir com qualquer desses serviços significa reduzir gravemente a vida e as oportunidades de uma pessoa, porque as tarefas mais comuns – encontrar um emprego, deslocar-se de um local a outro, procurar comida, manter contato com amigos e parentes, acessar notícias e informações – nos expõe à vigilância e à coleta de dados" (tradução nossa).

e, até mesmo, à prestação de serviços públicos (considerados os esforços de digitalização da Administração Pública[110], motivados pelos ganhos de eficiência com as plataformas digitais).

Consequentemente, agrava-se o cenário de vulnerabilidade e dependência, em que os usuários de plataformas digitais se veem à mercê dos desígnios livremente estabelecidos pelos agentes econômicos que as operam. Bioni (2020, p. 157) identifica, nesse aspecto, uma tríplice dimensão da vulnerabilidade (informacional, técnica e econômica), constatando "uma sobreposição de fraquezas, na medida em que aquele sujeito vulnerável é inserido em um novo contexto: o do mercado informacional".

De fato, como examinamos no presente capítulo, as assimetrias informacionais no contexto do uso de plataformas digitais se caracterizam pela *falta de conhecimento* adequado dos usuários a respeito das técnicas utilizadas (e das escolhas feitas) na definição da arquitetura das plataformas digitais. De qualquer forma, ainda que fossem dotados de conhecimento técnico especializado para compreender as minúcias do *design* das plataformas, os usuários não teriam qualquer *poder de barganha* com o qual negociar este ou aquele aspecto técnico da plataforma digital (e, bem assim, esta ou aquela cláusula da política de privacidade).

Ademais, assimetrias informacionais aprofundam a vulnerabilidade e a efetividade das técnicas de manipulação envolvidas no desenho das plataformas digitais, na medida em que proveem ao agente econômico um grau aprofundado de *conhecimento a respeito do perfil comportamental* dos usuários. Com isso, é possível moldar o fluxo informacional ou a própria arquitetura de escolhas a partir do objetivo a ser atingido por meio do comportamento do usuário. Como vimos no presente subcapítulo, o avanço do processo de integração das plataformas digitais à vida cotidiana induz a crescente relação de dependência entre usuários e plataformas, com o que se tem mais um elemento relevante da (hiper)vulnerabilização dos indivíduos no contexto da sociedade algorítmica (ou, na dicção de Marques e Mucelin, tem-se novos "fatores especiais de vulnerabilização"[111]).

---

[110] Nesse particular, vale mencionar o Decreto Federal nº 12.069/2024, que institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027. A Estratégia tem, como uma das prioridades das ações de transformação digital da administração pública federal e dos integrantes da Rede Gov.br, o "fomento do uso da ferramenta de autenticação da Plataforma gov.br e do Serviço de Identificação do Cidadão". Vale ainda acrescentar, a propósito do assunto, que o Decreto define a transformação digital como a "utilização de tecnologias digitais para o atendimento eficiente do cidadão, a integração de serviços e de políticas públicas e a promoção da transparência, com vistas a inserir o Estado de maneira mais eficaz no ambiente digital e torná-lo mais dinâmico e próximo da população".

[111] "A vulnerabilidade do consumidor não deixa de representar –como sempre foi –um valor latente de potencial exploração de fraquezas do sujeito que consome. A diferença é que, no mundo digital, esse 'valor' é muito mais facilmente percebido e revelado, ou mesmo criado, por conta das arquiteturas de escolha, da automação do mercado, das grandes plataformas-fornecedoras e do engajamento constante dos consumidores em uma internet

Importa notar, também, que a vulnerabilidade é – em maior ou menor medida – ínsita ao próprio fluxo informacional. É dizer: sempre que determinada informação sobre um indivíduo é transmitida a outrem, aquele que a recebe torna-se dotado do *poder* de utilizá-la, em alguma extensão, em detrimento do emissor da informação. A vulnerabilidade, enquanto aspecto relevante da circulação de dados pessoais (discussão que guarda, como se pode notar, íntima relação com o direito à privacidade), será aprofundada no Capítulo 4. Contudo, por ora, importa consignar apenas que a vulnerabilidade havida no fluxo informacional das plataformas digitais é sobremaneira intensificada pelas assimetrias informacionais e mesmo de poder entre as partes, na medida em que o *potencial de causar dano* ao indivíduo adquire dimensão sem precedentes. Como dizem Richards e Hartzog (2016, p. 450):

> Quando os "confiadores" confiam informações sobre si mesmos, eles se tornam vulneráveis. Sua vulnerabilidade pode incluir maior risco de uso indevido de informações, divulgação não autorizada, manipulação ou perda de autonomia. Um banco pode deixar seus números de conta em um laptop em um aeroporto. Um mecanismo de busca pode entregar suas consultas para o governo ou para o público em geral. [...]. As possibilidades de divulgação, lesão ou manipulação em tais casos são limitadas apenas pelo potencial humano para inovação. (Tradução nossa)

A dependência, convém observar, não se revela apenas pelo uso das plataformas, mas, também, pela sujeição – muitas vezes não percebida – à tomada de decisão unilateral algorítmica, que pode afetar aspectos existenciais relevantes dos usuários. Nesse contexto (que Han denomina "regime de informação"[112]), por exemplo, mecanismos de análise de crédito operam sobre avaliações feitas por algoritmos, baseadas em dossiês a respeito de perfis comportamentais, que vão do histórico de consumo e adimplência à projeção de tendências futuras[113] (que envolvem a avaliação sobre a probabilidade de que o cliente venha a contrair futuras obrigações e, portanto, não honrar as presentes).

Do exposto no presente capítulo, constata-se que as características elementares do capitalismo de vigilância evidenciam a defasagem, com relação aos dias atuais, do mundo

---

cada vez mais ubíqua, onisciente e onipresente –o que demanda a evolução no conceito de *vulnerabilidade*... agora digital." (Marques; Mucelin, 2022, p. 26)

[112] "Chamamos de regime de informação a forma de dominação na qual informações e seu processamento por algoritmos e inteligência artificial determinam decisivamente processos sociais, econômicos e políticos. [...]. Não é, então, a posse de meios de produção que é decisiva para o ganho de poder, mas o acesso a dados utilizados para vigilância, controle e prognóstico de comportamento psicopolíticos." (Han, 2022, p. 7)

[113] Cabe mencionar, nesse particular, o produto "Serasa Score", utilizado para medição de escores de crédito. Surgido em 2017, o Serasa Score tem passado por atualizações que envolvem a agregação cada vez maior de dados pessoais dos consumidores brasileiros. Na versão "2.0", passaram a ser utilizados dados do SPC Brasil no cálculo da pontuação. Na versão "3.0", "com foco em tornar o cálculo da pontuação ainda mais personalizado, a partir da inclusão das informações bancárias por meio da Conexão Bancária". Disponível em: https://epocanegocios.globo.com/empresas/noticia/2024/03/serasa-aposta-em-tecnologia-para-analisar-dados-e-dar-pontuacao-de-credito-para-mais-de-80-milhoes-de-brasileiros.ghtml. Acesso em: 9 nov. 2024.

narrado por George Orwell em *1984*. Dataficação, assimetrias informacionais, dependência e (hiper)vulnerabilidade conduzem os indivíduos a um cenário que mais se assemelha ao descrito por Franz Kafka em O Processo. Afinal, apresenta-se a inescapável subjugação da pessoa humana a decisões automatizadas, tomadas por algoritmos programados por indivíduos desconhecidos, não raro contaminados por preconceitos e em vieses ínsitos à racionalidade humana. Os meios de acesso aos fundamentos das decisões são labirínticos, burocráticos e desestimulam (ou dificultam sobremaneira) o exercício de direitos no ambiente virtual.

Mais do que isso, o contexto de que estamos a tratar – no qual se inserem as plataformas digitais como mecanismos eficientes de manipulação dos usuários – envolve a concepção de um regime jurídico protetivo orientado por um paradigma ineficiente, porque pautado na atribuição de um *poder idealizado de controle*[114] ao indivíduo para que, sozinho, assuma todo o ônus de conter e direcionar o fluxo informacional a partir de suas íntimas convicções. Erigir o grande edifício da proteção de dados pessoais unicamente sobre o fundamento da autodeterminação informativa remete, como dizem Solove e Hartzog (2024, p. 1041), ao "clássico enredo de Kafka: as pessoas sabem que sua jornada está fadada ao fracasso e mesmo assim persistem nela" (tradução nossa).

Fixadas as características fundamentais do contexto em que se insere o uso de plataformas digitais na sociedade algorítmica, importa adensarmos o estudo na perspectiva dos mecanismos utilizados por tais tecnologias para instrumentalizar a agência humana. Desse modo, será possível visualizar de que modo os elementos estruturantes do capitalismo de vigilância se manifestam no contexto concreto das plataformas digitais. Demais disso, cabe compreendermos melhor o que se deve compreender por *manipulação*, estabelecendo adequadamente a correlação triangular do conceito com a arquitetura enganosa das plataformas digitais e o livre desenvolvimento da personalidade, aspecto estruturante do regime jurídico de proteção de dados pessoais.

---

[114] "Primeiro, o controle é ilusório. [...]. Isso porque o controle que nos é dado online é mediado, o que significa que ele não pode deixar de ser projetado para produzir resultados específicos. Quando se trata de controle, o design é tudo. As realidades da tecnologia em escala significam que os serviços que usamos devem necessariamente ser construídos de uma forma que restrinja nossas escolhas. Imagine um mundo onde cada usuário pudesse ditar seus próprios termos em uma caixa de texto aberta em vez de termos de uso padronizados. As empresas nunca sairiam do papel. Em vez disso, temos caixas para marcar, botões para pressionar, interruptores para ativar e desativar e outras configurações para mexer." (Hartzog, 2018, p. 426, tradução nossa)

2 DESAFIOS À AUTONOMIA NO MUNDO VIRTUAL: MANIPULAÇÃO E *DESIGN* MALICIOSO DAS PLATAFORMAS DIGITAIS

A autonomia é um valor fundante das democracias liberais (Susser; Roessler, Nissenbaum, 2019b, p. 4). Instituições democráticas haurem a sua legitimidade do exercício autônomo da escolha individual, consubstanciado no direito ao voto periódico, livre e secreto. Em outra perspectiva, a autonomia também delimita um âmbito de proteção do sujeito de direitos contra interferências externas ilegítimas, dentro do qual os indivíduos são livres para decidir, de acordo com suas próprias convicções, a respeito de aspectos existenciais de suas vidas, intimamente relacionados à formação e ao desenvolvimento de sua personalidade (*autodeterminação individual*[115]). A autonomia individual é, portanto, um atributo fundamental da personalidade da pessoa natural[116].

A autonomia guarda, ainda, relação estreita com o ideal kantiano de dignidade[117], cujo aspecto substantivo se traduz na conhecida formulação de que indivíduos devem ser considerados *fins em si mesmos* (Corrales; Bertoncini, 2019, p. 257). Segundo Sarlet (2006, p. 33), para Kant, "a autonomia da vontade, entendida como a faculdade de determinar a si mesmo e agir em conformidade com a representação de certas leis, é um atributo apenas encontrado nos seres racionais, constituindo-se no fundamento da dignidade da pessoa humana". De fato, a ideia de autonomia decorre diretamente de uma imagem da humanidade como intrinsecamente livre, imagem essa que subjaz a todas as liberdades e direitos humanos (Grisse, 2023, p. 102).

O exercício pleno da autonomia depende, em boa medida, do meio em que se inserem os indivíduos. Como vimos, no regime ditatorial de *1984*, a supressão da autonomia individual era um importante pilar do projeto de poder do Partido. A hipervigilância, por si só, não seria tão eficiente para a dominação das pessoas quanto a virtual eliminação de sua autonomia por meio do discurso manipulativo que, ao mesmo tempo em que impunha uma única narrativa *verdadeira* (embora baseada em constantes reinvenções do passado), buscava construir uma figura carismática e protetora – mas, ao mesmo tempo, hostil e implacável com os inimigos –

---

[115] "[...] o ser humano age autonomamente quando pode, por um lado, relacionar suas decisões e ações com a imagem que tem de sua própria pessoa e quando, por outro, ele é aquela pessoa com a qual se entende por força de um desenvolvimento auto-determinado." (Britz, 2021, p. 27)

[116] Como lembram De Marco e Castro (2013, p. 42), "o direito da personalidade surge da qualificação discursiva de certos fatos, reputados como relevantes para a autonomia e dignidade humanas, interpretados dessa forma com base na ordem jurídica nacional e internacional".

[117] "O princípio ético da autonomia baseia-se na afirmação kantiana de que se deve sempre respeitar o estatuto moral especial, que mais tarde veio a ser conhecido como dignidade, dos seres humanos, tratando-os como pessoas e não como meros recursos." (Botes, 2022, p. 318, tradução nossa)

capaz de docilizar o comportamento dos habitantes de Oceânia, fazendo com que acreditassem que as decisões do *Grande Irmão* eram intrinsecamente boas e corretas.

Como também torna claro o romance orwelliano, a informação (e o acesso a ela) tem estreita relação com o exercício da autonomia individual. Em regimes democráticos, a expressão da autonomia individual pelo voto será tão livre quanto maior (e melhor) seja o acesso das pessoas aos fatos e às informações[118] relevantes para a formação de sua livre convicção íntima. Assim, quem controla a informação (*o que* será informado, de que *forma*, em que *medida* e para *quem*) ostenta importante parcela do poder de interferir, ainda que indiretamente, sobre processos democráticos[119].

Todavia, considerado o contexto descrito no Capítulo 1 – diversamente do que ocorria à época em que o acesso à informação era centralizado nos veículos tradicionais de mídia (*mass media*) –, a maior capacidade de segmentação da informação atribui às plataformas digitais, sobretudo àquelas exploradas pelas *big five*[120], a aptidão de atribuir ênfase a um determinado conteúdo (ou posicionamento) em detrimento de outro(s). Essa amplificação do poder de direcionar o fluxo informacional (além das consequentes ameaças à autonomia), decorre, em grande medida, da *informação sobre quem terá acesso à informação*, ou seja, da formação de perfis psicográficos que tornam possível a identificação e delimitação de grupos de interesse[121].

Nesse sentido, cabe acrescentar que a priorização de conteúdos que despertem reações de raiva, ódio ou revolta se revela como uma estratégia de engajamento que submete os usuários

---

[118] "Com o advento da televisão e do rádio, logo se observou o potencial dos meios de comunicação de massa para o controle da informação, o que poderia ser implementado por meio de várias estratégias, como a definição das pautas dos assuntos considerados relevantes (*agenda setting*), a omissão dos assuntos inconvenientes e a 'moldura' das informações que seriam transmitidas ao grande público (*framing*), de modo a influenciar diretamente a formação da sua convicção sobre os assuntos mais importantes." (Frazão, 2021, p. 743)

[119] "[...] se as tecnologias manipuladoras secretamente, gradualmente e persistentemente efetuarem mudanças nas crenças e valores pessoais dos indivíduos, isso levará a mudanças na maneira como os indivíduos pensam, avaliam suas escolhas, formam intenções sobre elas e agem com base nessas intenções. Isso pode impactar os processos de tomada de decisão coletiva e, em última análise, afetar as democracias." (Botes, 2022, p. 319, tradução nossa)

[120] Denominação atribuída às cinco maiores empresas de tecnologia do mundo: Alphabet/Google, Amazon, Apple, Meta/Facebook e Microsoft. Também são, em conjunto, designadas pelo acrônimo "GAFAM". Disponível em: https://www.clicksign.com/blog/o-que-sao-big-techs. Acesso em: 13 nov. 2024.

[121] Incontornável a referência, ainda que breve, ao escândalo protagonizado pela empresa de consultoria política *Cambridge Analytica*, relacionado ao uso da plataforma de anúncios do Facebook para exercer influência sobre eleitores norte-americanos, considerado o contexto da eleição presidencial de 2016. Como narram Susser, Roessler e Nissenbaum (2019a, p. 9), a empresa se utilizou de um *quiz* de personalidade, chamado "thisisyourdigitallife", distribuído aos usuários do Facebook a partir de um aplicativo dentro da plataforma, para gerar vastos repositórios de perfis digitais. De acordo com os autores, os participantes receberam alguns dólares para responder o teste e dar acesso às suas contas. A partir de algumas centenas de milhares de respondentes, "a Cambridge Analytica acumulou dezenas de milhões de contas de usuários do Facebook por meio de um recurso (não mais ativo) que permitia que os desenvolvedores ganhassem acesso às contas dos 'amigos' dos respondentes – um número possivelmente tão alto quanto 87 milhões" (*Idem*, p. 10, tradução nossa).

das plataformas à condição de *meios* para o atingimento de finalidades políticas ou econômicas escusas ou, no mínimo, não reveladas. Assim, seja pelo controle do fluxo informacional (que interfere na capacidade de livre decisão sobre o conteúdo a ser consumido), seja pela consequente redução do espaço de reflexão crítica dos indivíduos (que depende da interação dialógica entre teses antagônicas), plataformas digitais despontam, no mundo contemporâneo, como estruturas dotadas de grande potencial *manipulativo*, mitigando-se, consequentemente, a autonomia individual[122].

Entretanto, não é apenas na condução de processos eleitorais[123] e no desenho das instituições democráticas que se manifesta a estreita relação entre informação e autonomia individual. A informação, como dito, também é imprescindível para a tomada de decisões existenciais autônomas (portanto, para o exercício da autodeterminação individual[124]).

Contudo, o fenômeno da *desinformação* vem causando graves preocupações devido às suas drásticas e negativas repercussões sobre a vida humana. Como exemplo, mencione-se a questão das variações nos índices de vacinação. Recente estudo de Sousa Neto e Pisa (2024)[125] avaliou publicações de grupos antivacinação[126] (*antivax*) em redes sociais e sua relação com a hesitação vacinal (a respeito da imunização de crianças contra a Covid-19). Segundo a pesquisa, "[a] desinformação sobre os imunizantes pediátricos **está intrinsecamente associada** aos '3Cs'

---

[122] Albuquerque, Valença e Falcão (2024, p. 3), a propósito, definem a autonomia como "o valor normativo de acordo com o qual usuários têm o direito de agir segundo suas próprias razões ao tomar decisões, sem ser excessivamente influenciados ou compelidos por forças externas [...]" (tradução nossa).

[123] "Obviamente, o objetivo final de influenciar os meios de comunicação é influenciar as pessoas que os consomem. Da mesma forma, influenciar as pessoas pode ser uma forma de alterar as instituições das quais elas participam – por exemplo, quando elas votam. No coração dessas preocupações, entretanto, estão inquietações sobre indivíduos e a independência de seus processos de tomada de decisão." (Susser; Roessler; Nissenbaum, 2019b, p. 13, tradução nossa)

[124] "[...] a autodeterminação não pode ser compreendida em abstrato, mas na consciência das escolhas e das consequências decorrentes dela [...]. O segundo aspecto é que a autodeterminação é pressuposto do desenvolvimento da personalidade [...] e, por isso, para sua existência, depende ao menos da possibilidade de ação dentro da ordem jurídica, de forma desejável, ao menos de maneira pressuposta pela ordem jurídica (standard), caso dependesse apenas de si." (Alves; Fernandes; Goldim, 2017, p. 250)

[125] Outro estudo, publicado por Lee *et al*. (2022, p. 9), demonstra que teorias da conspiração envolvendo falsos efeitos colaterais da vacina contra a Covid-19 interferiram gravemente na hesitação vacinal. Segundo os autores: "O estudo identificou, a partir da análise de respostas abertas, que as pessoas foram expostas à desinformação conspiratória sobre vacinas contra a Covid-19 tais como que as vacinas incluem um microchip ou são perigosas e prejudiciais, causando a morte ou alterando o DNA. O teste de conhecimento utilizado no estudo quantitativo também confirmou que muitas pessoas acreditavam em tal desinformação relativa às vacinas da Covid-19 como verdadeira e o conhecimento impreciso pareceu aumentar sua hesitação vacinal e reduzir a intenção de ser vacinado." (Tradução nossa)

[126] Em agosto de 2023, o Jornal da Universidade de São Paulo repercutiu pesquisa desenvolvida pela Sociedade Brasileira de Pediatria (SBP), em parceria com o Instituto Questão de Ciência, junto a mais de 980 médicos pediatras. Segundo os achados da investigação, as mídias digitais (em especial as redes sociais) são a principal fonte de hesitação vacinal entre as famílias atendidas. Disponível em: https://jornal.usp.br/atualidades/desinformacao-cientifica-uma-pandemia-de-mentiras/. Acesso em: 12 nov. 2024.

da OMS, podendo produzir a hesitação vacinal, colocando em risco a imunização de rebanho, foco da política pública de imunização [...]"[127] (grifo nosso).

A regulação de fluxos informacionais por meio de decisões unilaterais dos algoritmos[128] empregados no funcionamento de plataformas digitais – sobretudo as redes sociais – enseja graves distorções no acesso à informação, na medida em que a priorização de conteúdos gera verdadeiras "bolhas informacionais", caracterizadas pela reunião de usuários com interesses (logo, com opiniões e perspectivas) semelhantes, os quais produzem e consomem, em grande medida, conteúdos alinhados às suas preferências e ideologias. Como lembra Frazão (2019, p. 346), "a ideia de que os filtros dão aos usuários apenas o que eles querem tem o efeito de polarizar as populações, deixando os usuários suscetíveis a manipulações de todos os tipos e destruindo a legitimidade das instituições democráticas".

O fenômeno da segmentação de conteúdos inspira preocupações não apenas pelo potencial de radicalização e de polarização de perspectivas ideológicas (que causam o agravamento de conflitos políticos e sociais) mas, também, por sua capacidade de impactar diretamente aspectos importantes à preservação da própria saúde dos usuários, que passam a reforçar a crença em teorias da conspiração, mesmo diante de fatos sobre os quais haja amplo consenso científico. É nesse sentido a *Opinion 3/2018* do European Data Protection Supervisor (EDPS), que situa o uso dos dados pessoais no fenômeno aqui em comento:

> Esta questão de usar informações e dados pessoais para manipular pessoas e a política vai, é claro, muito além do direito à proteção de dados. Um ambiente online personalizado e microdirecionado cria "bolhas de filtro" onde as pessoas são expostas a informações "mais do mesmo" e encontram menos opiniões, resultando em maior polarização política e ideológica. **Aumenta a difusão e a persuasão de histórias falsas e conspirações**. (2018, p. 7, tradução e grifo nossos)

Embora, como se vê, a interação dialógica entre os conceitos de dignidade, autonomia e informação abra campo fértil de estudos no campo da teoria da democracia, da teoria dos direitos fundamentais – dentre tantos outros –, pretendemos adensar a discussão a respeito das

---

[127] O modelo 3C's (confiança, complacência e conveniência) foi desenvolvido pela Organização Mundial da Saúde (OMS) como metodologia de análise do fenômeno da aceitação vacinal, caracterizada por ser um "processo complexo que pode ser afetado por vários fatores" (Frugoli *et. al*, 2021, p. 2). A confiança se refere à credibilidade na eficácia das vacinas; a complacência se refere à postura de hesitação amparada em baixa compreensão sobre os riscos de doenças que poderiam ser evitadas com vacinas; a conveniência, por fim, envolve elementos como a disponibilidade dos imunizantes e a acessibilidade aos pontos de vacinação (*Idem*, *ibidem*).

[128] Lu (2024, p. 2) destaca a existência de duas perspectivas distintas sobre os reflexos da tomada de decisão algorítmica sobre a autonomia individual. A primeira propõe que algoritmos poderiam melhorar "a eficiência e a precisão decisórias, bem como fornecer serviços que melhor refletem os genuínos interesses e identidade individuais". A segunda se concentra nas questões éticas decorrentes da delegação de decisões à inteligência artificial, tais como "engano algorítmico, *nudging*, e manipulação, resultando em um desalinhamento entre as ações e os objetivos individuais" (tradução nossa).

repercussões do uso de técnicas maliciosas de *design* da arquitetura de plataformas digitais, chamadas de padrões obscuros, sobre a autonomia individual.

Em outros termos, importa-nos compreender em que medida a manipulação pelo emprego dos ditos padrões obscuros (também denominados *deceptive patterns* ou *dark patterns*) nas plataformas digitais interfere na manifestação (e na formação) autônoma da vontade individual nos ambientes virtuais, ao impor dificuldades para que os usuários exerçam direitos relacionados ao controle do fluxo de seus próprios dados pessoais e, sobretudo, ao criar estímulos que, de modo malicioso e sub-reptício, interferem em escolhas e comportamentos no mundo digital, de forma a – dentre outros objetivos – maximizar o compartilhamento de informações pelos indivíduos e a consequente extração de dados pessoais necessários a modelos de negócio que se nutrem de tais insumos[129].

O papel da *informação*, na complexa dinâmica da *manipulação digital*, não é menos importante. Muito ao contrário: na sociedade algorítmica, (acesso à) informação é poder[130]. Nessa perspectiva, controlar a extensão do conhecimento dos indivíduos acerca das práticas de tratamento de dados pessoais – e, portanto, a deliberação autônoma[131] a respeito de riscos e consequências – envolvidas no uso das plataformas digitais é fundamental para a economia movida a dados (e, também, para a *manipulação movida a dados*). Não por acaso, em contrapartida, a disponibilização de informações claras e transparentes a respeito das atividades de tratamento de dados pessoais e suas respectivas finalidades é um dos pilares de normas sobre a proteção de dados ao redor do mundo[132].

---

[129] "A economia política do capitalismo digital cria incentivos perversos para empresas de mídias sociais. Ela encoraja companhias a vigiar, viciar e manipular seus usuários finais e a fechar acordos com terceiros que irão manipulá-los ainda mais." (Balkin, 2018, p. 1, tradução nossa)

[130] "O poder derivado do conhecimento, e o conhecimento definido pelo poder, podem ser ainda mais dominantes quando há uma assimetria de conhecimento entre duas partes. Se, digamos, o Facebook sabe tudo o que há para saber sobre você, e você não sabe nada sobre o Facebook, então o Facebook terá mais poder sobre você do que se ambas as partes soubessem quantidades iguais uma da outra. A assimetria torna-se ainda mais acentuada se o Facebook souber tudo sobre você, e você achar que o Facebook não sabe nada, ou se você não souber o quanto o Facebook sabe. Isso torna você duplamente ignorante." (Véliz, 2021, p. 82)

[131] "Ao permitir que sejamos vigiados e sutilmente regulados de forma contínua, altamente granular e generalizada, podemos lentamente, mas seguramente, estar a corroer nossa capacidade para processos autênticos de autocriação e desenvolvimento." (Yeung, 2017, p. 131, tradução nossa)

[132] Ver, por exemplo, o art. 2º, III, da LGPD, que estabelece a *liberdade de informação* como um dos fundamentos da disciplina da proteção de dados pessoais. No contexto europeu, o Considerando 39 do RGPD dispõe que o princípio da transparência "exige que as *informações* ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples". O California Consumer Privacy Act (CCPA), de 2018, da mesma forma, estabelece que os negócios que coletam informações pessoais têm o dever geral de, "no momento ou antes da coleta, *informar* os consumidores sobre o seguinte: (1) As categorias de informações pessoais a serem coletadas e os propósitos para os quais as categorias de informações pessoais são coletadas ou usadas e se essas informações são vendidas ou compartilhadas" (tradução nossa).

Como vimos, na lógica do "pegar ou largar", a sujeição dos indivíduos ao modo de funcionamento das plataformas digitais se revela necessária à sua participação no mundo digital, à aquisição de bens e à contratação de serviços, circunstância que agrava as assimetrias (e acentua as vulnerabilidades[133]) de que já tratamos no capítulo anterior. Para além disso, mesmo intuitivamente se pode supor que empresas não anunciam[134] aos usuários de suas plataformas digitais o emprego de arquiteturas enganosas (mesmo porque a *ocultação*, nesse particular, é imprescindível à implementação bem-sucedida de mecanismos de extração massiva de dados pessoais) voltadas a fazer com que tomem decisões que as beneficiem[135].

É importante notar, ainda, que **a autonomia mantém relação simbiótica (ou simultânea) de causa e efeito com o direito à privacidade**[136], razão pela qual compreende-se necessário identificar, nesse estudo, os contornos da **manipulação em ambientes digitais** e **problematizar suas repercussões sobre a autonomia** e, de conseguinte, sobre a privacidade. Afinal, se, por um lado, a autonomia atribui ao indivíduo o poder de *controlar o que* se sabe, *quem* sabe, e *em que extensão* se sabe a respeito de aspectos de sua personalidade (a partir da imposição de limites ao fluxo das informações sobre si próprio), por outro, é com a delimitação de um âmbito privado, longe da vigilância e de interferências externas, que a autonomia ganha reforço. Com efeito, a existência de uma esfera individual privada permite que as pessoas se comportem e tomem decisões de acordo com suas próprias convicções, sem interferências[137] e sem o receio de sofrer retaliações ou perseguições futuras[138].

---

[133] "Como a tecnologia da informação torna a geração, coleta, análise e aproveitamento de tais dados sobre nós baratos e fáceis, e em uma escala dificilmente compreensível, a preocupação é que tais tecnologias nos tornem profundamente vulneráveis aos caprichos daqueles que constroem, controlam e implantam esses sistemas". (Susser; Roessler; Nissenbaum, 2019b, p. 2, tradução nossa)

[134] "A manipulação esconde informações vitais das pessoas, o que as priva de ser aptas a adequadamente considerar suas opções para exercer uma decisão que se alinhe com suas crenças e valores pessoais, e é, portanto, antiética, ao completamente desrespeitar a autonomia do decisor." (Botes, 2022, p. 318, tradução nossa)

[135] "A ocultação das influências manipulativas explica como é possível alienar alguém de seus próprios poderes de decisão. Para fazer com que alguém aja do jeito que você quer sem perceber *por que* ele está agindo daquela forma, ele não deve notar a influência. Assim que nos tornamos conscientes de influências externas, dos planos de outra pessoa e como estamos envolvidos neles, nós incorporamos essa influência em nossa própria tomada de decisão." (Susser; Roessler; Nissenbaum, 2019b, p. 20, tradução nossa)

[136] É no mesmo sentido a lição de Cohen (2000, p. 1424): "Devemos aprender a processar informações e tirar nossas próprias conclusões sobre o mundo ao nosso redor. Devemos aprender a escolher, e devemos aprender algo antes de escolhermos qualquer coisa. Aqui, entretanto, a teoria da informação sugere um paradoxo: 'Autonomia' conota uma independência essencial das faculdades críticas e uma impermeabilidade à influência." (Tradução nossa)

[137] "A ideia liberal nuclear de personalidade articulada em termos de autonomia pessoal requer que indivíduos possam escolher e perseguir seus diferentes planos ou caminhos de vida por si sós sem a interferência de outros […]." (Yeung, 2017, p. 129, tradução nossa)

[138] "[...] a autonomia sob a perspectiva da privacidade diz respeito à possibilidade de que as pessoas possam fazer escolhas e delas serem responsáveis, com base em seu caminho de vida, sem que para isso precisem expressar justificativas e sem que haja influência externa nessas decisões. A construção da identidade do ser transita pelos

Considerado esse contexto, um dos principais desafios impostos ao paradigma do controle (de que cuidaremos no Capítulo 3) está na proteção e na promoção da autonomia individual – por meio do empoderamento dos titulares de dados pessoais, para que exerçam os direitos inerentes à titularidade – em ambientes desenhados, implementados e administrados por agentes econômicos que procedem a partir de incentivos à extração crescente de dados pessoais[139].

2.1 Manipulação e riscos à autonomia individual no contexto das plataformas digitais

Em junho de 2014, Adam Kramer, Jamie Guillory e Jeffrey Hancock publicaram, no volume 111 do prestigioso periódico *Proceedings of the National Academy of Sciences* (PNAS), o artigo "Evidências experimentais de contágio emocional massivo através de redes sociais"[140]. No estudo, os pesquisadores concluíram que "estados emocionais podem ser transferidos a outros via contágio emocional, fazendo com que as pessoas experimentem as mesmas emoções sem que saibam" (Kramer; Guillory; Hancock, 2014, p. 8788, tradução nossa).

Para que o grupo, liderado por Kramer (cientista de dados do Facebook), chegasse à descoberta, o Facebook manipulou, durante uma semana, a exposição de quase 700.000 de seus usuários a conteúdos de teor positivo ou negativo nos seus *feeds* de notícias, a fim de avaliar "se a exposição a emoções levou as pessoas a mudar seus próprios comportamentos de postagem, em particular se a exposição a conteúdo emocional levou as pessoas a postarem conteúdos que fossem consistentes com a exposição [...], uma forma de contágio emocional" (*Idem*, *ibidem*, tradução nossa). Na publicação, os autores afirmam, também, que a implementação da técnica "foi consistente com a Política de Uso de Dados do Facebook, com a qual todos os usuários concordam antes de criar uma conta [...], constituindo consentimento informado para essa pesquisa" (*Idem*, p. 8789, tradução nossa).

A publicação gerou compreensível revolta. Afinal, a fim de medir o grau de influência do conteúdo apresentado nos *feeds* de notícias sobre as emoções humanas, o Facebook interferiu

---

meandros nem sempre fáceis da autonomia decisória, e, certamente, a proteção da dignidade pessoal de cada indivíduo tem como pressuposto o respeito àquele direito." (Freitas; Mezzaroba; Zilio, 2019, p. 171)

[139] "[...] pensadores como Thaler e Sunstein (2009) propõem a arquitetura de escolhas como uma tática que deve ser usada aberta e transparentemente pelos formuladores de políticas para promover o bem público. Os profissionais de marketing, por outro lado, buscam controle sobre a arquitetura de escolhas para promover os interesses de seus clientes. O que permanece contínuo em estratégias que se concentram na construção de significado ou na arquitetura de escolhas é que os profissionais de marketing e anunciantes estão seguindo seu impulso de explorar as vantagens estruturais que possuem – que agora podem incluir a capacidade de explorar sistematicamente os vieses e impulsos cognitivos dos consumidores." (Nadler; McGuigan, 2017, p. 153, tradução nossa)

[140] *Experimental evidence of massive-scale emotional contagion through social networks*, no título em inglês.

nas publicações vistas por centenas de milhares de pessoas, impingindo-lhes estados emocionais como tristeza, angústia e melancolia. Assim, à época, repercutiu o portal *Animal New York*[141] sobre o experimento: "o que muitos de nós temíamos já é uma realidade: o Facebook está nos usando como ratos de laboratório, e não apenas para entender a que anúncios vamos responder, mas para *efetivamente mudar nossas emoções*" (tradução nossa).

As reações negativas fizeram com que Kramer viesse a público formalizar um pedido de desculpas pela "forma como o artigo descreveu a pesquisa e qualquer ansiedade que ele tenha causado"[142] (tradução nossa). A nota pública, entretanto, não deixou de consignar que a pesquisa fora realizada "porque nós [os autores] nos importamos com o impacto emocional do Facebook e com as pessoas que usam nosso produto"[143] (tradução nossa).

Para além das discussões éticas envolvidas na manipulação do estado emocional de mais de meio milhão de indivíduos para fins de pesquisa sobre os potenciais do "contágio emocional" a partir do *feed* de publicações do Facebook, o caso descortina preocupações ainda maiores com relação ao poder que as plataformas digitais podem exercer sobre o comportamento individual. Além disso, a retratação pública de Kramer é reveladora de uma lógica segundo a qual quaisquer finalidades que possam se encaixar em expressões genéricas, como "melhorar nossos serviços" ou "recomendar conteúdos mais interessantes"[144], ainda que de duvidosa ética, estariam amparadas pelo mero consentimento com os usos de dados pessoais (sem o qual, aliás, sequer seria possível criar um perfil na plataforma) previstos em políticas de privacidade.

No caso concreto, dispunham as políticas do Facebook, à época, que as informações de seus usuários poderiam ser usadas "para operações internas, incluindo solução de problemas, análise de dados, testes, **pesquisas** e melhoria do serviço"[145] (tradução e grifo nossos). Assim, a anuência das "cobaias" do experimento com os termos de uso da plataforma seria, para todos os efeitos, suficiente para o emprego de técnicas de *pesquisa* (muito embora consistissem, essencialmente, em *manipulação*) voltadas a testar a extensão do impacto dos conteúdos apresentados pelo Facebook sobre os estados emocionais de seus usuários. Para os autores, a

---

[141] Disponível em: https://animalnewyork.com/2014/06/27/facebook-experiment-manipulates-emotions-600000-users/. Acesso em: 12 nov. 2024.

[142] Disponível em: https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html. Acesso em: 12 nov. 2024.

[143] Disponível em: https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html. Acesso em: 12 nov. 2024.

[144] "Qualquer declaração de vontade deve ter um direcionamento, já que não se consente no vazio e de forma genérica. Seria o equivalente a emitir uma espécie de "cheque em branco" que esvaziaria qualquer esfera de controle do cidadão sobre seus dados. Em termos práticos, o famoso 'para fins de melhorar a sua experiência', constante de inúmeras políticas de privacidade, deve ser abandonado." (Bioni, 2020, p. 186)

[145] Disponível em: https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/. Acesso em: 12 nov. 2024.

concordância com o uso de dados pessoais para "pesquisas" afastaria alegações de que os indivíduos teriam sido manipulados pela rede social.

A manipulação consiste, de fato, em um dos principais desafios impostos ao exercício da autonomia no ambiente digital. As assimetrias informacionais de que já tratamos dão às empresas que exploram as plataformas digitais sofisticada compreensão a respeito do perfil comportamental de seus usuários[146], tornando-se possível, dessa forma, conhecer e explorar[147] vulnerabilidades, vieses comportamentais e heurísticas, para que ajam ou decidam neste ou naquele sentido. Cabe anotar que a manipulação, no mundo digital, não se resume a apenas uma técnica ou modo de proceder, sendo cada vez mais criativos os mecanismos de interferência no processo decisório dos indivíduos, assim como vários são os objetivos a que pode servir[148]. Como demonstra o caso do estudo de Kramer e outros, as *emoções* dos usuários podem ser manipuladas (e, consequentemente, também o seu comportamento) a partir de uma simples exposição continuada a conteúdos que expressem tristeza ou alegria.

Vê-se, assim, que o *comportamento* e a *tomada de decisão* dos usuários (não apenas no ambiente digital, como também no mundo real) é passível de manipulação a partir do uso de funcionalidades aparentemente inofensivas – e até mesmo recebidas com entusiasmo – das plataformas digitais. Zuboff (2020, p. 354), nesse sentido, trata do caso envolvendo o jogo de realidade aumentada *Pokémon Go*, desenvolvido pela empresa Niantic Labs, que representou um verdadeiro avanço no potencial manipulativo das plataformas digitais[149].

O objetivo do jogo, de grande sucesso comercial em meados de 2016, era o de capturar criaturas fictícias que se tornavam visíveis a partir do uso da câmera do telefone celular. O mapa de *Pokémon Go* indicava aos jogadores, por meio do GPS, em que locais do mundo físico se

---

[146] "Os vastos estoques de informações e perfis comportamentais detalhados compilados sobre cada indivíduo facilitam muito as práticas manipuladoras. Quanto mais se sabe sobre a personalidade, preferências, hábitos e vulnerabilidades de cada pessoa, mais fácil é construir ambientes de escolha que irão guiar sua tomada de decisão na direção desejada." (Susser; Roessler; Nissenbaum, 2019b, p. 38, tradução nossa)

[147] "O extremo conhecimento que agentes econômicos e políticos têm dos indivíduos a partir dos seus dados pessoais possibilita uma série de classificações e perfilizações a partir das quais se viabiliza o microdirecionamento de conteúdos de qualquer espécie, seja comercial, seja político, seja de notícias, ainda quando estas sejam falsas ou meros disfarces de pura propaganda comercial ou política." (Frazão, 2024, p. 9)

[148] Em 2017, o Facebook protagonizou outro escândalo, envolvendo usuários adolescentes, que veio a conhecimento do público pelo vazamento de documentos internos. Relatórios produzidos por executivos da empresa na Austrália, direcionados a anunciantes, demonstravam como o Facebook "consegue monitorar postagens e fotos em tempo real para determinar quando jovens se sentem 'estressados', 'derrotados', 'sobrecarregados', 'ansiosos', 'nervosos', 'burros', 'idiotas', 'inúteis' e um 'fracasso'" (Disponível em: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens. Acesso em: 1 dez. 2024).

[149] Segundo Zuboff (2020, p. 357), o *Pokémon Go* "oferecia um laboratório vivo para *telestimulation* em escala à medida que os donos do jogo aprendiam como condicionar e pastorear o comportamento coletivo, dirigindo-o para constelações em tempo real de mercados de comportamentos futuros".

encontravam os *pokémons*, como numa espécie de caça ao tesouro, dando à Niantic Labs a possibilidade de negociar o comportamento futuro de usuários (i.e., a certeza de que centenas de jogadores se deslocariam) com negócios do mundo real (ou "locais patrocinados"). Como diz Zuboff (2020, p. 362),

> [a] noção de "locais patrocinados" é um eufemismo para os mercados de comportamentos futuros da Niantic [...]. Os elementos e a dinâmica do jogo, combinados com a novíssima tecnologia de realidade aumentada, operam de modo a pastorear populações de jogadores mediante pontos de checagem de monetização no mundo real. Estes são constituídos pelos verdadeiros clientes do jogo: as entidades que pagam para jogar no tabuleiro do mundo real, atraídos pela promessa de resultados garantidos.

Helberger *et al*. (2021, p. 191) mencionam o *Pokémon Go*, noutra perspectiva, como exemplo eloquente de como a mitigação da privacidade acentua a vulnerabilidade no ambiente digital. A extração massiva de dados pessoais conferia à Niantic Labs um manancial de informações a respeito das diferentes formas de interação de cada jogador com o aplicativo. Esse conjunto de dados permitiu que a empresa testasse, continuamente, diferentes estratégias para induzir a compra de itens virtuais (para viabilizar o uso de uma ou mais funções específicas ou dar certa vantagem ao jogador). Além disso, a análise massiva de dados pessoais incrementou as possibilidades de manipulação em *Pokémon Go*, tornando o jogo viciante para seus usuários, e dando à Niantic Labs conhecimento detalhado sobre o comportamento e as necessidades de cada jogador[150], de modo que pudesse estruturar suas ações comerciais a partir de um cenário de razoável certeza a respeito dos comportamentos futuros.

Dos botões de *like* nas redes sociais à *gamificação*[151], é amplo o leque de estratégias de manipulação dos usuários de plataformas digitais[152]. Os padrões obscuros, de que trataremos no tópico seguinte, também se revelam, eles próprios, como poderoso mecanismo de interferência sub-reptícia nos processos decisórios individuais no ciberespaço, comprimindo o âmbito de exercício da escolha autônoma dos indivíduos. Implementados de modo oculto,

---

[150] Como notam, acertadamente, Susser, Roessler e Nissenbaum, "os sistemas digitais com os quais as pessoas interagem estudam tanto as suas idiossincrasias individuais quanto os padrões que emergem entre os grupos demográficos aos quais elas pertencem, potencialmente revelando fraquezas e disposições que os indivíduos, eles próprios, não conseguem ver" (2019b, p. 32, tradução nossa).

[151] "O design pode nos manipular a fazer escolhas que servem a interesses corporativos, ao invés dos nossos. Vemos isso por todo o ecossistema digital. O Facebook nos diz quando nossos amigos 'curtiram' uma página, nos encorajando a fazer o mesmo; as assim chamadas *dark patterns*, ou truques de design que nos manipulam a tomar certas ações online, despertam nossa preferência por botões brilhantes e coloridos, ao invés dos cinzas; plataformas nos incentivam a comprar produtos que outros compraram antes de nós; e apps *gamificam* o compartilhamento ao encorajar-nos a continuar uma 'onda' com nossos amigos." (Waldman, 2021, p. 165, tradução nossa)

[152] "Progressivamente são colocadas em prática inúmeras estratégias de empresas e governos que, por meio de uma série de técnicas de manipulação, trazem evidentes riscos à privacidade mental dos indivíduos e ao livre pensamento." (Frazão, 2024, p. 3)

produzem nos usuários a impressão de que a decisão em um ou em outro sentido resulta do exercício livre de sua autonomia. Como ilustram os casos da pesquisa de Kramer e do *Pokémon Go*, compreender o fenômeno da manipulação no contexto das plataformas digitais é necessário para que sejam adequadamente visualizadas (e apropriadamente endereçadas) as ameaças à autonomia individual no ciberespaço[153].

Para tanto, cabe, antes de mais nada, incursionarmos brevemente no sentido de *manipulação* em uma perspectiva geral. Trata-se, efetivamente, de conceito polissêmico; todavia, na acepção que nos importa, manipulação designa o exercício velado de influência – em grau variado – sobre o comportamento e, particularmente, sobre o processo decisório individual, buscando-se atingir os fins perseguidos pelo manipulador a partir da *instrumentalização da agência humana*[154], que se dá por meio do emprego de estratégias que exploram vieses cognitivos, vulnerabilidades e heurísticas, "de modo a impossibilitar uma tomada de decisão autônoma" (Frazão, 2024, p. 4).

Nessa mesma perspectiva, Spencer (2020, p. 990) propõe, a partir do estudo de definições apresentadas por diversos autores (como Daniel Susser, Cass Sunstein, Tal Zarsky, Ryan Calo e outros), um conceito de manipulação baseado na *intencionalidade* e na *exploração de vieses cognitivos*. Segundo o autor, "manipulação é uma tentativa intencional de influenciar o comportamento de um sujeito ao explorar um viés ou vulnerabilidade" (tradução nossa). Assim, ausentes a interferência e o ardil do manipulador, o manipulado provavelmente seria capaz de fazer escolhas que não necessariamente beneficiassem aquele[155].

Vale destacar, todavia, que nem sempre a manipulação serve a objetivos espúrios ou prejudiciais a quem se manipula: como lembram Susser, Roessler e Nissenbaum, "é possível manipular alguém para que tome decisões mais ideais" (2019a, p. 19, tradução nossa). Em

---

[153] O combate ao uso de técnicas de manipulação, segundo Spencer (2020, p. 991), se justifica por quatro razões fundamentais. Em primeiro lugar, pelo enfraquecimento das capacidades de tomada de decisão das pessoas; em segundo lugar, pela geração de resultados ineficientes, na medida em que os indivíduos farão escolhas em desconformidade com suas reais preferências; em terceiro, pelos prejuízos à deliberação democrática; e, finalmente, em quarto, pela redução dos indivíduos a *meios* para o atingimento de realização dos objetivos desejados por outrem. No mesmo sentido, cf. Zarsky, 2019, p. 174.

[154] "Ainda, uma terceira forma de articular o argumento baseado na manipulação é notar que tais ações são inaceitáveis porque equivalem à experimentação humana. Por trás da declaração populista está um argumento muito mais profundo, de que a conduta que caracteriza indivíduos tratando os outros como meios para um fim, ao invés de provê-los do nível de respeito apropriado, é socialmente inaceitável." (Zarsky, 2019, p. 175, tradução nossa)

[155] "Onde a influência falha e o influenciador não atinge seu objetivo, não se pode dizer que alguém tenha sido manipulado, mas o ato de influenciar em si ainda conta como manipulativo. Mesmo um ato malsucedido de tentativa de influência manipulativa desrespeita a autonomia do outro. Considerando isso, é convincente dizer que uma influência pode ser manipulativa mesmo quando a pessoa influenciada não teria agido de modo diferente sem a influência." (Grisse, 2023, p. 110, tradução nossa)

complemento, Grisse (2023, p. 110) cita as hipóteses em que órgãos do Estado ajam em defesa do interesse público, ou em que pais – sobre os quais recai o dever de cuidado – interfiram no comportamento de seus filhos, agindo em seu melhor interesse[156]. O mesmo, aliás, pode se verificar no contexto da arquitetura de plataformas digitais[157].

A seu turno, Sunstein (2016, p. 6) assevera que "um esforço para influenciar as escolhas das pessoas conta como manipulativo na medida em que não envolva ou apele **suficientemente** à sua capacidade de reflexão e deliberação" (tradução e grifo nosso). De fato, a busca pela produção de *influência sobre comportamentos e decisões individuais* não é, propriamente, uma novidade, sendo o apelo à capacidade de decisão individual um elemento contextual potencialmente descaracterizador do fenômeno da manipulação[158].

Afinal, além da manipulação, pode-se cogitar da persuasão, da coerção ou até mesmo dos *nudges* (ou "pequenos empurrões") – na expressão cunhada por Sunstein e Thaler[159] – como métodos, nem todos lícitos, de interferir sobre o comportamento e sobre as escolhas dos indivíduos. A disposição de mercadorias nas gôndolas de supermercados, por exemplo, não é aleatória. Ao contrário, estrutura-se a partir de análises de padrões de comportamento dos consumidores, que tendem a colocar em seus carrinhos os produtos que estejam mais facilmente em seu campo de visão. Embora supermercados não costumem avisar os consumidores dos critérios que utilizam para organizar suas prateleiras, o apelo a vieses comportamentais, nesse caso, não se mostra necessariamente manipulativo, na medida em que os indivíduos conservam o poder de deliberação, compreendendo a existência de outras opções, pelo que mantêm a consciência da autoria de suas próprias decisões ao fazerem compras.

A *persuasão* pressupõe o apelo à própria faculdade individual de tomada de decisão. Busca-se, com ela, expor de modo convincente as razões em favor da decisão em um ou em outro sentido. Em todo o caso, o sujeito é *livre*, tanto para avaliar fatos e argumentos de acordo

---

[156] Não por outra razão, a *redução do bem-estar* do indivíduo manipulado é elemento fundamental da definição de manipulação estabelecida por Balkin (2018, p. 4). Os outros dois componentes de seu conceito são o aproveitamento de vulnerabilidades emocionais ou da falta de conhecimento do manipulado e a intenção do manipulador de obter benefício para si ou para outrem.

[157] "Um *design* que é manipulativo, mas não malicioso, pode ser considerado moralmente problemático, pois o designer está tentando encorajar o usuário a tomar um curso de ação diferente por meio da exploração de vieses cognitivos. No entanto, apesar dos meios ilícitos, o objetivo final pode ser benéfico, derivando de um *background* de *design* ético [...]." (Jarovsky, 2023, p. 6, tradução nossa)

[158] "Entre a persuasão e a manipulação há um amplo leque de tecnologias de engenharia tecno-social que visam a impactar a maneira como as pessoas pensam, percebem as informações e agem de acordo com elas." (Botes, 2022, p. 317, tradução nossa)

[159] Segundo os autores, o *nudge* "é um estímulo, um empurrãozinho, um cutucão: é qualquer aspecto da arquitetura de escolhas capaz de mudar o comportamento das pessoas de forma previsível sem lhes vetar qualquer opção e sem introduzir nenhuma mudança significativa em seus incentivos econômicos" (2023, p. 21).

com suas próprias convicções no curso de seu processo decisório, quanto para decidir sem ameaças ou receios de retaliações, muito embora as consequências da tomada de decisão componham, amiúde, o quadro geral dos elementos a serem considerados. Além do mais, o indivíduo *tem consciência* do apelo de outrem à sua capacidade decisória, na medida em que a persuasão se apresenta de modo claro e aberto.

Por outro lado, a *coerção* representa constrição ilegítima da esfera decisória do indivíduo, restringindo-se o âmbito de escolha a uma única alternativa válida (aquela desejada por quem exerce a coerção), seja pela eliminação de alternativas aceitáveis, seja pela imposição de incentivos irresistíveis. Assim como a persuasão, a coerção promove uma interferência sobre o âmbito decisório do sujeito (embora, aqui, se trate de influência ilegítima). Tanto em um quanto em outro caso, o indivíduo conserva a consciência sobre a tomada de decisão, muito embora, na coerção, adotar comportamento em sentido contrário ao pretendido pelo agente externo em geral represente algum prejuízo imediato ou futuro a quem decide.

Na classificação proposta por Susser, Roessler e Nissenbaum (2019a, p. 13), em uma acepção *ampla*, persuasão pode envolver tanto a *persuasão racional* (persuasão em acepção *estrita*), quanto a coerção, na medida em que, em ambas, o indivíduo conserva a consciência das influências externas; além disso, não há subversão[160] de seu poder de decidir. A distinção entre os dois possíveis significados da persuasão é relevante, dizem os autores, por suas diferentes conotações normativas. Assim, a persuasão "no sentido estrito é usualmente compreendida como perfeitamente aceitável moralmente, enquanto a persuasão no sentido amplo denota comportamentos que aceitamos e comportamentos que não aceitamos" (*Idem*, p. 14, tradução nossa)

Os autores ilustram a distinção com o exemplo em que se busca persuadir um sujeito a escolher entre as opções A e B a partir da apresentação de argumentos ou mesmo da oferta de benefícios (*persuasão racional*), ou, então, busca-se persuadir um sujeito a escolher entre as opções A e B *com uma arma apontada para a sua cabeça* (*coerção*). Embora, nesse caso, haja apenas uma alternativa válida – partindo-se do pressuposto que o indivíduo deseje resguardar sua vida –, a consciência do exercício da decisão (e a consciência sobre ela) ainda permanece consigo[161].

---

[160] "De fato, a natureza subconsciente da manipulação é uma razão pela qual a manipulação é tão poderosa. [...]. Independentemente de se o estímulo manipulativo é visível ou oculto, se o sujeito não sabe como ou por que o estímulo afeta a sua tomada de decisão, então o seu poder de decisão continua subvertido." (Spencer, 2020, p. 990, tradução nossa)

[161] Como bem elucidam os autores: "Persuadir alguém deixa a escolha do assunto inteiramente a seu cargo, enquanto coagir alguém priva-o de escolha. Ao mesmo tempo, embora coagir alguém o prive de escolha, num

A diferença de tais conceitos para o de manipulação reside, essencialmente, em que, neste, o agente externo (manipulador) subverte o processo decisório do indivíduo (manipulado) sem que ele se dê conta disso[162], explorando-se vieses cognitivos, limitações de racionalidade e vulnerabilidades de modo ilegítimo (pelo ardil ou engano), ou mesmo impondo-lhe falsas representações da realidade[163]. Ademais, a própria formação da *vontade* individual pode sofrer interferências ilegítimas por meio da manipulação[164].

Por sua própria definição, portanto, a manipulação é a negação da decisão autônoma *paradigmática*, tomada "por um indivíduo mentalmente competente, e totalmente informado, alcançada por meio de um processo de autodeliberação racional, de modo que o resultado escolhido pelo indivíduo possa ser justificado e explicado com referência às razões que o agente identificou e endossou" (Yeung, 2017, p. 124, tradução nossa).

Como intuitivo, para que uma estratégia de manipulação seja bem-sucedida, é importante conhecer as vulnerabilidades e vieses cognitivos do manipulado, o que depende de um prévio entendimento a respeito de traços característicos de sua personalidade, de seu comportamento e de seus padrões decisórios. No paradigma da sociedade algorítmica, aliás, o uso de inteligências artificiais amplificou sobremaneira os potenciais de uma *leitura completa* sobre características diversas dos indivíduos, trazendo consigo os *custos sociais* – dentre os quais o de manipulação – sobre os quais discorrem Mills, Costa e Sunstein. Para esses autores, "a IA pode ser usada para conduzir os consumidores em direções que não sejam em seus melhores interesses, talvez ao explorar uma falta de informação ou vieses comportamentais" (2023, p. 393, tradução nossa).

---

sentido importante, deixa intacta a sua capacidade de tomada de decisão consciente. Afinal, reconhecer que algum incentivo é irresistível, ou que uma alternativa é inaceitável, exige que tenhamos o nosso juízo sobre nós." (Susser; Roessler; Nissenbaum, 2019a, p. 15, tradução nossa)

[162] "Ao contrário da persuasão, que é o apelo direto ao poder de decisão de outra pessoa, ou da coerção, que é a restrição das opções aceitáveis entre as quais outra pessoa pode escolher, a manipulação funciona a partir da exploração das fraquezas cognitivas (ou afetivas) e das vulnerabilidades do manipulado para conduzir seu processo de tomada de decisão rumo aos objetivos do manipulador." (Susser; Roessler; Nissenbaum, 2019a, p. 3, tradução nossa)

[163] Nesse sentido, Hoofnagle *et al*. (2012, p. 294) observam que uma "combinação de tecnologias de rastreamento disfarçadas, técnicas de invalidação de escolha e modelos para enganar os consumidores a revelar dados sugere que os anunciantes não veem os indivíduos como seres autônomos" (tradução nossa).

[164] Como asseveram Verbicaro, Rodrigues e Ataíde (2018, p. 361), "a indústria cultural se vale de estudos sobre o comportamento humano para entender a psique dos indivíduos e, assim, manipular suas vontades através dos estímulos adequados para fomentar nestes uma ânsia em se atender aos padrões de consumo impostos".

Há vasta literatura no campo da psicologia e da economia comportamentais[165] a respeito do tema, que colocou em xeque o paradigma da racionalidade cartesiana[166] do *homo economicus*, reconhecendo e catalogando, ao revés, "uma longa lista de vieses cognitivos [...] que podem ser aproveitados por potenciais manipuladores para influenciar a trajetória de nossa tomada de decisões ao moldar nossas crenças, sem a necessidade de enganar completamente" (Susser; Roessler; Nissenbaum, 2019b, p. 5, tradução nossa)[167]. Além do mais, sabe-se que as decisões individuais são, também, influenciadas pela interação entre diversos fatores contextuais[168] (ambientais, sociais e econômicos, para além dos psicológicos e emocionais).

A superação do paradigma da racionalidade ilimitada dos indivíduos é especialmente importante na discussão a respeito do emprego de técnicas de manipulação em arquiteturas digitais e sua interface com a proteção de dados pessoais. De fato, em se considerando – como será mais bem explorado no próximo subcapítulo – que padrões obscuros se baseiam na exploração de vieses cognitivos para manipular usuários, mitigando (ou, em muitos casos, eliminando) o seu efetivo potencial de controlar o fluxo de dados pessoais e de avaliar adequadamente as consequências (a médio e longo prazo) de suas decisões a respeito de sua privacidade, os padrões obscuros "tornam o modelo do *Homo Economicus* fortemente implausível – e até mesmo errado – no ambiente da proteção de dados" (Jarovsky, 2023, p. 47, tradução nossa).

Ainda nesse particular, a formulação de Kahneman (2012) nos ajuda a visualizar os diferentes *sistemas* envolvidos na tomada de decisão, dando-nos conta de que as decisões humanas – ao contrário do que propõe o paradigma da racionalidade, criticado, dentre outros, por Akerloff e Shiller[169] – muitas vezes não decorrem da reflexão, da ponderação e da avaliação

---

[165] "Estudos na psicologia cognitiva e comportamental indicam instâncias previsíveis nas quais indivíduos sistematicamente agem irracionalmente – indicações de que estes podem ser abusados pelas entidades manipuladoras." (Zarsky, 2019, p. 169, tradução nossa)

[166] "Esse tipo de questão de *design* não é algo típico para economistas pensarem porque economistas têm uma concepção de comportamento humano que assume, implicitamente, que todos confiam completamente em seu sistema reflexivo, e um muito bom nisso! Presume-se que agentes econômicos raciocinem brilhantemente, cataloguem enormes quantidades de informações que podem acessar instantaneamente de suas memórias e exerçam uma força de vontade extraordinária." (Sunstein; Thaler; Balz, 2010, p. 4, tradução nossa)

[167] No mesmo sentido, cf. Nadler e McGuigan (2017, p. 161): "Os vieses cognitivos sistêmicos identificados pela economia comportamental contribuem para as condições de vulnerabilidade, assim como os 'gatilhos de eventos de vida', como o casamento ou o divórcio, que podem induzir escassez de tempo ou estados emocionais temporários que [...] os profissionais de marketing viram e tentam explorar." (Tradução nossa)

[168] "A autonomia não é puramente individualista, mas relacional e em princípio compatível com fatores externos que influenciam as decisões dos indivíduos" (Brenncke, 2024, p. 19, tradução nossa)

[169] "Há uma história em relação aos livres mercados que é bastante aceita nos Estados Unidos e também exerce influência no exterior. Essa história vem de uma interpretação natural da economia padrão. Ela diz que a economia dos livres mercados, sujeita às advertências da distribuição da receita e externalidades, produz o melhor possível. Simplesmente deixe alguém ser 'livre para escolher', diz o mantra, e teremos um paraíso na

de custos e benefícios (Sistema 2), mas, sim, do pensamento rápido (Sistema 1). Em suas palavras, o Sistema 1 "detecta relações simples [...] e se sobressai em integrar informação sobre uma coisa, mas ele não lida com tópicos distintos e múltiplos de uma vez" (Kahneman, 2012, p. 49). O Sistema 2, a seu turno, "é o único que pode seguir regras, comparar objetos com base em diversos atributos e fazer escolhas deliberadas a partir de opções" (*Idem*, *ibidem*).

O reconhecimento da existência de modos distintos de fazer escolhas é importante para a compreensão da interferência dos padrões obscuros no contexto das plataformas digitais, na medida em que, como acertadamente observam Luguri e Strahilevitz (2021, p. 44), os *dark patterns* "normalmente levam os usuários a confiar na tomada de decisão do Sistema 1 em vez dos processos mais deliberados do Sistema 2, explorando vieses cognitivos como efeitos de enquadramento, a falácia do custo irrecuperável e a ancoragem" (tradução nossa). Como também reconhece Brenncke (2024, p. 8), há diversas pesquisas empíricas no campo da economia comportamental que demonstram a recorrência com que as decisões de consumidores ficam distantes de uma racionalidade econômica, "o que os torna previsíveis e exploráveis por práticas comerciais como arquiteturas de escolha online" (tradução nossa).

Para corrigir prejuízos causados pelos ditos vieses, a figura dos "*nudges*" se apresenta como uma interferência essencialmente benéfica no processo decisório que busca reduzir os potenciais danos que os indivíduos venham a causar a si próprios por conta de suas limitações cognitivas. São conhecidos, nesse sentido, os exemplos da ordem de disposição dos alimentos em cafeterias[170] e em refeitórios escolares, nos quais, para estimular nos alunos uma alimentação mais saudável, legumes e vegetais são apresentados antes dos alimentos doces, ultraprocessados ou gordurosos (por modificações no que Thaler e Sunstein denominam de *arquitetura de escolhas*[171]).

Ainda na seara conceitual, distinguir adequadamente a manipulação dos *nudges* é fundamental[172], sobretudo porque estes, assim como aquela, não se revelam como interferências

---

Terra, tão próximo do Jardim do Éden quanto nossa tecnologia existente, capacidade humana e distribuição de renda permitirem." (Akerloff; Shiller, 2016, p. 154)

[170] "Thaler e Sunstein destacam como o contexto de escolha decisória circundante pode ser intencionalmente projetado de maneiras que influenciam sistematicamente a tomada de decisão humana em direções específicas. Por exemplo, para encorajar os clientes a escolher itens alimentares mais saudáveis, eles sugerem que gerentes de cafeteria posicionem as opções saudáveis de forma mais proeminente – como colocar as frutas na frente do bolo de chocolate." (Yeung, 2017, p. 120, tradução nossa)

[171] "Um arquiteto de escolhas tem a responsabilidade de organizar o contexto no qual as pessoas tomam decisões. [...] muitas pessoas desempenham esse papel no mundo real – e a maioria nem se dá conta disso." (Thaler; Sunstein, 2023, p. 17)

[172] "Assim como na manipulação, moldar intencionalmente a arquitetura de escolhas de alguém em uma direção específica envolve influenciar o seu processo decisório sem força. Mais ainda, os *nudges* em geral funcionam alavancando vieses cognitivos. Aqueles familiarizados com a crescente literatura sobre *nudges* reconhecerão

ostensivas sobre o poder de decisão individual. De acordo com Susser, Roessler e Nissenbaum (2019a, p. 26), a manipulação é direcionada e, para tanto, depende do conhecimento e da exploração das vulnerabilidades e dos vieses cognitivos dos indivíduos para que sejam atingidos objetivos que favorecem o manipulador. Os *nudges*, ao contrário, têm, por definição, o intuito de auxiliar os indivíduos a tomarem decisões que lhes sejam mais benéficas (consumir mais vegetais ao invés de ultraprocessados, por exemplo), sem, contudo, vedar-lhes a tomada de decisões que possam causar-lhes prejuízos a curto, médio ou longo prazo. Os *nudges* buscam corrigir vieses decisórios; a manipulação busca aproveitar-se deles para beneficiar a outrem.

Importa-nos, contudo, ressalvar a posição de Klenk e Hancock (2019, p. 1), que questionam a compreensão de manipulação vinculada à perda de autonomia. Para os autores, indivíduos poderiam ser manipulados e conservar plenamente sua autonomia pessoal, na medida em que não haveria, ao contrário do que propõem Susser, Roessler e Nissenbaum (2019a), uma ligação conceitual entre manipulação e falta de autonomia. Klenk e Hancock afirmam que a visão de autonomia defendida pelos três autores antes mencionados seria essencialmente *externalista* (isto é, baseada na compreensão de que a autonomia individual consiste na capacidade de compreender e endossar as razões por trás de uma determinada ação).

Os autores utilizam como exemplo um aplicativo fictício chamado *Breakthrough*, que teria o propósito de fazer com que seus usuários sejam autônomos e tomem decisões autênticas e livres de expectativas e convenções sociais, lembrando-os de seus objetivos e criando oportunidades para que sempre reflitam e revisitem seus motivos e propósitos. Nessa hipótese, os usuários seriam autônomos na perspectiva externalista – porque compreendem e endossam as motivações e as razões de suas ações –, mas, ao mesmo tempo, poderiam estar sendo manipulados pelo aplicativo, que "parece exercer uma influência **avassaladora** e **ilegítima** em seu comportamento" (Klenk; Hancock, 2019, p. 8, tradução e grifo nossos).

A crítica de Klenk e Hancock, todavia, não enfrenta alguns aspectos importantes da construção teórica de Susser, Roessler e Nissenbaum. Para estes, importa recordar, a manipulação está no aproveitamento malicioso de vieses e limitações cognitivas do manipulado, sem o seu conhecimento, para atingir finalidades que podem interessar apenas ao manipulador. Além disso, se o aplicativo imaginado por Klenk e Hancock apela à capacidade deliberativa de seus usuários, para que *reflitam sobre* e *potencialmente revisitem* suas motivações (essas as expressões utilizadas pelos autores), seu modo de funcionamento não é

---

muitas de suas principais características em nossa caracterização da manipulação como influência oculta e nossa descrição da exploração de vulnerabilidades como o principal meio de manipulação." (Susser; Roessler; Nissenbaum, 2019a, p. 23, tradução nossa)

efetivamente manipulativo, aproximando-se mais do uso da persuasão racional. Afinal, não se trata de uma influência *oculta* que explora vieses e vulnerabilidades dos usuários (elementos fundamentais da definição de manipulação estabelecida por Susser, Roessler e Nissenbaum).

De todo modo, Klenk e Hancock não deixam claro o que, afinal, entendem por manipulação (e em que medida o aplicativo *Breakthrough* estaria manipulando seus usuários). Dizem, apenas, que ela não é incompatível com a noção *externalista* de autonomia. Se o usuário do aplicativo resolve, voluntariamente, delegar suas decisões existenciais a um aplicativo criado para esse fim, não há que se cogitar de manipulação (não há um agente externo se aproveitando de seus vieses e limitações cognitivas); em sentido contrário, se decisões individuais decorrem da exploração oculta de vieses cognitivos e de vulnerabilidades, terá havido manipulação.

Se, por um lado, uma decisão individual autônoma não pressupõe a total falta de interferências externas, por outro, os autores tampouco discutem a noção de manipulação enquanto interferência ilegítima qualificada pela ocultação e pelo engano[173]. Como dizem Susser, Roessler e Nissenbaum (2019a, p. 26), a manipulação envolve influenciar crenças, desejos, emoções, hábitos ou comportamentos sem a consciência do indivíduo, ou por meio de expedientes que "frustrariam sua capacidade de se tornar ciente disso" (tradução nossa). Em verdade, a manipulação é intrinsecamente antagônica à autonomia e à dignidade individuais, como ensina Sunstein (2016, p. 18):

> Do ponto de vista da autonomia, o problema é que a manipulação pode privar as pessoas de agência, repousando em um contínuo para o qual a coerção é o ponto final. [...] Do ponto de vista da dignidade, o problema é que a manipulação pode ser humilhante. Adultos saudáveis, que não sofrem de falta de capacidade, não devem ser enganados; eles devem ser tratados como totalmente capazes de tomar suas próprias decisões. Sua autoridade sobre suas próprias vidas não deve ser minada por abordagens que os tratem como crianças ou como fantoches. Um ato de manipulação não trata as pessoas com respeito. (Tradução nossa)

Explorar os aspectos conceituais das noções antagônicas de manipulação e autonomia se revela como tarefa importante ao ter-se em perspectiva as suas potenciais repercussões sobre a órbita jurídica individual e, além do mais, ao considerar-se o necessário dimensionamento da resposta legal-regulatória a ser oferecida pelo Direito[174] à implementação de estratégias de subversão dos processos decisórios individuais *no ciberespaço*, à vista de suas complexas

---

[173] "O engano é um erro moral *prima facie* porque viola a autonomia da pessoa enganada, envolvendo o controle de outra sem o consentimento dessa pessoa." (Yeung, 2017, p. 127, tradução nossa)

[174] "Tanto em contextos tradicionais quanto online, os atores legais têm que tomar decisões difíceis sobre onde está a linha precisa entre persuasão e manipulação, e qual conduta é enganosa o suficiente para eliminar o que poderiam ser direitos constitucionalmente protegidos dos vendedores de se envolverem em discurso comercial." (Luguri; Strahilevitz, 2021, p. 46, tradução nossa).

repercussões existenciais, políticas, econômicas e sociais, sobretudo no delicado contexto socioeconômico brasileiro, de que trataremos no Capítulo 3.

Muito embora a manipulação, *per se*, não seja algo novo, os danos que por ela podem ser causados à esfera individual (e coletiva) ganharam expressão inédita no contexto do uso ubíquo de plataformas digitais[175]. Afinal, como tivemos ocasião de referir, trata-se de ambiente permeado pela lógica de extração massiva de dados pessoais; caracterizado pelo controle quanto à extensão do conhecimento das práticas de tratamento por trás das interfaces digitais; marcado pela formação de perfis comportamentais altamente precisos e granularizados que, a um só tempo, cada vez mais acentuam assimetrias informacionais e viabilizam a exploração de vieses cognitivos e de vulnerabilidades. A formação de perfis de persuasão é apenas a ponta do *iceberg* (Helberger *et al.*, 2021, p. 176) no delicado problema da manipulação *online*.

Nos ambientes digitais, como vimos, todo comportamento individual se transforma em dados pessoais. No "mundo físico", da mesma forma, sistemas digitais são capazes de converter em dados – e, consequentemente, em informações – o comportamento individual para finalidades comerciais, como também de controle e vigilância. As vulnerabilidades dos usuários, com isso, tornam-se mais bem conhecidas dos agentes de tratamento do que deles próprios, o que catalisa os riscos de mitigação de autonomia pela implementação de técnicas manipulativas (como os padrões obscuros).

A publicidade comportamental (*behavioral advertising*), nesse particular, se vale, em grande medida, dos padrões comportamentais e demais características individuais identificadas no ciberespaço para compreender o momento em que a exposição do usuário a um anúncio se converterá na aquisição de algum produto ou serviço, com surpreendente grau de assertividade e certeza[176] (*targeted advertising*)[177]. Tal ordem de coisas conduz a um agravamento da vulnerabilidade individual na economia digital. Com enfoque nas relações de consumo, Helberger *et al*. (2021, p. 176) delimitam o cenário subjacente à *hipervulnerabilidade*[178] na economia digital:

---

[175] "[...] as práticas baseadas em dados digitais devem ser consideradas substancialmente diferentes de todas as formas anteriores de manipulação — entre outras coisas, por causa de sua mecânica oculta, bem como de sua capacidade de personalização, o que permite maior manipulação." (Zarsky, 2019, p. 171, tradução nossa)

[176] "Ao contrário dos anúncios tradicionais, que eram estáticos e disseminados em massa, as plataformas mediadas digitalmente, como sites e aplicativos de mídia social, constituem arquiteturas de escolha dinâmicas, interativas, intrusivas e personalizadas." (Susser; Roessler; Nissenbaum, 2019a, p. 31, tradução nossa)

[177] "[...] a navegação de cada usuário nos diversos Web sites revela um rastro que permite às plataformas ter uma noção da personalidade do consumidor e, com base nesta tipologia, programar e oferecer produtos, serviços e sites, tudo isso através da microssegmentação." (Solís, 2022, p. 1054)

[178] No mesmo sentido, aliás, a OCDE destaca: "Dada a capacidade das empresas *online* de executar repetidamente experimentos e alavancar dados coletados para aprimorar os designs de interface do usuário, a maior

> Nos mercados digitais, a vulnerabilidade do consumidor não é simplesmente um ponto de vista para avaliar a falta de capacidade de alguns consumidores de ativar sua consciência de persuasão. Nos mercados digitais, a maioria, se não todos os consumidores, são potencialmente vulneráveis. Em vez de destacar certos grupos de consumidores, a vulnerabilidade digital descreve um estado universal de indefensabilidade e suscetibilidade à (exploração de) desequilíbrios de poder que são o resultado da crescente automação do comércio, relações consumidor-vendedor dataficadas e a própria arquitetura dos mercados digitais. (Tradução nossa)

Noutra perspectiva, importa observarmos que, diferentemente do que ocorre no mundo *real*, a arquitetura utilizada na construção das plataformas digitais é essencialmente *plástica*, podendo ser modificada a partir dos padrões de comportamento, demonstrações de interesse, agregação de dados (vindos, inclusive, de outras fontes), tudo para interferir, com o máximo de eficiência possível, nos processos decisórios individuais. Assim, a interface de uma mesma plataforma digital pode assumir diferentes formatos e configurações, a depender do perfil comportamental do usuário.

No importante registro de Susser, Roessler e Nissenbaum, "se manipulação é influência oculta, então as tecnologias digitais são os veículos ideais para manipulação, porque elas já estão, em um sentido real, ocultas" (2019b, p. 7, tradução nossa). Efetivamente, à medida que o uso de ditas tecnologias adere ao tecido social, tornando-se pilares estruturais dos novos modos de ser e estar em sociedade, elas deixam de ser vistas ou percebidas como tais, sendo o seu uso tão naturalizado que os indivíduos nem mais se dão conta de que estão inseridos no ambiente virtual, concentrando-se, em verdade, na funcionalidade, bem ou serviço que precisam ser obtidos com o seu uso. Não por outra razão, Botes (2022, p. 319) observa que a "facilidade com que as tecnologias se integram à sociedade contribui para a tempestade perfeita em que a manipulação pode corroer as pessoas da sua autonomia e controle sobre o seu processo de tomada de decisão" (tradução nossa).

O quadro geral dos riscos à autonomia no contexto das plataformas digitais, portanto, está posto. Sendo a informação o veículo primordial de dinamização das relações sociais, econômicas e de poder[179], figuram as plataformas como nós interconectados em uma complexa e crescente rede informacional que alimenta modelos de negócios estruturados sobre o paradigma do capitalismo de vigilância. Nesse sentido, a oportuna crítica de Faustino e Lippold

---

suscetibilidade dos consumidores ao engano *online* [...], bem como a escala de consumidores alcançáveis *online*, os padrões obscuros provavelmente serão um motivo de maior preocupação do que práticas análogas em lojas físicas." (2023, p. 22, tradução nossa)

[179] "[...] se a forma mais fundamental de poder em uma sociedade tecnológica e informacional é a capacidade de influenciar e manipular as pessoas, é fácil concluir que os principais riscos da nova economia vão muito além da violação à privacidade dos usuários, alcançando a própria liberdade e a identidade pessoal e, consequentemente, a cidadania e a democracia." (Frazão, 2019b, p. 346)

(2023, p. 78) coloca em evidência a sistemática empregada pelas plataformas digitais no contexto da conversão das experiências humanas nos ambientes digitais em dados pessoais e a consequente extrativização inerente ao *colonialismo de dados*:

> Estamos diante de um verdadeiro saque milionário de informações transformadas em ativos econômicos, perpetrado por corporações imperialistas que extraem, armazenam e processam dados, *expertise* e padrões sociais, quantificando parte fundamental de nossa vida para melhor mercantilizá-la. Trata-se [...] de uma *acumulação primitiva de dados*. Ao mesmo tempo, observa-se, no mundo todo, uma tendência à colonização, ou melhor, à subsunção da vida cotidiana e de seus processos cognitivos ao universo digital. É um passo largo, aparentemente sem volta, em direção a uma ciborguização objetificada e mercantilizada de nossa experiência e de nosso senso de realidade.

Nesse intrincado e sofisticado contexto informacional, "cada vez mais atenção está sendo dada às chamadas 'dark patterns' – estratégias de design que exploram as vulnerabilidades decisórias dos usuários para induzi-los a agir contra seus interesses (ou, ao menos, agir de acordo com os interesses do site ou *app*)" (Susser; Roessler; Nissenbaum, 2019b, p. 7, tradução nossa). É precisamente sobre tais estratégias que falaremos no tópico a seguir.

2.2 Padrões obscuros: o poder brando das plataformas digitais

Não há nomenclatura uniforme a respeito dos padrões obscuros. Além da denominação utilizada no presente trabalho (também empregada, por exemplo, por Calonga *et al*., 2022, e Ramadas, 2023), há outros estudos publicados no Brasil que se referem a interfaces maliciosas (Lemos; Marques, 2019), *dark patterns* (Marques; Mendes; Bergstein, 2023) e padrões de design deceptivos (Torres, 2024). O nome inicialmente atribuído ao conceito – *dark patterns* – foi originalmente cunhado por Harry Brignull, que os definiu como "abordagens de *design* eticamente duvidosas, quando características de interface e aspectos de uma dada tecnologia modificam a arquitetura de escolhas dos usuários para ganhar sua atenção, dados e dinheiro" (Albuquerque; Valença; Falcão, 2024, p. 1, tradução nossa).

De todo modo, por mais que sejam heterogêneas as denominações, todas designam, com relativa uniformidade conceitual (embora com enfoques diferentes[180]), diversas técnicas de *design* – de uso disseminado[181] – que se caracterizam pelo intuito malicioso e pelo objetivo de manipular usuários de interfaces digitais – para que tomem decisões que favoreçam o autor da

[180] Como pontua Jarovsky (2023, p. 4), "[a] interface humano-computador, a ciência da computação e a literatura jurídica oferecem várias descrições dos dark patterns, refletindo diferentes nuances que podem ser destacadas do ponto de vista desses campos" (tradução nossa).

[181] "Pesquisas em todo o mundo indicam que padrões escusos estão presentes em mais de 10% dos sites de compras globais e em mais de 95% dos 200 aplicativos mais populares." (Marques; Mendes; Bergstein; 2023, p. 2)

estratégia – para reter a sua atenção, para aumentar ganhos financeiros, ou para que deixem de colocar em prática as suas verdadeiras preferências com relação à sua privacidade (como alterar uma determinada configuração na plataforma ou exercer um direito, por exemplo), seja pela *dificuldade* em fazê-lo, seja por terem a *falsa impressão* de que estariam de fato exercendo algum controle.

Nesse sentido, a definição da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) evidencia que o termo se refere a um *conjunto* de

> práticas em interfaces online de usuários que, em geral explorando vieses cognitivos e comportamentais comuns, orientam, enganam, coagem ou manipulam os consumidores a fazerem escolhas, por exemplo, relativas a compras, seus dados pessoais ou tempo gasto em sites, que podem não ser em seus melhores interesses. (OCDE, 2023, p. 22, tradução nossa)

Como se colhe dos conceitos acima, padrões obscuros produzem repercussões diretas sobre a esfera da autonomia individual, "na medida em que levam consumidores a tomar decisões que de outro modo não tomariam, negam a escolha aos consumidores, obscurecem opções disponíveis ou oneram o exercício da escolha" (OCDE, 2022, p. 23, tradução nossa). Entretanto, os danos à autonomia individual (e, evidentemente, a outros direitos fundamentais a ela diretamente associados, como a dignidade e a isonomia) não são ainda totalmente dimensionados.

Cabe observar, todavia, que importantes pesquisas já foram conduzidas a respeito da efetividade dos padrões obscuros. Luguri e Strahilevitz (2021, p. 47), a propósito, obtiveram evidências empíricas de que o uso *dark patterns* suaves mais do que *dobrou* o percentual de usuários que se inscreveram em um (fictício) serviço duvidoso de proteção contra roubo de identidade, ao passo que o emprego das *dark patterns* mais agressivas praticamente *quadruplicou* o percentual de indivíduos que se inscreveram naquele mesmo serviço.

Embora os autores tenham correlacionado a efetividade dos padrões obscuros suaves e agressivos com os distintos graus de escolaridade dos participantes da pesquisa (2021, p. 47), trabalhos mais recentes (Zac *et al*., 2023) concluíram que "que todos os consumidores online são potencialmente vulneráveis quando confrontados com padrões obscuros, com possível vulnerabilidade aumentada para usuários mais velhos" (2023, p. 28, tradução nossa), sendo fracas as evidências de que a suscetibilidade dos usuários seja atingida de modo proporcional a métricas geralmente utilizadas em pesquisas sobre a efetividade das *dark patterns* (como renda ou nível educacional).

Nada obstante, a pesquisa de Luguri e Strahilevitz é reveladora do grave potencial manipulativo dos padrões obscuros que, muito além de meras inconveniências[182] no uso de plataformas digitais – pense-se, por exemplo, nos *banners* de consentimento com *cookies* –, envolvem técnicas sofisticadas de interferência no comportamento e de subversão do processo decisório dos usuários, fazendo-os manifestar opções que não traduzem as suas verdadeiras preferências. No experimento dos autores, resulta claro o porquê de as *dark patterns* estarem se tornando cada vez mais comuns: "porque as empresas sabem que elas são efetivas em induzir os consumidores a agir contra suas próprias preferências" (2021, p. 67, tradução nossa).

Efetivamente, em mercados competitivos nos quais não haja uma clara vedação ao seu uso, agentes econômicos veem-se incentivados a se utilizar dos padrões obscuros para obter vantagens concorrenciais (OCDE, 2022, p. 8). Como destacam Akerloff e Shiller (2016, p. xii), ao se utilizarem da *pescaria de tolos* como metáfora para a manipulação empregada por agentes econômicos, "no equilíbrio resultante do mercado, se houver uma oportunidade para pescar, até mesmo as firmas conduzidas por pessoas com integridade moral genuína geralmente terão que fazer isso para competirem e sobreviverem".

Os resultados da pesquisa de Luguri e Strahilevitz, além do mais, colocam em xeque a função do sistema de preços no contexto do livre mercado, na medida em que a demanda é artificialmente construída pelos próprios agentes econômicos, vendendo mais aqueles que sejam mais aptos a manipular as vontades e escolhas[183] dos consumidores no ambiente virtual, e não os que ofereçam melhores preços. Frazão (2023), nesse particular, nota que "o ambiente digital pode diluir ou até mesmo neutralizar a importância do mecanismo de preços".

Com efeito, sendo cada vez mais comum e disseminado o uso de interfaces digitais para a realização de atividades cotidianas, o campo de oportunidades para a incidência de padrões obscuros é crescente[184]. Dado o potencial de extração massiva de dados pessoais, plataformas digitais – por seus algoritmos – são capazes de aprender, a todo o tempo, como diferentes

---

[182] "Na melhor das hipóteses, os padrões obscuros incomodam e frustram os usuários. Na pior das hipóteses, eles podem enganar e iludir os usuários, por exemplo, causando perdas financeiras, enganando os usuários para que forneçam grandes quantidades de dados pessoais, ou induzindo comportamento compulsivo e viciante em adultos e crianças." (Mathur *et al*., 2019, p. 2, tradução nossa)

[183] "A manipulação no mercado é um problema antigo, mas eventos recentes tornaram o problema muito pior, e os dados apresentados aqui dão a dica mais forte até agora de quão grande é a incompatibilidade entre o que os consumidores querem e o que eles supostamente consentem." (Luguri; Strahilevitz, 2021, p. 104, tradução nossa)

[184] A propósito, Mathur *et al*. (2019) conduziram importante investigação empírica a fim de identificar o uso de padrões obscuros em aproximadamente 11.0000 sites de compras, tendo, nesse universo, identificado 1.818 ocorrências de *dark patterns*, concentradas em 1.254 dos sites analisados (sendo mais recorrentes nos sites mais populares).

usuários interagem e se comportam no ambiente digital, de modo que suas arquiteturas de escolhas podem ser constantemente moldadas para que prevaleçam os interesses das empresas a partir da exploração de vieses e vulnerabilidades. Trata-se da característica que Helberger *et al*. (2021, p. 186) denominam de *ajustabilidade dinâmica*.

Assim, plataformas de *fitness*, redes sociais, comércio eletrônico – além de *chatbots* e assistentes virtuais, que geram conhecimento sobre os usuários e, consequentemente, poder persuasivo (Helberger *et al*., 2021, p. 177; Calo, 2014, p. 999) –, dentre tantas outras, expõem indivíduos a técnicas sofisticadas de manipulação baseadas em um conhecimento sem precedentes sobre o seu perfil comportamental, aprofundando ou mesmo criando novas vulnerabilidades.

Aliás, como acertadamente nota Jarovsky (2023, p. 9), embora os padrões obscuros sejam distintos – tanto pelo viés cognitivo explorado, quanto pela técnica empregada –, todos eles exacerbam o conhecimento das empresas que operam as plataformas sobre seus usuários e, consequentemente, e a assimetria de *poderes* entre eles. Nesse sentido, a *Commission Nationale de l'Informatique et des Libertés* (CNIL) pondera que as escolhas plasmadas nas arquiteturas de interfaces digitais desempenham "um papel importante ao definir o campo de possibilidades [...], ações (que podem ser encorajadas ou, ao contrário, dificultadas) e, ao fim e ao cabo, as preferências dos usuários (já que tendemos a preferir aquilo a que estamos acostumados)" (2019, p. 22, tradução nossa).

Em seu âmbito de aplicação prática, padrões obscuros podem ser empregados para o atingimento de um amplo leque de finalidades, como para que consumidores adquiram produtos ou serviços que não desejam (ou para que os adquiram em quantidade maior do que a pretendida – *sneak into basket*, por exemplo); para que desistam de requerer o cancelamento de serviços (*roach motel*); para que gastem mais dinheiro do que de início planejavam (*hidden costs*; *loss aversion*); para que forneçam mais dados pessoais do que o necessário (como *trick questions*, *privacy zuckering*, *confirmshaming*, etc.), dentre outras[185].

Em um caso célebre envolvendo o uso de *dark patterns* para obtenção de vantagens comerciais, a *Amazon Inc*. passou a empregar padrões obscuros para fazer com que seus clientes se inscrevessem, sem perceber (*sneak into basket*), no serviço denominado "*Amazon Prime*", com cobranças de recorrência mensal que se renovavam automaticamente, tornando o seu

[185] "Da mesma forma que os golpes online estão sempre se desenvolvendo e se tornando cada vez mais convincentes as *Dark Patterns* também estão em constante evolução e não se limitam as que já foram nomeadas [...], pois, elas também interagem entre si, em muitos casos tendo mais de um tipo de *Dark Pattern* sendo aplicado na mesma página." (Custódio; Godoy, 2023, p. 52)

cancelamento excessivamente difícil[186] (técnica que, na taxonomia de Luguri e Strahilevitz, é denominada de *roach motel*). O caso foi levado ao Poder Judiciário norte-americano a partir de uma *civil action* ajuizada pela Federal Trade Commission (FTC)[187], com fundamento em violações à seção 4 do *Restore Online Shoppers' Confidence Act* (ROSCA)[188]. Como relatado na petição inicial da FTC,

> [...] o objetivo principal do processo de cancelamento do Prime não era permitir que os assinantes cancelassem, mas sim frustrá-los. Apropriadamente, a Amazon nomeou esse processo de "Ilíada", que se refere ao épico de Homero sobre a longa e árdua Guerra de Troia. A Amazon projetou o processo de cancelamento da Ilíada ("Ilíada Flow") para ser labiríntico, e a Amazon e sua liderança [...] retardaram ou rejeitaram mudanças na experiência do usuário que teriam tornado a Ilíada mais simples para os consumidores porque essas mudanças afetaram negativamente os resultados financeiros da Amazon. (Tradução nossa)

Ainda sobre o caso, o Conselho de Consumidores da Noruega (*Forbrukerrådet*) publicou o interessante relatório "*You can log out, but you can never leave*" ("Você pode se deslogar, mas você nunca pode sair", em tradução nossa), demonstrando como os padrões obscuros presentes no cancelamento do serviço Amazon Prime impõem aos consumidores um "grande número de obstáculos, incluindo menus de navegação complicados, redação distorcida, escolhas confusas e 'nudges' repetidos" (Forbrukerrådet, 2021, p. 3, tradução nossa).

No estudo, que ilustra o difícil passo-a-passo a ser seguido até o cancelamento do serviço, o órgão norueguês de defesa dos consumidores destaca que as assimetrias de poder e de informações entre o provedor do serviço e o consumidor deveriam se traduzir em uma clara obrigação daquele de viabilizar um processo de cancelamento facilitado, "mesmo que isso não se alinhe aos seus incentivos financeiros" (*Idem*, p. 29, tradução nossa).

Os padrões obscuros não são, aliás, estranhos ao contexto brasileiro. Cabe citar, nesse sentido, decisão proferida pelo Conselho Nacional de Autorregulamentação Publicitária

---

[186] "Durante o processo de checkout online da Amazon, os consumidores se depararam com inúmeras oportunidades de assinar o Amazon Prime por US$ 14,99/mês. Em muitos casos, a opção de comprar itens na Amazon sem assinar o Prime era mais difícil para os consumidores localizarem. Em alguns casos, o botão apresentado aos consumidores para concluir sua transação não declarava claramente que, ao escolher essa opção, eles também estavam concordando em se juntar ao Prime para uma assinatura recorrente." (Disponível em: https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their. Acesso em: 6 dez. 2024. Tradução nossa)

[187] O caso, ainda não concluído, teve julgamento agendado para junho de 2025. Disponível em: https://www.reuters.com/legal/litigation/ftc-lawsuit-over-amazons-prime-program-set-june-2025-trial-2024-06-12/. Acesso em: 6 dez. 2024.

[188] Assim dispõe a seção 4: "Será ilegal para qualquer pessoa cobrar ou tentar cobrar de qualquer consumidor por quaisquer bens ou serviços vendidos em uma transação efetuada na Internet por meio de um recurso de opção negativa (conforme definido na Regra de Vendas por Telemarketing da Comissão Federal de Comércio na parte 310 do título 16, Código de Regulamentos Federais), a menos que a pessoa: [...] (3) disponibilize mecanismos simples para que o consumidor interrompa o lançamento de cobranças recorrentes em seu cartão de crédito, cartão de débito, conta bancária, ou outra conta financeira ." (Tradução nossa)

(Conar) nos autos da representação n. 203/2022 (relatora a Conselheira Camila Felix, julgada em dezembro de 2022). No caso, o Conselho aplicou à Drogaria São Paulo as sanções de alteração e advertência pelo uso de padrões obscuros como "isca" (*bait-and-switch*) para atrair consumidores. Em material publicitário da Drogaria, anunciava-se a oferta de 80% de desconto na compra da segunda unidade de um mesmo item, inserindo-se no anúncio imagens de fraldas e lenços umedecidos (que, contudo, não estavam inclusos na promoção). Como narra a decisão, "a consumidora foi informada que a promoção não existe, sugerindo a caracterização da arquitetura de oferta digital (o chamado *dark pattern*) que serviria de isca com a intenção de promover produtos diferentes" (CONAR, 2023, p. 8).

Outra importante decisão, também no âmbito administrativo, foi a medida cautelar deferida pela Autoridade Nacional de Proteção de Dados contra a Meta Platforms Inc. no contexto da alteração não notificada dos termos de sua política de privacidade e do uso de dados pessoais (incluindo os de crianças e adolescentes) disponíveis nos produtos da Meta (*Facebook*, *Instagram*, *WhatsApp*) para o treinamento de algoritmos de inteligência artificial generativa. Dentre os aspectos mencionados no Voto n. 11/2024/DIR-MW/CD, proferido em julho de 2024, estava o de que o recurso de opt-out oferecido aos usuários dos serviços da Meta "não é disposta de maneira evidente, e a complexidade para exercício dessa opção assemelha-se a um padrão obscuro de mascaramento de informações". A prática, conhecida como *dead end*, enquadra-se, na classificação proposta pelo EDPB, entre os padrões obscuros obstrutivos (*obstructing*)[189].

No âmbito do Superior Tribunal de Justiça, importa fazer menção à decisão proferida nos EDcl no REsp n. 1.737.428/RS (rel. p/ o ac. Min. Paulo de Tarso Sanseverino, julgado em 6.10.2020, DJe de 19.11.2020), em que a Terceira Turma da Corte Superior acolheu tese de violação do dever de informação "pela empresa demandada, na medida em que referida taxa de conveniência vem sendo ocultada na fase pré-contratual, como se estivesse embutida no preço, para depois ser cobrada como um valor adicional, gerando aumento indevido do preço total".

Embora o acórdão não tenha feito referência expressa aos padrões obscuros, o Ministro Relator – ao analisar a temática sob a ótica do direito consumerista – bem consignou que a oferta de um produto ou serviço por preço artificialmente menor para que, depois, seja cobrada a diferença sob pretexto de um "serviço adicional" é prática comercial que, "além de ser abusiva sob a ótica do direito do consumidor [...], é também desleal sob a ótica da livre concorrência".

[189] Segundo o EDPB (2022, p. 3), *obstructing* "significa dificultar ou bloquear os usuários em seu processo de se informar ou gerenciar seus dados, tornando a ação difícil ou impossível de ser alcançada" (tradução nossa).

O padrão obscuro a que faz referência o acórdão, à luz da taxonomia de Luguri e Strahilevitz, denomina-se *hidden costs* (custos ocultos).

Na perspectiva jurídica – sobretudo em se considerando que "a interface é o primeiro objeto de mediação entre a lei, os direitos e os indivíduos" (CNIL, 2019, p. 10, tradução nossa) – a relevância do *design* para a estruturação de plataformas digitais não deve ser menosprezada. Waldman (2019, p. 5), aliás, destaca que

> no mínimo, o poder do *design* significa que as nossas escolhas nem sempre refletem nossas reais preferências pessoais. Na pior das hipóteses, as plataformas online nos manipulam a manter os dados fluindo, alimentando um modelo de negócios faminto por informações. Essa manipulação é em geral o resultado dos assim chamados "dark patterns" no *design* das plataformas. (Tradução nossa)

A própria experiência cotidiana evidencia que o exercício de direitos no ambiente digital depende, em grande medida, do *design* das plataformas digitais. De fato, o desenho dos ambientes virtuais pode tanto favorecer quanto dificultar não apenas a expressão da vontade autônoma dos indivíduos (Verbicaro; Homci, 2024, p. 1), como também o acesso aos ambientes adequados à formalização de solicitações, à formulação de denúncias, à apresentação de reclamações[190], dentre outros. Aliás, como referimos no início desse capítulo, padrões obscuros podem dificultar até mesmo o acesso à *informação sobre o exercício dos direitos*, pressuposto essencial à agência dos usuários no ambiente virtual.

As consequências da utilização de padrões obscuros não se restringem à usabilidade das interfaces digitais, mas se projetam de modo relevante sobre aspectos existenciais fundamentais dos usuários das plataformas (como, por exemplo, a própria perda de tempo[191] ou o exercício de direitos), *ultrapassando os limites* do mundo virtual. Considerado esse contexto, os padrões obscuros se revelam como elementos importantes do modo de exercício do poder brando (*soft power*) pelas empresas que operam plataformas digitais. Afinal, a implementação de estratégias de indução sub-reptícia e maliciosa das decisões individuais é expressão de como "o poder brando é frequentemente manipulador – ele nos leva a fazer algo em benefício de outros sob o pretexto de que é em nosso próprio benefício", como leciona Véliz (2021, p. 91).

---

[190] Como consignado no Voto n. 11//2024/DIR-MW/CD, proferido no processo administrativo instaurado no âmbito da ANPD a respeito das alterações feitas pela Meta Platforms Inc., "[...] o design e a disponibilização de ferramentas simples e intuitivas para atendimento e obtenção de manifestação dos titulares são fatores essenciais para garantir que estes tenham efetivo controle sobre o uso e a destinação de seus dados pessoais".

[191] "A passagem do tempo deveria ser a favor das pessoas, mas hoje as situações em que o tempo do outro é absolutamente desprezado não são, infelizmente, raras. [...]. E vários exemplos de padrões comerciais obscuros estão relacionados à perda de tempo dos consumidores ou à necessidade dos consumidores de uma transação rápida." (Marques; Mendes; Bergstein, 2023, p. 5)

A manifestação do poder brando verificada no uso de padrões obscuros na arquitetura de escolhas das plataformas digitais está na interferência direta sobre a racionalidade[192] dos indivíduos, subvertendo seu processo decisório e subordinando-lhes à vontade dos agentes econômicos que as controlam. Como se verifica da situação-exemplo trazida por Marques, Mendes e Bergstein (2023, p. 4):

> Mesmo que a assinatura do serviço pudesse ser feita preenchendo apenas um pequeno formulário, o cancelamento dependia de conversar com um operador no chat. Não havia a opção de cancelar o serviço livremente. Nesse dia, o cancelamento levou duas tentativas e mais de uma hora e quarenta minutos. O exemplo mostra como a disparidade entre a velocidade de inscrição e os acordos demorados necessários para o cancelamento é um padrão obscuro implementado para manter os consumidores vinculados ao serviço pelo máximo de tempo possível.

Convém notar – assim como ponderamos com relação à manipulação – que padrões obscuros, enquanto técnicas maliciosas de exploração de vieses cognitivos, vulnerabilidades e heurísticas, não são algo exatamente inédito. Entretanto, o seu potencial manipulativo foi, de fato, amplificado pela intensa extração e acumulação de informações a respeito de aspectos comportamentais dos usuários nas mãos das empresas. A agregação do uso de tecnologias de informação e comunicação catalisou intensamente o fluxo de geração de conhecimento a respeito de perfis individuais, vulnerabilizando ainda mais os usuários (e, evidentemente, impondo ao Direito o dever de oferecer respostas apropriadas ao fenômeno[193]).

Nesse aspecto, a OCDE (2022, p. 12) aponta duas principais razões que distinguem as *dark patterns* atuais daquelas empregadas antes do advento do Big Data:

> Primeiro, os negócios online de hoje estão muito mais cientes das oportunidades oferecidas por insights comportamentais para refinar suas estratégias de marketing [...], inclusive explorando vieses e heurísticas importantes que afetam o comportamento do consumidor online. [...].
>
> [...]
>
> Segundo, em contraste com as transações presenciais, as transações entre consumidores e negócios online são mediadas por meio de um dispositivo interativo e conectado, como um computador ou telefone celular [...]. Isso permite que os negócios online coletem dados sobre como os consumidores

[192] "A digitalização dos mercados de consumo e das transações eletrônicas permitiu formas inteiramente novas de estratégias de persuasão personalizadas que descobrem e se baseiam em vieses, fraquezas, preferências e necessidades individuais e que podem ser direcionadas, muito propositalmente, para tornar os consumidores — mesmo aqueles que não pertencem às categorias típicas de consumidores vulneráveis — vulneráveis, no sentido de afetar sua capacidade de lidar racionalmente com uma prática de marketing específica." (Helberger *et al.*, 2021, p. 180, tradução nossa)

[193] "Há muito a aprender olhando para trás, mas a escala das *dark patterns*, sua rápida proliferação, as possibilidades de uso de algoritmos para detectá-las e a amplitude das diferentes abordagens que já surgiram significam que este é um reino onde é necessária uma criatividade jurídica significativa." (Luguri; Strahilevitz, 2021, p. 102, tradução nossa)

> interagem com o negócio por meio do dispositivo e otimizem suas práticas comerciais de acordo. (Tradução nossa)

Considerado o contexto atual, convém fazer menção a interessante investigação conduzida por Calonga *et al*. (2022) por meio "entrevistas semiestruturadas e grupos focais, a fim de analisar se os usuários jovens, mesmo estando conscientes da existência dos *dark patterns*, aceitam ser permissivos em relação às manipulações propostas pelos *sites*" (2022, p. 3). Dentre as descobertas da pesquisa, os autores constataram que, na visão dos entrevistados, "não há como combater ou mesmo evitar padrões sombrios, devido à dependência de certos serviços e empresas" (2022, p. 16); de todo modo, identificou-se, também, a visão de que "as empresas consideram a indução de um comportamento por meio dos padrões obscuros como a única possibilidade de sobrevivência e, por isso, normalizam a ação" (2022, p. 17).

Os resultados da pesquisa, de fato, confirmam a tendência de normalização do emprego de padrões obscuros em interfaces digitais, à medida em que o uso de plataformas se torna cada vez mais disseminado e corrente. A visão *normalizadora* do fenômeno dos padrões obscuros está atrelada a uma perspectiva que se escora, de um lado, na dependência das novas tecnologias, e, de outro, em uma compreensão baseada na natureza das práticas competitivas entre agentes econômicos, de modo que aqueles que não os implementem estarão em desvantagem na disputa por mercados[194], como tivemos ocasião de referir. De fato, como bem anota Brenncke (2024, p. 3), "os 'padrões obscuros' em arquiteturas de escolha online são prevalentes e cada vez mais utilizados por negócios de todos os tamanhos" (tradução nossa).

A mencionada tendência à normalização se situa no contexto do que alguns autores, como Daniel Solove, Ezra Waldman e Ignacio Cofone, denominam *paradoxo da privacidade* (de que trataremos no subcapítulo a seguir), que designa um comportamento aparentemente contraditório de indivíduos que, ao tempo em que se dizem preocupados com a proteção de sua privacidade, sujeitam-se à sistemática de extração massiva de dados pessoais em favor do acesso a bens e serviços mediados por plataformas digitais.

Merece registro, por outro lado, o fato de que não apenas agentes econômicos do setor privado se utilizam de padrões obscuros. Nesse particular, Lemos e Marques (2019) analisaram interfaces maliciosas encontradas em dez aplicativos utilizados pelo Município de Salvador/BA para a coleta de dados pessoais. Assim como na pesquisa de Calonga *et al*., os autores identificaram uma tendência à normalização do uso de padrões obscuros, como fenômenos

---

[194] Cabe ponderar, contudo, sob a ótica concorrencial, que "*dark patterns* podem, em tese, ser enquadradas como infrações da ordem econômica [...], na medida em que prejudicam a livre concorrência, criando dificuldades ao funcionamento ou desenvolvimento dos demais fornecedores de bens ou serviços, utilizando-se de meios enganosos aos consumidores." (Marques; Mendes; Bergstein, 2023, p. 6)

naturais de um contexto maior, de digitalização e plataformização da sociedade. Na pesquisa, os autores estabeleceram, inicialmente, uma "escala de gravidade" em termos de ameaças à privacidade representadas pelas interfaces maliciosas (sendo de nível 1 as ameaças leves; nível 2 as intermediárias; e nível 3 as graves).

Os pesquisadores constataram que 70% dos aplicativos apresentavam padrões obscuros de nível 1 na escala de potenciais ofensas à privacidade, ao passo que 17% e 13% corresponderam aos níveis 2 e 3, respectivamente. Diante disso, identificaram a existência de uma *crescente naturalização e pervasividade* dos padrões obscuros, com o potencial de "gerar impactos na forma como entendemos a negociação de dados pessoais com as plataformas, pois à medida que práticas abusivas de interface se tornam lugar comum, os consumidores tendem a abrir mão da sua privacidade mais facilmente" (Lemos; Marques, 2019, p. 7)[195].

Como evidenciado pela pesquisa de Lemos e Marques, embora sejam largamente utilizados no âmbito das relações de consumo, os padrões obscuros têm sido objeto de vasta aplicação no campo da coleta massiva de dados pessoais, considerado o papel de tais informações enquanto insumos fundamentais de inúmeros modelos de negócio no capitalismo de vigilância[196]. É sobre esse aspecto que discorreremos, com maior vagar, no tópico a seguir.

2.2.1 Compreendendo os padrões obscuros na perspectiva da proteção de dados pessoais

Como vimos, dados pessoais são necessários para o treinamento de algoritmos, para a formação de perfis comportamentais cada vez mais precisos, para a obtenção de conhecimento refinado a respeito de vulnerabilidades e para a predição de comportamentos futuros, bem como para viabilizar novas in(ter)ferências sobre as agências e processos decisórios individuais.

---

[195] A ideia de normalização da abusividade identificada nas plataformas digitais – na perspectiva da proteção de dados pessoais –, defendida por Lemos e Marques (2019), pode ser articulada com a interessante noção de *privacy nicks*, apresentada em recente trabalho de Hartzog, Selinger e Gunawan (2024). Para o autor, a crise de efetividade das normas de proteção à privacidade se deve ao fato de que essas mesmas normas se baseiam nas expectativas dos indivíduos para definirem os limites da vigilância. Ocorre, todavia, que, à medida em que as pessoas vão se habituando a pequenas invasões à privacidade (os *privacy nicks*), cria-se uma "uma sociedade que é gradualmente condicionada a ser observada" (Hartzog; Selinger; Guanawan, 2024, p. 721), o que se reflete na produção da própria norma jurídica.

[196] "Estratégias comerciais orientadas por dados são embutidas em uma rede sofisticada de alto-falantes inteligentes, eletrodomésticos inteligentes, vigilância em lojas e aplicativos e rastreadores que alimentam o fluxo de dados – dados que irão finalmente criar representações virtuais de consumidores e, talvez mais importante, o 'potencial de comercialização' do consumidor. O propósito geral dessas práticas é tornar os consumidores receptivos a estratégias de marketing digital que usam tecnologias digitais para otimizar as práticas comerciais com o objetivo de vender produtos e serviços." (Helberger *et al*., 2021, p. 176, tradução nossa)

Dados pessoais fornecem importantes vantagens competitivas aos agentes econômicos e, por esse motivo, consubstanciam a matéria-prima a ser constantemente extraída[197], dada a mutabilidade do comportamento humano, permeável a contingências sociais, políticas, ambientais e econômicas. Pode-se com isso afirmar que, por mais variados que sejam os ramos de atividade econômica sobre os quais se estruturam os negócios na sociedade da informação, subjacente a todos eles está o *negócio* do tratamento de dados pessoais (Frazão, 2018, p. 643).

Efetivamente, na economia da atenção[198], a que já nos referimos, têm vantagem as plataformas digitais que consigam fazer com que seus usuários se mantenham ativos por mais tempo, maximizando a coleta de dados pessoais e aperfeiçoando a formação de perfis comportamentais[199]. Assim, parte relevante dos padrões obscuros serve a fazer com que usuários forneçam (e sigam fornecendo, sem se dar conta das consequências disso) mais dados pessoais do que o necessário; deixem de exercer direitos relacionados à proteção de seus dados (como a oposição ao tratamento, mencionada no caso da medida cautelar envolvendo a Meta); tenham a *impressão* de que de fato exercem controle significativo sobre seus dados pessoais; não compreendam adequadamente a natureza das atividades de tratamento que serão realizadas, em geral expostas nas políticas de privacidade. De fato, padrões obscuros podem obfuscar os perigos da divulgação de informações e, ao mesmo tempo, incentivar os usuários a compartilharem cada vez mais (Waldman, 2019, p. 6).

Vale citar, como exemplo, as redes sociais, projetadas para serem viciantes. Como já registramos, há uma miríade de técnicas implementadas por redes sociais para que seus usuários nelas permaneçam por cada vez mais tempo[200]. Essas estratégias, contidas na própria arquitetura das plataformas, são cuidadosamente pensadas e desenhadas à luz das características do

---

[197] Em dissertação de Mestrado, Jandrey (2023, p. 14) acertadamente adota a compreensão de padrões obscuros como "ferramentas derivadas de estudos da economia comportamental, que foram adaptadas pelo capitalismo de vigilância para serem utilizadas pelas empresas em suas práticas comerciais".

[198] "A economia da atenção está relacionada a um dos maiores problemas da atualidade: a alocação de tempo e atenção das pessoas diante de uma miríade de atividades, negócios e relacionamentos possíveis. Nesse cenário, potencializado pelas facilidades trazidas pelo meio digital, os maiores custos de transação deixam de ser os tradicionais, como os de transporte, e passam a ser os de avaliar e escolher o que fazer ou adquirir e com quem fazer ou adquirir." (Frazão, 2018, p. 642)

[199] "Como consequência dessa economia da atenção, a noção de investimento social retém os usuários por meio de recompensas constantes e atua como a pedra angular das plataformas de mídia social. Métricas como total de reações ou seguidores têm o potencial de estabelecer uma espécie de 'vínculo' entre os usuários e a plataforma na qual eles têm um perfil. Portanto, tais funcionalidades incutem nos usuários a percepção de que é necessário continuar usando a plataforma para não perder seu 'progresso'." (Albuquerque; Valença; Falcão, 2024, p. 4, tradução nossa)

[200] "Para que a economia digital prospere, é imprescindível às empresas de tecnologia a captura e mobilização da atenção dos usuários para que eles passem o máximo de tempo possível conectados em suas plataformas. Porque quanto mais tempo passam enganchados e engajados em seus serviços, maior será a produção, coleta e armazenamento de dados, e maior será, assim, a acuidade preditiva dos mecanismos algorítmicos, o que, por sua vez, aumentará o valor atribuído à mercantilização dos dados." (Bentes, 2021, p. 24)

comportamento humano. É precisamente esse o ponto de Véliz (2021, p. 91), quando, ao discorrer sobre o poder brando das plataformas digitais, anota que

> *A manipulação exercida pelo poder brando nos torna cúmplices de nossa própria vitimização*. É o *seu* dedo rolando seu feed de notícias, fazendo você perder tempo precioso, e lhe deixando com dor de cabeça. Mas, é claro, você não estaria preso a esse pergaminho infinito se plataformas como o Facebook não estivessem tentando convencê-lo de que, se você não continuar a deslizar seu dedo, você vai perder alguma coisa. (Grifo no original)

Saber quantas pessoas "curtiram" uma publicação desperta a sensação de validação, inclusão e relevância; visualizar conteúdos apresentados a partir de uma análise prévia de perfis de interesse deflagra a liberação de dopamina, aumentando a sensação de bem-estar (e a vontade de consumir cada vez mais conteúdo); jogos e *trends* estimulam e satisfazem, por meio de uma interface lúdica, a necessidade de expressão, de afirmação e de manifestação da própria identidade no ambiente digital.

Essas, dentre tantas outras funcionalidades das redes sociais, criam e mantêm um fluxo incessante de fornecimento de dados pessoais[201]. Lemos e Marques (2019, p. 2), a propósito, situam o fenômeno das interfaces maliciosas no contexto que designam pela sigla "PDPA": *plataformização da sociedade*, *dataficação* e *performatividade algorítmica*. Trata-se, segundo os autores, de "fenômenos que caracterizam o atual estado da cultura digital, apontando para a expansão das plataformas digitais na mediação do cotidiano" (*Idem*, *ibidem*).

Aliás, a extração massiva de dados pessoais viabilizada por padrões obscuros em plataformas digitais retroalimenta as próprias interfaces maliciosas, na medida em que o conhecimento aprofundado a respeito de vieses e vulnerabilidades permite a modulação dos ambientes digitais, de forma a que os arquitetos de escolha consigam direcionar eficientemente o comportamento dos usuários – de modo sutil, discreto, mas poderoso (Yeung, 2017, p. 119) – para que venham ao encontro de seus próprios interesses. Por mais variadas que sejam as formas de manipulação, qualquer delas que "auxilie, por ação ou omissão, o compartilhamento adicional de dados pessoais ou a disrupção do processo decisório sobre a privacidade, pode ser considerada negativa – um dano à privacidade" (Jarovsky, 2023, p. 13, tradução nossa)

Como acertadamente pontua Zarsky (2019, p. 160), as plataformas "usam várias técnicas, que são parcialmente derivadas das informações pessoais que coletam, para seduzir indivíduos a fornecer mais informações pessoais [...] ou a se negligenciar a mudar padrões relativos à privacidade que são favoráveis às empresas" (tradução nossa). O cenário que se

---

[201] "Quanto mais um aplicativo consegue atrair o nosso tempo e a nossa atenção, mais dados pessoais poderá coletar e mais recursos terá para nos influenciar ou manipular ou para possibilitar que seus parceiros comerciais ou políticos o façam." (Frazão, 2024, p. 15)

apresenta, portanto, relativamente à dinâmica dos dados pessoais no contexto de plataformas digitais, é marcado por um poder altamente assimétrico, que dá aos arquitetos de escolhas a capacidade de utilizar as informações dos indivíduos contra eles próprios, expostos, todos os dias, a diversas técnicas de manipulação[202] (Cofone, 2024, p. 67).

Para além dos prejuízos à livre formação da personalidade e à autonomia[203], sobre os quais discorremos nesse capítulo, as consequências do emprego de padrões obscuros se estendem, na perspectiva dos indivíduos, às perdas financeiras, aos agravos à saúde mental (incluindo-se o vício no uso das plataformas, ansiedade e depressão) e, sobretudo, a violações à privacidade, que expõem os indivíduos a possíveis discriminações arbitrárias e ilegítimas, perseguições, risco de violência moral e física, humilhação pública, roubo de identidade, espionagem, *stalking*, coação, comprometimento do desenvolvimento cognitivo de crianças e adolescentes, baixa autoestima, dentre outros (OCDE, 2023, p. 22).

Sob essa perspectiva, em reação ao fenômeno – ainda relativamente recente – do *design* malicioso das plataformas digitais, vieram a lume as primeiras normas jurídicas direcionadas à proteção da privacidade individual frente aos padrões obscuros. Na Califórnia, por exemplo, o California Consumer Privacy Act (CCPA)[204] foi o primeiro diploma legal a expressamente estabelecer um conceito de *dark pattern*, definindo-o como "uma interface de usuário desenhada ou manipulada com o efeito substancial de subverter ou comprometer a autonomia, tomada de decisão, ou escolha do usuário, nos termos da regulamentação" (Sec. 1798.140, "l", tradução nossa).

---

[202] Zarsky (2019, p. 169), a propósito, identifica quatro principais repercussões da manipulação sobre a proteção de dados pessoais: "(1) a manipulação envolverá a capacidade de adaptar respostas únicas a cada indivíduo com base em dados coletados anteriormente e (2) a capacidade de adaptar e alterar a resposta personalizada em vista do feedback contínuo do usuário e de outros, tornando assim a manipulação um processo contínuo, em oposição a uma ação única; (3) a manipulação ocorrerá frequentemente enquanto o indivíduo estiver alheio aos processos observados (ou, em outras palavras, em um ambiente não transparente); e (4) a manipulação será facilitada pela disponibilidade de ferramentas avançadas de análise de dados (incluindo aquelas que aplicam mineração de dados), que permitem ao projetista do sistema adquirir insights profundos sobre quais formas de persuasão estão se mostrando eficazes ao longo do tempo" (tradução nossa).

[203] "[...] a prática em discussão, além de causar um dano informacional em razão da utilização de mecanismos digitais de *design* para dificultar o acesso do titular de dados à informação clara, precisa e direta, provoca uma indeterminação situacional, que afeta a autodeterminação por atingir o exercício da liberdade do titular." (Verbicaro; Homci, 2024, p. 7)

[204] Ainda com relação ao contexto norte-americano, cite-se o *Deceptive Experiences To Online Users Reduction Act* (DETOUR Act), ainda em tramitação, que visa a proibir o uso de práticas enganosas por grandes provedores de serviço online e promover a transparência e a escolha do consumidor no uso da pesquisa comportamental por esses provedores. A seção 3 do DETOUR Act impõe vedações à implementação de práticas enganosas, estabelecendo o item (a) (1), como prática ilícita, "projetar, modificar ou manipular uma interface de usuário em um serviço online com o propósito ou efeito substancial de obscurecer, subverter ou prejudicar a autonomia do usuário, a tomada de decisão ou a escolha para obter consentimento ou dados do usuário".

No contexto europeu, leis da União Europeia vêm protegendo consumidores e usando a autonomia como uma lente normativa para regular os padrões obscuros. Nesse sentido, impõe-se mencionar o Considerando 67 do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho (*Digital Services Act* – DSA), que correlaciona expressamente os padrões obscuros ao comprometimento da autonomia individual. De acordo com o texto normativo europeu, "padrões obscuros nas interfaces em linha das plataformas em linha são práticas que distorcem ou prejudicam de forma substancial, intencional ou de facto, a capacidade dos destinatários do serviço de fazerem escolhas ou **decisões autónomas** e informadas"[205] (grifo nosso).

Com efeito, iniciativas legislativas mostram-se oportunas diante de um cenário em que, na ausência de vedação explícita, o uso crescente de padrões obscuros **tem comprometido o exercício dos direitos relacionados à proteção de dados pessoais nos ambientes virtuais**. Seja pelo excesso de opções e configurações (*cognitive overload*), pela dificuldade de exercer direitos (*obstructing*), pela ocultação maliciosa de informações ou ferramentas de controle, deixando os indivíduos confusos e perdidos (*left in the dark*) – ou mesmo pelo uso de apelos à emoção (*stirring* ou *confirmshaming*) –, o *design* malicioso forma um ambiente hostil ao exercício de garantias e salvaguardas previstas pelo Direito[206]. Aliás, "as preferências acerca da privacidade respondem a contextos específicos e são maleáveis, na medida em que [...] os contextos podem ser manipulados para se adequarem a inferências preditivas sobre o indivíduo" (Nadler; McGuigan, 2018, p. 162, tradução nossa).

Ao contrário de facilitarem e garantirem adequadamente o exercício dos direitos de seus usuários, o que fazem as interfaces digitais maliciosas, na verdade, é estimular incessantemente o compartilhamento (*oversharing*) de informações pessoais pelos usuários, sem que saibam, ao fim e ao cabo, que estão colocando em risco seus próprios direitos e liberdades (CNIL, 2019, p. 10). Como, então, compreender os resultados de pesquisas recentes que indicam uma paradoxal e crescente preocupação dos indivíduos com a sua privacidade[207]? Não apenas no

---

[205] Nessa mesma toada, o artigo 13 (6) do Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho (*Digital Markets Act* – DMA) estabelece que "O controlador de acesso não pode deteriorar as condições ou a qualidade de nenhum dos serviços essenciais de plataforma prestados a utilizadores profissionais ou utilizadores finais [...], nem dificultar indevidamente o exercício desses direitos ou escolhas, nomeadamente mediante a oferta de escolhas ao utilizador final de forma não neutra, ou utilizando a estrutura, a conceção, a função ou o modo de funcionamento de uma interface de utilizador ou de parte dela **para condicionar a autonomia, a tomada de decisões ou a livre escolha** do utilizador final ou do utilizador profissional." (grifo nosso)

[206] "Nosso comportamento de exposição também é manipulado pelo *design*: o *design* tem funções de sinalização que nos encorajam a fazer certas escolhas, ele nos fornece apenas um certo conjunto definido de opções e nos manipula ao desencadear as muitas limitações cognitivas que tornam a autonomia perfeita impossível." (Waldman, 2021, p. 60, tradução nossa)

[207] De acordo com os resultados obtidos pela pesquisa "Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil", tem-se notado uma maior preocupação dos usuários com a adoção de práticas de proteção de privacidade nos ambientes virtuais. Assim, "entre as atividades

Brasil, como também no contexto estrangeiro (Waldman, 2019, p. 5), há evidências de que indivíduos se importam com o tema da privacidade, muito embora o seu comportamento no ambiente digital não se revele compatível com essa afirmação.

Como esclarece Solove (2021, p. 19), a figura do *design* malicioso produz tais contradições entre as preferências individuais sobre a privacidade e o compartilhamento cada vez maior de informações pessoais (o que caracteriza o "paradoxo da privacidade" – *privacy paradox*), na medida em que "o comportamento das pessoas está sendo manipulado por empresas e disrtorcido pelo *design* tecnológico" (2021, p. 18, tradução nossa). No mesmo sentido, Waldman (2019, p. 2) acrescenta que o paradoxo da privacidade, na realidade, não significa o desinteresse dos usuários de plataformas em proteger sua própria privacidade mas, sim, sua previsível reação ao *design* orientado a se aproveitar de suas limitações cognitivas.

Considerado o delicado cenário que se apresenta pela inserção ubíqua de padrões enganosos como formas de levar indivíduos a tomarem decisões que, de outro modo, não tomariam[208] nas plataformas digitais, a partir da interferência maliciosa sobre seus vieses cognitivos e vulnerabilidades, e suas repercussões sobre a efetividade do regime jurídico da proteção de dados pessoais, cabe-nos indagar a respeito das efetivas potencialidades do paradigma do controle – modelo epistemológico sobre o qual se estrutura a dogmática nacional a respeito da proteção de dados – como pressuposto da proteção de dados pessoais.

Embora, efetivamente, não se vislumbre a necessidade de edição de novas propostas legislativas, tal como vem ocorrendo nos estados norte-americanos – na medida em que se verifica, no contexto brasileiro, a existência de um arcabouço normativo suficiente à contenção de práticas maliciosas ofensivas à autonomia individual nas plataformas digitais –, é necessário refletir sobre o uso que se tem feito desse mesmo arcabouço.

É dizer: a epistemologia incidente sobre o regime jurídico brasileiro de proteção de dados pessoias tem feito frente aos desafios apresentados pela realidade, sempre cambiante, do mundo digital? A efetividade da norma jurídica tem sido suficiente a impor aos negócios digitais um uso ético do *design* dos das plataformas digitais?

---

realizadas para gerenciar o acesso a seus dados pessoais, os usuários de Internet com 16 anos ou mais reportaram em maior proporção a leitura de políticas de privacidade de páginas ou aplicativos (67%) e a verificação de segurança de página ou aplicativo (67%), seguidas pela recusa de permissão de uso de seus dados para publicidade personalizada (66%)" (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 48),

[208] "As empresas sempre projetaram escolhas para influenciar as pessoas, como por meio de posicionamento de produtos ou métodos de pagamento. Mas a extensão e a escala dessa influência na economia da informação, e sua exploração resultante, não têm precedentes. Na economia da informação, aqueles que projetam nossas escolhas também projetam como nos comunicamos uns com os outros e têm poder para usar nossos dados pessoais contra nós. A influência é exercida sobre todos, todos os dias." (Cofone, 2024, p. 67, tradução nossa)

Incumbe-nos, no próximo capítulo, passar a uma análise mais detida a respeito dos pressupostos que dão sustentação à epistemologia calcada no paradigma do controle, que orienta o regime protetivo centralizado pela Lei Geral de Proteção de Dados Pessoais.

3 O PARADIGMA DO CONTROLE E O MODELO PROCEDIMENTAL DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

O Brasil é um país de profundas desigualdades. Dentre os vários parâmetros usualmente examinados em estudos estatísticos sobre o tema, os índices de concentração de renda nos auxiliam a visualizar com maior nitidez as dimensões de tais discrepâncias. Nesse particular, cabe a menção a relatório produzido pelo Observatório Brasileiro das Desigualdades – iniciativa ligada ao Pacto Nacional pelo Combate às Desigualdades[209] –, divulgado em agosto de 2024, que apontou que o rendimento médio mensal *per capita* dos 1% mais ricos da população brasileira é 31,2 vezes maior do que o de 50% dos indivíduos mais pobres (Pacto Nacional pelo Combate às Desigualdades, 2024, p. 4).

A desigualdade, efetivamente, não se mede apenas pela concentração de renda, embora essa seja um importante indicador do cenário geral do País[210]. Afinal, as diferenças com relação à renda projetam seus efeitos sobre outros possíveis recortes de pesquisa, como a escolaridade, o acesso à saúde, e – o que nos parece mais relevante, na perspectiva do objeto de nossa investigação – o acesso à Internet (exclusão digital[211]) e as *habilidades digitais*[212].

Como revela a edição mais recente da Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros ("TIC Domicílios 2023"), por nós já mencionada no presente estudo, 84% dos *domicílios* brasileiros (aproximadamente 64 milhões) têm acesso à Internet[213]. A distribuição de tal quantitativo guarda estreita relação com o recorte

---

[209] Trata-se de programa que congrega organizações sociais, associações de municípios, centrais sindicais e entidades de classe, com apoio de instâncias governamentais dos Poderes Executivo, Legislativo e Judiciário. O Observatório "atua inicialmente no **monitoramento** das diferentes dimensões da desigualdade no Brasil; no incentivo ao **mapeamento** das desigualdades pelo poder público; no **reconhecimento** de políticas públicas bem-sucedidas de combate às desigualdades; e na sugestão de medidas para que municípios, sindicatos e empresas possam atuar no tema". Disponível em: https://combateasdesigualdades.org/#iniciativas. Acesso em: 10 dez. 2024.

[210] Segundo o Relatório, os números apontam uma maior "concentração de rendimento, isto é, a razão do rendimento do 1% mais rico e os 50% mais pobres aumentou 1,3% [em comparação com 2023], ficando em 31,2 vezes" (Pacto Nacional de Combate às Desigualdades, 2024, p. 31).

[211] Como esclarece Silveira (2008, p. 43), "[a] ideia de exclusão foi introduzida na Sociedade da Informação para denunciar os processos que impedem a maioria da população de acessar a comunicação mediada por computador, ou seja, de utilizar as redes informacionais".

[212] De acordo com o *framework* conceitual adotado pela União Internacional de Telecomunicações (UIT) para a condução de pesquisas envolvendo habilidades digitais, elas se compõem de cinco competências fundamentais: informação e letramento digital, comunicação e colaboração, criação de conteúdo digital, segurança e solução de problemas (União Internacional de Telecomunicações, 2020, p. 62, tradução nossa).

[213] Há no Brasil, portanto, cerca de 12 milhões de domicílios sem acesso à Internet. Dentre esses, importa registrar que as justificativas predominantes para a falta de acesso são o custo do serviço (55%) e a falta de habilidade dos moradores com a Internet (50%) (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 27).

socioeconômico[214], na medida em que, ao passo que 67% dos domicílios inseridos nas classes DE estão conectados, ao olhar-se para as classes A e B, o percentual sobe para 98%. Por outro lado, há acesso à Internet em 74% dos domicílios situados em áreas rurais, enquanto 86% dos lares nas regiões urbanas têm conexão à rede mundial de computadores (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 65).

Já no que diz respeito aos *cidadãos brasileiros* (com 10 anos ou mais) que já tenham utilizado a Internet, ainda de acordo com a TIC Domicílios 2023, o percentual é de 89% (aproximadamente 156 milhões de pessoas). Dentre os 21 milhões de indivíduos que declararam nunca ter acessado a Internet (em números aproximados) – dos quais 42% têm 60 anos ou mais, e 22% pertencem às classes DE – o principal motivo apontado foi a *falta de habilidade* (*Idem*, p. 27). Noutra perspectiva, considerando-se as habilidades digitais exercidas pelos brasileiros de 60 anos ou mais que tenham utilizado a Internet, a alteração de configurações de privacidade foi a *menos* referida[215] (apenas 13%), o que, de acordo com a pesquisa, "pode indicar maior vulnerabilidade diante de riscos digitais" (*Idem*, p. 79).

A TIC Domicílios 2023 nos revela como condição socioeconômica, faixa etária, exclusão digital e habilidades digitais são fatores importantes – por guardarem estreita correlação entre si – na avaliação da relação dos brasileiros com as tecnologias de informação e comunicação (e, *a fortiori*, com o controle exercido sobre os próprios dados pessoais). É à luz desse cenário que importa discutir as potencialidades do paradigma do controle enquanto pressuposto epistemológico essencial do regime jurídico brasileiro de proteção de dados pessoais. Como bem observado por Comini, Gozzi e Perra (2024),

> Em toda a América Latina, a exclusão digital não é apenas uma questão tecnológica, mas um reflexo explícito da desigualdade de renda. O Brasil não é exceção. O acesso à internet, uma porta de entrada crucial para a educação, oportunidades de emprego e serviços essenciais, continua a ser distribuído de modo desigual. A pesquisa [conduzida pelos próprios autores] destaca uma disparidade significativa - indivíduos mais ricos geralmente desfrutam de conectividade contínua, enquanto as populações mais pobres muitas vezes lutam com acesso limitado ou nenhum, perpetuando as divisões socioeconômicas e impedindo o desenvolvimento regional.

---

[214] Gonçalves e Diniz (2024), a propósito, anotam: "Apesar do índice alto de domicílios que acessam a internet, a qualidade do acesso é discrepante entre classes, regiões e grupos sociais. Parte da população não dispõe de infraestrutura complexa que possibilite, por exemplo, a realização de atividades escolares e o estudo ou trabalho à distância".

[215] Segundo dados do Censo Demográfico de 2022, conduzido pelo Instituto Brasileiro de Geografia e Estatística (IBGE), há 32,1 milhões de idosos no Brasil. O número representa um aumento de 56% em relação a 2010. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38186-censo-2022-numero-de-pessoas-com-65-anos-ou-mais-de-idade-cresceu-57-4-em-12-anos. Acesso em: 10 dez. 2024.

Efetivamente, em um país marcado por brutais desigualdades – e pelo assustador índice de 12,3% de analfabetos funcionais[216] –, que têm correlação direta com os níveis de conectividade (21 milhões de excluídos digitais e 12 milhões de domicílios sem acesso à Internet, de acordo com a TIC Domicílios 2023) e com a aquisição e o desenvolvimento de habilidades digitais básicas, efetivar o direito fundamental à proteção de dados pessoais a partir do controle individual é uma tarefa, quando menos, desafiadora.

É relevante ter-se em perspectiva que o fluxo de dados pessoais em ambientes digitais importa, também, aos milhões de brasileiros que não têm (ou nunca tiveram) acesso à Internet, na medida em que, mesmo que em suas atividades cotidianas não a utilizem, a forçosa participação no mercado de consumo – ou mesmo a utilização de serviços públicos – implica, invariavelmente, o tratamento de seus dados pessoais com o uso de sistemas digitais. Ainda que assim não fosse, o art. 5º, LXXIX, da Constituição Federal, torna claro que o direito fundamental à proteção de dados pessoais se estende, também, às atividades de tratamento realizadas em suporte físico.

Se, por um lado, os números mais recentes sobre a exclusão digital no Brasil causam preocupação – como referido, aproximadamente 21 milhões de indivíduos em 2023, muito embora o acesso à Internet seja um dos objetivos da disciplina do uso da Internet no Brasil (nos termos do art. 4º, I, do Marco Civil da Internet – MCI) –, por outro, os índices a respeito das habilidades digitais são ainda mais alarmantes.

Segundo levantamento conduzido pela Agência Nacional de Telecomunicações (Anatel), apenas 29,9% dos brasileiros têm habilidades digitais *básicas* (como copiar ou mover um arquivo ou pasta, ou enviar e-mails com arquivos anexados, por exemplo). O resultado é compatível com aqueles obtidos pela TIC Domicílios 2023, que apurou que, dentre os usuários de Internet, apenas 39% alteraram configurações de privacidade[217] para limitar o compartilhamento de seus dados pessoais (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 78).

No que concerne às habilidades digitais *intermediárias*, o percentual é ainda menor: apenas 17,9% dos brasileiros são capazes de criar apresentações eletrônicas ou de encontrar, baixar, instalar e configurar um *software*, por exemplo. O recorte regional reforça a compreensão corrente de que *há vários "Brasis" dentro do mesmo Brasil*. Como identificou a

---

[216] Segundo dados do Relatório Nacional do 5º Ciclo de Monitoramento das Metas do Plano Nacional de Educação 2024 (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, 2024, p. 218).

[217] De acordo com o *toolkit* de habilidades digitais editado pela União Internacional das Telecomunicações, a alteração de configurações de privacidade em *smartphones* é uma habilidade básica (UIT, 2018, p. 6).

pesquisa conduzida pela Anatel, considerando-se a discrepância entre o percentual de indivíduos com habilidades intermediárias nas regiões sudeste (21,5%) e nordeste (12%), "cerca de 4,8 milhões de pessoas teriam que alcançar o nível intermediário de habilidades tão somente para que a proporção **futura** do NE se equipare à **atual** proporção do SE" (Anatel, 2024, p. 13, grifo no original).

Os recortes de classe social e nível de renda, novamente, se mostram importantes para compreendermos a relação direta entre desigualdade socioeconômica e habilidades digitais básicas. Enquanto 53,5% do demonstrativo geral das habilidades digitais básicas dos brasileiros é ocupado por indivíduos pertencentes à classe A, o quantitativo representado pelas classes DE corresponde a apenas 12,5% do total (Anatel, 2024, p. 10). Já no cenário global, dentre os países integrantes do G20, apenas a Turquia (com 28,2%) e a África do Sul (com 15,1%) ficam atrás do Brasil no *ranking* do percentual de indivíduos com habilidades digitais básicas (Anatel, 2024, p. 21).

Os índices de habilidades digitais mencionados contrastam, curiosamente, com o número de usuários brasileiros ativos em plataformas digitais. No quinto maior mercado de mídias sociais do mundo[218], enquanto apenas 1 a cada 4 indivíduos tem habilidades digitais básicas, 8 a cada 10 utilizam plataformas de comunicação, como o *WhatsApp*, e redes sociais, como *Instagram*, *Facebook* ou *TikTok* (Núcleo de Informação e Coordenação do Ponto BR, 2024, p. 81). Tais dados estatísticos bem demonstram os delicados contornos do cenário formado, no Brasil, pela interação entre desigualdades socioeconômicas, habilidades digitais e uso das plataformas digitais. É sobre essa complexa e multifacetada realidade que incide o regime jurídico de proteção de dados pessoais, estruturado, em larga medida, sobre o controle do indivíduo sobre o fluxo informacional a seu respeito nos ambientes digitais. Como oportunamente advertem Bandura e Leal (2022, p. 2)

> [...] adquirir o conjunto certo de habilidades digitais não é importante apenas para o aprendizado e para a prontidão da força de trabalho: habilidades digitais também são vitais para promover sociedades mais abertas, inclusivas e seguras. Quando as pessoas interagem com infraestruturas digitais, elas precisam estar cientes dos riscos à privacidade e aos dados, bem como dos desafios de cibersegurança (por exemplo, *ransomware* e ataques de *phishing*). (Tradução nossa)

O cenário europeu difere, em larga medida, do brasileiro. Por meio do *Digital Economy and Society Index* (DESI), a Comissão Europeia monitora, desde 2014, a *performance* dos Estados-Membros da União Europeia com relação ao uso de tecnologias digitais por seus

[218] Disponível em: https://epocanegocios.globo.com/tecnologia/noticia/2024/02/saiba-qual-e-a-rede-social-mais-usada-no-brasil.ghtml. Acesso em: 10 dez. 2024.

cidadãos, de sorte a identificar pautas prioritárias de ação institucional nacional, bem como a indicar áreas-chave para políticas digitais no âmbito comunitário. Uma das dimensões de análise do DESI é, exatamente, o nível de habilidades digitais[219].

De acordo com o DESI 2024, o percentual *médio* de indivíduos, em toda a União Europeia, que tenham *no mínimo* habilidades digitais básicas, é de 55,56%. Os índices mais altos pertencem à Holanda e à Finlândia, com 82,7% e 81,9%, respectivamente. Os mais baixos, por outro lado, pertencem à Bulgária (com 35,5%) e à Romênia (com 27,7%)[220]. É especialmente relevante notar que um dos eixos de avaliação que integram o levantamento anual do DESI sobre os índices de habilidades digitais básicas é o da *segurança*, que envolve, essencialmente, competências a respeito da proteção de dados pessoais nos ambientes digitais[221]. Confira-se a descrição desse vetor de avaliação:

> 4. *Segurança*: Gerenciar o acesso aos seus próprios dados pessoais verificando se o site onde o entrevistado forneceu dados pessoais era seguro, lendo as declarações de privacidade antes de fornecer dados pessoais, restringindo ou recusando o acesso à sua localização geográfica, limitando o acesso ao perfil ou conteúdo em sites de redes sociais ou armazenamento on-line compartilhado, recusando-se a permitir o uso de dados pessoais para fins publicitários, alterando as configurações no próprio navegador da Internet para impedir ou limitar cookies em qualquer um dos dispositivos do entrevistado. (Tradução nossa)

Cabe acrescentar, por fim, que, no Brasil, ainda não existe uma estratégia de governo voltada ao letramento digital. O Decreto Federal n. 11.542, de junho de 2023, instituiu Grupo de Trabalho Interministerial (GTI) para produzir subsídios para a elaboração da *proposta* de um Plano Nacional de Inclusão Digital (PNID). Os subsídios a serem produzidos pelo GTI deverão contemplar, dentre outros elementos, o letramento digital e a promoção de habilidades digitais (art. 1º, parágrafo único, I) e a necessidade de habilidades digitais mínimas para o pleno exercício da cidadania (art. 1º, parágrafo único, VI). Até dezembro de 2024, os trabalhos do GTI ainda não haviam começado[222].

---

[219] Os outros três parâmetros de pesquisa do DESI são infraestrutura digital, digitalização dos negócios e digitalização dos serviços públicos. Disponível em: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts. Acesso em: 13 dez. 2024.

[220] Disponível em: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dsk_bab&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE. Acesso em: 13 dez. 2024.

[221] Disponível em : https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/indicators. Acesso em: 17 dez. 2024.

[222] Disponível em: https://www.gov.br/mcom/pt-br/noticias/2024/novembro/grupo-de-trabalho-para-desenvolvimento-do-plano-nacional-de-inclusao-digital-comeca-em-2025. Acesso em: 13 dez. 2024.

Considerando-se o contexto brasileiro – e recordando-se que, segundo a pesquisa de Luguri e Strahilevitz (2021, p. 81), índices menores de instrução têm relação direta com o aumento da vulnerabilidade a padrões obscuros –, passaremos a discutir a adequação entre o *paradigma do controle*, adotado pela LGPD, e a proteção da autonomia individual no contexto das plataformas digitais. Desde logo, mostra-se fundamental realçar a precisa observação de Frazão (2024, p. 12), ao comentar sobre o fenômeno das arquiteturas enganosas à luz da realidade brasileira:

> Todas essas estratégias, que já são extremamente graves em países desenvolvidos, tornam-se ainda mais preocupantes em um país que, como o Brasil, há grandes índices de analfabetismo – inclusive o funcional – e mesmo de ignorância sobre aspectos centrais da vida social. Assim, na ausência das proteções que derivariam do conhecimento e de uma boa educação, as possibilidades de manipulação aumentam consideravelmente.

A reflexão crítica sobre o paradigma do controle impõe prévia contextualização histórica da aprovação da LGPD, a fim de identificar as circunstâncias políticas, sociais e econômicas da ocasião e dimensionar a sua influência sobre a formação do *espírito* da norma. Além disso, o resgate histórico mostra-se oportuno a bem de compreender os pressupostos acolhidos pelo legislador brasileiro ao definir os contornos e características do regime jurídico de proteção de dados pessoais.

Como já tivemos ocasião de referir, a lei brasileira – assim como diversas outras leis de proteção de dados pessoais ao redor do mundo[223] – manifesta nítida inspiração no Regulamento Geral de Proteção de Dados europeu[224], que entrou em vigor em 2018. Anote-se, desde logo, a respeito da norma europeia, que o RGPD se situa na esteira de um longo processo histórico – político, legislativo e jurisprudencial – de afirmação de garantias individuais relacionadas à tutela da privacidade que, posteriormente, evoluiriam no contexto do reconhecimento da necessidade de proteção das liberdades fundamentais diante do fenômeno do tratamento automatizado de dados pessoais e da criação dos bancos de dados eletrônicos[225].

---

[223] "Em todo o mundo, os regimes de proteção de dados se concentram em quando os dados podem ser coletados, como estão sendo tratados, quando podem ser acessados ou devem ser excluídos e se são pessoais, confidenciais ou desidentificados." (Richards; Hartzog, 2020a, p. 1, tradução nossa)

[224] "Apesar das diferentes técnicas legislativas, há uma convergência perceptível entre os princípios previstos no RGPD e na LGPD. Essa convergência pode ser atribuída menos a uma influência direta do processo legislativo europeu na lei brasileira do que a um longo processo de construção de um consenso transnacional acerca dos princípios básicos que regem essa matéria." (Mendes; Bioni, 2019, p. 165)

[225] "A proteção de dados no estilo da UE não foi um trabalho apressado. É fruto de décadas de pensamento cuidadoso com base em experiência real. O RGPD é o produto de montanhas de sabedoria coletiva, negociação e experiência, incluindo vinte anos de experiência com a Diretiva e vinte anos de desenvolvimento dos FIPs antes disso. O próprio RGPD levou anos para ser formulado." (Richards; Hartzog, 2020b, p. 1717, tradução nossa)

Nesse particular, cabe fazer menção à Convenção 108[226] do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 1981 e, no mesmo sentido, à Carta dos Direitos Fundamentais da União Europeia, de 2000, cujo art. 8º expressamente previu a proteção de dados pessoais como um direito fundamental[227].

Já ao contrário da longa evolução legislativa, jurisprudencial e dogmática do contexto europeu, no Brasil, contingências históricas (e, sobretudo, pressões externas) impulsionaram, em um espaço de tempo inferior a dez anos – do anteprojeto à sanção –, a tramitação do processo legislativo de nossa LGPD, que se integrou ao ordenamento jurídico nacional sem que houvesse propriamente uma tradição ou aculturamento coletivo e institucional sobre o tema da proteção de dados, ou mesmo conhecimento adequado a respeito da matéria que estava a ser debatida, à época, no âmbito do Poder Legislativo[228].

Como veremos com maior detalhamento, diferentemente do contexto europeu, o advento tardio[229] da LGPD no ordenamento jurídico brasileiro foi marcado por influências internacionais – notadamente as relações comerciais com países estrangeiros – bem como pelo próprio incremento do fluxo transnacional de dados pessoais decorrente do rápido desenvolvimento das tecnologias da comunicação e informação a partir da segunda década do século XXI.

---

[226] Confira-se a redação do art. 1º da Convenção 108/1981: "Artigo 1 – Objeto e finalidade. A presente Convenção tem por finalidade proteger todas as pessoas, independentemente da sua nacionalidade ou residência, no que diz respeito ao tratamento dos seus dados pessoais, contribuindo assim para o respeito dos seus direitos humanos e liberdades fundamentais e, em especial, do direito à vida privada."

[227] Assim está redigido o art. 8º da Carta: "Artigo 8.º Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

[228] Necessário referir, a fim de ilustrar a falta de conhecimento do público geral sobre o tema da proteção de dados pessoais, à necessidade de se cogitar de estratégias de comunicação em massa destinadas a tornar a pauta mais difundida dentre os cidadãos brasileiros. Um desses esforços está na campanha "Seus Dados São Você: por que o Brasil precisa de uma lei de proteção de dados pessoais", idealizada, em 2017, pela Coalizão Direitos na Rede. Nesse sentido, cf. https://idec.org.br/noticia/seus-dados-sao-voce-campanha-alerta-sobre-uso-de-informacoes-pessoais. Acesso em: 13 dez. 2024.

[229] Na América Latina, o Chile foi o primeiro país a aprovar uma lei geral de proteção de dados pessoais (Ley n. 19.628/1999 – *Ley de Protección de la Vida Privada*). Interessante destacar, na esteira do que leciona Rostión (2015, p. 501), que a autodeterminação informativa surgiu, no Chile, de uma criação jurisprudencial, tendo sido elevada à categoria de princípio: "Foi definido como o direito de cada pessoa de controlar o fluxo de informações que lhe dizem respeito – tanto na coleta quanto posteriormente processamento e utilização de dados pessoais – através de uma série de direitos subjetivos como o consentimento, o direito de acesso, a restrição, etc., sendo assim evidenciando seu aspecto ativo, frente ao direito à privacidade." (Tradução nossa)

O conjunto normativo da LGPD transparece o intento fundamental de *empoderar* os indivíduos – por meio do controle – como forma de reduzir assimetrias de poder. Com inspiração em uma tendência que deflui das *Fair Information Practices* (ou FIPs), concebidas na década de 70, a LGPD se estrutura sobre uma carta principiológica que inclui, por exemplo, os princípios de *necessidade* e *transparência*, voltados a impor limitações ao tratamento de dados pessoais por empresas e governos.

Além disso, forte na incidência do princípio da *autodeterminação informativa* – alçado a fundamento da disciplina brasileira da proteção de dados pessoais (art. 2º, II, da LGPD) e reconhecido pela jurisprudência do Supremo Tribunal Federal como decorrência dos direitos da personalidade[230] –, a LGPD busca instrumentalizar o controle individual por meio do exercício de um plexo de direitos decorrentes da titularidade[231] dos dados pessoais, como os de acesso e correção (art. 18, I e II). São estabelecidos, ainda, salvaguardas, vedações e deveres, todos de caráter eminentemente procedimental, a serem observados pelos agentes de tratamento, de que trataremos no presente capítulo.

Em suma, à luz dos dados mais recentes a respeito do uso das tecnologias digitais no contexto brasileiro, e considerando-se o cenário subjacente à aprovação da norma brasileira definidora de um regime jurídico nacional a respeito da proteção dos dados pessoais, cabe-nos, nesse capítulo, problematizar as efetivas aptidões do paradigma do controle para a tutela material de bens jurídicos da mais alta relevância no contexto de uma democracia liberal, envolvidos no tratamento de dados pessoais (autonomia, isonomia, privacidade, liberdade). Tais bens jurídicos – cabe acrescentar, por último – não se limitam à esfera individual, na medida em que os efeitos da manipulação, em particular, e do exercício assimétrico do poder por plataformas digitais, em geral, podem produzir significativas repercussões coletivas[232].

---

[230] Destaque-se, no Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387/DF (relatora a Ministra Rosa Weber, julg. em 07.05.2020, DJe de 12.11.2020), o voto proferido pelo Ministro Gilmar Mendes, no sentido de que a "abrangência da proteção atribuída ao direito de autodeterminação constitui importante chave interpretativa do âmbito de proteção do direito fundamental à proteção de dados pessoais, o qual não recai propriamente sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros".

[231] A propósito, como bem observam Frazão, Carvalho e Milanez (2022, p. 72), "a eventual natureza jurídica dos dados pessoais como titularidade certamente não será suficiente para resolver vários dos importantes problemas relacionados ao seu exercício e proteção".

[232] "[...] precisa ser destacado o fato de que o problema da privacidade não é apenas individual, mas apresenta importante dimensão coletiva, de forma que a proteção de dados não deixa de ser um valor social sob diversos aspectos. De fato, os dados de um indivíduo normalmente contêm informações também a respeito de outras pessoas, de forma que, quando se autoriza o tratamento de dados, normalmente também está se autorizando o tratamento de dados de terceiros." (Frazão; Carvalho; Milanez, 2022, p. 60)

3.1 A LGPD e o paradigma do controle

Embora os dados pessoais tenham sido objeto de certa proteção, no âmbito nacional, desde a entrada em vigor do Código de Defesa do Consumidor[233], em 1990 (ao regular os bancos de dados e cadastros de consumidores em seus arts. 43 e 44), foi a partir da LGPD, sancionada em 2018, que se deu a estruturação e a sistematização de um regime protetivo sobre o tema[234]. Posteriormente, vale notar, a proteção de dados pessoais veio a ser reconhecida como direito fundamental, de modo expresso, a partir da promulgação da Emenda Constitucional n. 115/2022 (art. 5º, LXXIX)[235].

Como referimos, discutir os contornos do regime jurídico estabelecido pela LGPD – e, inclusive, o seu alinhamento com o desenho normativo assentado pelo RGPD no contexto europeu – envolve compreender os seus antecedentes históricos, bem como as preocupações e aspirações institucionais existentes durante a tramitação legislativa do respectivo projeto de lei. Desse modo, ter-se-ão por mais claras os pressupostos subjacentes à formação do perfil da lei brasileira, abrindo-se campo adequado à crítica reflexiva sobre o paradigma do controle, a que nos propomos na presente investigação.

3.1.1 Um breve histórico: do Anteprojeto do Ministério da Justiça à LGPD

Desde a década de 1970 a presença do tema da proteção de dados pessoais se faz notar no debate institucional brasileiro, muito embora não sob a roupagem de uma norma sistematizadora e centralizadora de um regime jurídico geral. Como observa Doneda (2021, p. 246), uma das "centelhas que inspiraram a criação de uma sistemática própria para a proteção de dados" foi o projeto de instituição do Registro Nacional de Pessoas Naturais (RENAPE), "que previa a criação de um órgão de abrangência nacional que integraria o Registro Civil de Pessoas Naturais e a Identificação civil, além da criação de uma base de dados" (*Idem*, p. 247).

Por mais que uma narrativa pormenorizada da sucessão dos eventos históricos e dos avanços dogmáticos ocorridos até a afirmação de um direito autônomo à proteção de dados

---

[233] Doneda (2021, p. 245) nota, contudo, que "a ausência de um quadro normativo específico não implicava, em absoluto, que a matéria não fosse relevante, dado que diversas situações relacionadas ao uso de dados pessoais geravam efeitos jurídicos que, por vezes, chegavam aos tribunais".

[234] Uma sucessão de normas relacionadas ao tema pavimentou o caminho para que se editasse, por fim, uma Lei Geral de Proteção de Dados Pessoais no Brasil. Nesse particular, cabe fazer referência às Leis de Acesso à Informação e do Cadastro Positivo, ambas de 2011, e ao Marco Civil da Internet, de 2014, como diplomas legislativos que disciplinaram importantes aspectos relacionados à proteção de dados pessoais previamente à entrada em vigor da LGPD. Todavia, como leciona Rodríguez (2021, p. 147), "a efetiva proteção jurídica dos dados pessoais no Brasil exigiu a criação de uma normativa geral a estabelecer os principais regramentos procedimentais a serem atendidos [...]".

[235] "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

pessoais não se coadune com o escopo investigativo deste trabalho[236], cabe-nos registrar que, em um passado mais recente, o início dos debates a respeito da edição de uma lei geral de proteção de dados pessoais no Brasil remonta ao ano de 2010, em que o Ministério da Justiça abrira consulta pública – realizada inteiramente pela Internet – para colher subsídios a respeito de um texto-base sobre o tema[237].

Desde a sua formulação inicial, o texto gestado no âmbito do Ministério da Justiça – que começara a ser formulado ainda em 2005 – já atribuía ao controle individual o papel de protagonismo no regime jurídico de proteção de dados pessoais. Como veiculado em reportagem publicada à época da primeira consulta pública[238],

> De acordo com o doutor em Direito Civil Danilo Doneda, consultor do Ministério da Justiça e um dos responsáveis pela elaboração do anteprojeto, **a proposta não se baseia na ideia de "silêncio", ou seja, de sigilo dos dados pessoais, mas sim de controle**. Numa compra feita a prazo, em que é necessário cadastro do consumidor, **a empresa terá de pedir autorização expressa para usar as informações** e dizer o que vai fazer com os dados. (Grifo nosso)

No âmbito do Poder Legislativo, a primeira propositura relativa a uma norma, de caráter geral, acerca do tema da proteção de dados pessoais, ocorreu em 2012 (o PL 4.060/2012, de autoria do Deputado Federal Milton Monti). Cabe destacar que esse PL, dentre outras características, adotava o conceito *reducionista* de dado pessoal[239], definindo-o como "qualquer informação que permita a identificação exata e precisa de uma pessoa determinada" (art. 7º, I), e não condicionava o tratamento de dados pessoais não sensíveis à previsão de alguma hipótese legal autorizativa, impondo ao responsável apenas o dever de tratar os dados pessoais "com lealdade e boa fé, (*sic*) de modo a atender aos legítimos interesses dos seus titulares" (art. 11).

---

[236] Para um quadro detalhado a respeito da evolução normativo-dogmática da proteção de dados pessoais no Direito brasileiro, cf., dentre outros, Doneda, 2021, p. 265 *et seq*., Ferreira; Pinheiro; Marques, 2022; Andréa; Arquite; Camargo, 2020; Sarlet, 2020.

[237] Doneda (2021, p. 252), todavia, refere que o processo que resultaria na elaboração da LGPD foi deflagrado em 2005, a partir de discussões havidas no âmbito do Subgrupo de Trabalho nº 13 (SGT13) do Mercosul, responsável por debater e encaminhar propostas em temas referentes ao Comércio Eletrônico. Como narra o autor, alguns marcos do processo de debate sobre o tema da proteção de dados pessoais pelo governo brasileiro "são, por exemplo, a realização, em 2005, do 'I Seminário Internacional sobre Proteção de Dados Pessoais', promovido pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior, do qual participaram, entre diversas autoridades e juristas, três presidentes de autoridades estrangeiras de proteção de dados: Stefano Rodotà (Diretor do Garante Italiano), José Luiz Piñar Manas (Presidente da autoridade espanhola) e Juan Antonio Travieso (Presidente da autoridade argentina)".

[238] Disponível em: https://www.conjur.com.br/2011-jan-25/consulta-publica-traca-diretrizes-lei-protecao-dados-pessoais/. Acesso em: 21 dez. 2024.

[239] Como esclarecem Frazão, Carvalho e Milanez (2022, p. 49), tal conceito "caracteriza-se por limitar a qualificação de dado pessoal àquele que esteja relacionado tão somente a uma pessoa identificada, ou seja, alguém que se conhece e se individualiza em meio a uma coletividade."

Em 2013, um importante acontecimento catalisou as discussões em torno da edição de um marco legal que garantisse tutela adequada às liberdades fundamentais, considerados os usos dos dados pessoais no ciberespaço e as potenciais violações deles decorrentes. Edward Snowden, ex-analista da Agência de Segurança Nacional dos Estados Unidos (*National Security Agency* – NSA), divulgou uma série de documentos ultrassecretos que revelavam a existência de uma sofisticada operação de espionagem do governo norte-americano a partir de dados obtidos por empresas como Google, Facebook e Microsoft.

Dentre os alvos da espionagem norte-americana estavam cidadãos e empresas brasileiras, sendo o Brasil "o país mais espionado da América Latina"[240]. Até mesmo comunicações da então presidente Dilma Roussef e de integrantes do alto escalão do Poder Executivo Federal foram interceptadas[241]. As revelações de Snowden causaram forte impacto sobre o contexto institucional brasileiro, tendo a presidente Dilma Roussef, na abertura da Assembleia Geral da ONU – em setembro daquele ano –, proferido duro discurso contra as ações de espionagem dos órgãos de inteligência dos Estados Unidos, afirmando, à época, "que 'a rede global de espionagem' da NSA provocou 'indignação e repúdio' em 'amplos setores da opinião pública mundial' e ainda mais no Brasil [...]"[242].

Ao mesmo tempo em que a divulgação do escândalo de espionagem[243] acelerou a aprovação do Marco Civil da Internet (que viria a ocorrer em abril de 2014), as articulações no âmbito do Poder Legislativo sobre a proteção de dados pessoais ganharam tração. Assim, três PLs foram propostos no Senado Federal sobre o tema: o PLS 131/2014 (resultante da "CPI da Espionagem"[244]), o PLS 181/2014 (proposto pelo Senador Vital do Rêgo), e o PLS 330/2013 (proposto pelo Senador Antonio Carlos Valadares), ao qual os demais foram apensados, por tratarem da mesma matéria[245].

---

[240] Disponível em: https://oglobo.globo.com/politica/relembre-caso-de-espionagem-da-nsa-cidadaos-empresas-no-brasil-9782018. Acesso em: 10 dez. 2024.

[241] Disponível em: https://noticias.uol.com.br/internacional/ultimas-noticias/2013/09/04/brasil-e-o-grande-alvo-dos-eua-diz-jornalista-que-obteve-documentos-de-snowden.htm. Acesso em: 10 dez. 2024.

[242] Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130924_dilma_assembleia_onu_lgb. Acesso em: 12 dez. 2024.

[243] "O Brasil ficou à frente da discussão internacional ao apresentar, com a Alemanha, uma resolução da ONU que foi a primeira grande iniciativa das Nações Unidas em defesa ao direito à privacidade em 25 anos. O Brasil ajudou a criar 'uma nova onda' na discussão global sobre a privacidade digital, e a liderou com base em sólidos princípios democráticos." Disponível em: https://www.hrw.org/pt/news/2014/06/04/253983. Acesso em: 10 dez. 2024.

[244] Assim dispôs o Relatório Final n. 1/2014, da "CPI da Espionagem": "[...] a interceptação irrestrita de comunicações, bem como a gravação injustificada de dados pelos serviços de inteligência dos EUA denota implacável violação à privacidade do ser humano". Disponível em: https://www2.senado.leg.br/bdsf/handle/id/609904. Acesso em: 13 dez. 2024.

[245] Interessante destacar o seguinte trecho da justificação do PLS 330/2013, que torna evidentes as repercussões do escândalo de espionagem revelado por Edward Snowden sobre a percepção da necessidade de uma

Em 2015, uma nova consulta pública foi aberta, no âmbito do Ministério da Justiça, para que fossem colhidos comentários a respeito do Anteprojeto de Lei[246] elaborado a partir dos subsídios oferecidos pela sociedade civil na primeira consulta pública sobre o tema. Essa segunda consulta, que teve mais de 1.000 contribuições, redundou na redação final do texto – com inspiração na norma europeia então vigente, a Diretiva 95/46/EC[247] – que, uma vez enviado à Câmara dos Deputados em maio de 2016, veio a se converter no PL 5.276/2016 (posteriormente apensado ao PL 4.060/2012)[248].

Tem-se, a partir de então, dois PLs *principais* a respeito de normas gerais sobre a proteção de dados pessoais – de conteúdo semelhante –, cada um tramitando perante uma das Casas do Congresso Nacional. Vale notar, de acordo com o registro histórico da tramitação legislativa elaborado pelo Observatório da Privacidade e Proteção de Dados, que as equipes envolvidas na produção dos textos finais – tanto no Senado quanto no Ministério da Justiça – estabeleceram "um processo de troca de informações e colaboração no conteúdo de ambos os textos"[249].

Cabe acrescentar que na Câmara dos Deputados, em que tramitavam os PLs 4.060/2012 e 5.276/2016, foi instaurada a "Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 4060, de 2012" (sob relatoria do Deputado Federal Orlando Gomes), que promoveu, ao

---

regulamentação geral do tema da proteção de dados pessoais: "O exemplo mais palpável dessa prática [uso de dados pessoais em detrimento da honra de seus titulares] talvez seja o das denúncias sobre o acesso do Estados Unidos aos dados de cidadãos de vários países, como revelou o ex-técnico da CIA Edward Snowden. As informações vazadas por ele permitiram à imprensa internacional detalhar alguns programas de vigilância do governo americano contra a população utilizando servidores de empresas como Google, Apple e Facebook. Há ainda documentos que mostram ações de espionagem em diversos países da América, incluindo o Brasil"

[246] "O Anteprojeto de Lei de Proteção de Dados Pessoais foi elaborado pela Senacon, em conjunto com a Secretaria de Assuntos Legislativos do Ministério da Justiça, após a realização de dois debates públicos, realizados via internet. O primeiro em 2010 e o segundo neste ano. No total foram mais de 2000 contribuições dos setores público e privado, academia e organizações não-governamentais. Durante os últimos cinco anos também foram realizadas inúmeras reuniões técnicas, seminários e discussões por diversos órgãos e entidades." Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais. Acesso em: 10 dez. 2024.

[247] Oportuno transcrever, a propósito, excerto da manifestação final da Comissão Especial destinada a proferir parecer ao Projeto de Lei n. 4.060/2012: "**Grande fonte de inspiração para os projetos advém do arcabouço europeu**. O primeiro instrumento daquele bloco na temática é a Convenção do Conselho da Europa nº 108, de 1981, 'Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais'. O segundo instrumento geral é a Diretiva Europeia nº 46, de 1995, conhecida como Diretiva de Proteção de Dados. Em terceiro lugar, citamos a Diretiva nº 58, de 2002, focada na proteção da privacidade no âmbito das comunicações eletrônicas." (grifo nosso)

[248] Nas palavras de Doneda (2021, p. 254): "Em 2015, uma nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais foi tornada pública pela Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça, que a submeteu a um novo debate público, também realizado pela Internet. Neste, que foi o último debate público, contabilizaram-se 1.127 contribuições enviadas diretamente na plataforma do debate, além de 67 contribuições e comentários enviadas em formato documental."

[249] Disponível em: https://observatorioprivacidade.com.br/memoria/2010-2015-o-tema-entra-em-pauta/. Acesso em: 12 dez. 2024.

todo, 11 audiências públicas e 2 seminários internacionais, organizados por temas[250]. Ao fim das disputas políticas relacionadas à aprovação dos PLs que tramitavam perante as diferentes Casas do Parlamento – cujo detalhamento, todavia, não se coaduna com o escopo investigativo desta pesquisa[251] –, sagrou-se vencedora a proposta oriunda do Poder Executivo, convertida na Lei Federal n. 13.709, de 14 de agosto de 2018.

Posto o contexto histórico em que se situaram a formulação e a tramitação do PL 5.276/2016, importa-nos, em particular, incursionar sobre alguns de seus aspectos que nos parecem particularmente relevantes para uma compreensão substancial das preocupações e aspirações institucionais relacionadas à temática da proteção de dados pessoais. Para tanto, é interessante notar, em primeiro lugar, as razões de apresentação do Anteprojeto de Lei gestado no Ministério da Justiça (que, posteriormente, viria a se tornar o PL 5.276/2016). Como se colhe da Mensagem EMI n. 73/2016/MJMP,

> A utilização, cada vez mais intensa, de dados pessoais na sociedade da informação cria um desequilíbrio entre os poderes dos indivíduos, titulares de seus próprios dados pessoais, e os dos utilizadores de tais dados, justamente pela quantidade de informações pessoais que as novas tecnologias são capazes de agregar e utilizar.

Sintonizado ao contexto histórico em que situado (no qual se destacavam, em especial, o escândalo de espionagem da NSA e a sanção, um ano após, do Marco Civil da Internet), e amparado pelas inúmeras contribuições recebidas nas duas consultas públicas (de 2010 e 2015) a respeito do tema, as razões do anteprojeto situavam os desafios a serem enfrentados pelo Direito na perspectiva dos crescentes e rápidos avanços nas tecnologias da informação e comunicação.

Em *primeiro* lugar, destacou-se a preocupação do Poder Executivo com o fenômeno da crescente *assimetria de poderes* entre indivíduos e agentes de tratamento, que "influencia diretamente a vida das pessoas, afetando oportunidades, escolhas e interações sociais, elementos que compõem o livre desenvolvimento da sua própria personalidade" (ainda nos termos da Mensagem EMI n. 73/2016/MJMP).

Nesse particular, nas razões apresentadas à Presidência da República, o Ministério da Justiça reitera, em diversas passagens, que o **controle**[252] seria, por excelência, o mecanismo a

---

[250] Disponível em: https://observatorioprivacidade.com.br/memoria/2016-2017-o-anteprojeto-chega-a-camara/. Acesso em: 12 dez. 2024.

[251] Para maior aprofundamento no tema, recomenda-se a consulta ao portal "Memória da LGPD", que detalha a sucessão de eventos que culminaram na sanção da Lei Federal n. 13.709/2018, no seguinte endereço: https://observatorioprivacidade.com.br/memorias/. Acesso em: 13 dez. 2024.

[252] No mesmo sentido, a Justificação do PLS n. 330/2013 revela o pressuposto do exercício do controle – materializado pelo consentimento com o tratamento de dados pessoais – como mecanismo de tutela dos dados

ser utilizado pela norma para assegurar "autonomia ao titular"[253] e mitigar o desequilíbrio de poderes. Em ao menos duas passagens, que adiante transcrevemos, evidencia-se o papel fundamental do controle individual, decorrente da noção de autodeterminação informativa, como elemento estruturante do regime jurídico estabelecido pela LGPD:

> A proposta **visa assegurar ao cidadão o controle e a titularidade sobre suas informações pessoais, com fundamento** na inviolabilidade da intimidade e da vida privada, na liberdade de expressão, comunicação e opinião, **na autodeterminação informativa**, no desenvolvimento econômico e tecnológico, bem como na livre iniciativa, livre concorrência e defesa do consumidor. (Grifo nosso)

> A aplicação efetiva do direito individual fundamental à privacidade depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na construção de uma democracia da informação **que proteja tanto a autodeterminação e a liberdade de controle das informações pessoais pelo cidadão** [...]. (Grifo nosso)

Em *segundo* lugar, um outro eixo central do anteprojeto foi o *alinhamento do Brasil ao cenário global*, tendo-se em vista tanto a desconformidade com padrões internacionais sobre o tema quanto as oportunidades comerciais advindas da adequação do País a normas estrangeiras[254] a respeito da proteção de dados pessoais. Nesse sentido, tal como consta da Mensagem EMI n. 73/2016/MJMP, "a partir da promulgação da lei brasileira [...], o país estará apto a entrar no rol de Estados com os quais as empresas europeias podem realizar negócios que envolvam o tratamento de dados pessoais".

Por fim, em *terceiro* lugar, mostra-se nítida a intenção do Poder Executivo de *compor diferentes perspectivas e interesses* de representantes do setor empresarial e organizações da sociedade civil[255]. Sem a intenção de impor restrições ou vedações substanciais ou peremptórias

---

pessoais: "Atualmente, o desenvolvimento da informática está a comprovar: dados pessoais trafegam pelas redes de informação, no mais das vezes sem o consentimento daquele a quem se referem, são comercializados, publicados, usados em detrimento de sua honra, em manifesta contrariedade aos preceitos constitucionais aludidos."

[253] "A principal intenção do governo foi a de apresentar um texto base que assegure autonomia ao titular para decidir sobre o uso e a coleta de seus dados pessoais, como explica Juliana Pereira." Disponível em: https://www.camara.leg.br/noticias/449278-consulta-publica-sera-base-para-projeto-de-lei-sobre-protecao-de-dados-pessoais/. Acesso em: 10 dez. 2024.

[254] No mesmo sentido foi o posicionamento conclusivo da Comissão Especial destinada a proferir parecer ao Projeto de Lei n. 4.060/2012: "Importante pontuar que as propostas se inserem em um contexto mundial, portanto, maior, em que legislações nacionais são introduzidas em cada país, de forma a tratar da questão dos dados pessoais e garantir a proteção das pessoas de maneira harmônica. Ao mesmo tempo, a construção de um arcabouço similar entre os países gera um ambiente propício aos negócios, principalmente globais [...]."

[255] De acordo com texto publicado pela Coalizão Direitos na Rede em 2017: "Conforme a maneira pela qual o texto foi consolidado, aponta se tratar de uma iniciativa resultante do consenso entre os diversos setores mencionados [setor empresarial, comunidade científica e acadêmica, organizações da sociedade civil e cidadãos brasileiros]. As diferenças e modificações entre as versões pré e pós-consulta publicados, e o texto do anteprojeto, são claros indicadores de que se procurou chegar a uma redação equilibrada, a fim de salvaguardar a inovação e

a determinadas práticas, finalidades ou consequências relacionadas ao tratamento de dados pessoais – que poderiam causar constrições indesejáveis à inovação e à livre iniciativa –, o legislador optou por uma abordagem eminentemente procedimental, buscando *regular*, e não *proibir* o tratamento de dados pessoais (mesmo aqueles que pudessem representar alto risco a direitos fundamentais).

Nessa perspectiva, se, por um lado, não se buscava alijar do âmbito da legalidade as práticas de tratamento de dados pessoais responsáveis por causar (e agravar) as assimetrias de poder que o legislador pretendia combater, por outro, pretendeu-se regular o uso dos dados pessoais por meio do cumprimento de parâmetros objetivos, de forma a *legitimar*[256] o tratamento e, desse modo, delimitar "um espaço de segurança jurídica", com o qual o legislador buscou incentivar "a utilização lícita de dados [...], favorecendo o fluxo de dados por agentes responsáveis e o desenvolvimento de setores econômicos ligados, por exemplo, às tecnologias de informação", também de acordo com a Mensagem EMI n. 73/2016/MJMP[257].

A redação originária do PL 5.276/2016 foi apenas o *marco zero* do processo legislativo que culminou na sanção da LGPD, em agosto de 2018. Ao longo de seus mais de dois anos de tramitação, sobretudo no âmbito da Comissão Especial destinada a proferir parecer ao Projeto de Lei n. 4.060/2012, o texto originalmente proposto pelo Poder Executivo recebeu críticas e contribuições e, como mencionado, foi alvo de discussões ocorridas em seminários (inclusive internacionais) e em audiências públicas temáticas.

O substitutivo ao PL 5.276/2016, apresentado em maio de 2018, foi o resultado dos trabalhos desenvolvidos no âmbito da Comissão Especial, cujo pronunciamento final reforçou a centralidade da noção de *controle* individual sobre os dados pessoais. Ao dispor, por exemplo, sobre a redação do art. 7º, § 5º, do substitutivo[258] (que trata do exercício do controle – veiculado

---

a proteção da privacidade dos cidadãos." Disponível em: https://direitosnarede.org.br/2017/01/27/por-que-a-aprovacao-do-pl5276-16-e-fundamental-para-o-brasil/. Acesso em: 13 dez. 2024.

[256] Como se colhe da Mensagem EMI n. 73/2016/MJMP, "[p]ara que esses dados possam ser utilizados com fins transparentes e legítimos [...], são necessárias normas e mecanismos institucionais que estabeleçam os parâmetros e limites deste tratamento [...]".

[257] "Regras processuais dão segurança jurídica às entidades que regulam – um benefício dos padrões legais. As empresas geralmente fazem lobby por regras processuais, que são específicas e previsíveis em sua aplicação, em oposição a padrões flexíveis. O sucesso dessa dinâmica de busca de certeza pode ser atribuído à forma como os FIPs têm sido historicamente aplicados." (Cofone, 2024, p. 98, tradução nossa)

[258] Assim foi redigido o referido dispositivo: "§ 5º O responsável que obteve o consentimento a que faz referência o inciso I que necessitar comunicar ou compartilhar dados pessoais com outros responsáveis deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei". O texto sancionado pelo Presidente da República foi ligeiramente modificado, mantido o sentido original previsto no projeto de lei.

pelo consentimento individual – nas hipóteses de comunicação ou compartilhamento dos dados pessoais entre o controlador e outros controladores), assim se manifestou a Comissão:

> **A profusão de aplicações para os dados pessoais**, assim como de empresas do mesmo e de outros grupos empresariais que realizam o compartilhamento de dados coletados de titulares, **evidenciou, em vários casos, a perda do controle do titular sobre seus próprios dados**. **Como forma de permitir um maior domínio**, assim como facilitar a revogação de consentimentos porventura concedidos, prevemos um novo §5º, dispondo que na transferência de dados para outros responsáveis **será necessária a obtenção de consentimento** específico para esse fim. (grifo nosso)

Em suma, o histórico da tramitação do PL 5.276/2016 revela tanto a inspiração no modelo europeu quanto as três aspirações institucionais centrais – inalteradas no curso do processo legislativo – que se refletiram no texto final da LGPD: redução de assimetrias de poder, alinhamento aos padrões internacionais (notadamente o europeu) e conciliação entre interesses antagônicos de representantes do setor empresarial[259] e entidades relacionadas à proteção dos direitos dos titulares de dados pessoais.

Para que tais objetivos fossem atendidos, pretendeu-se, em primeiro lugar, mitigar assimetrias de poder por meio da afirmação da *titularidade*, o que se manifestou pela previsão de princípios e direitos que assegurassem aos indivíduos o exercício do *controle* sobre seus próprios dados pessoais (como, por exemplo, os direitos de oposição e de revogação do consentimento), alocando sobre eles próprios o ônus de tomarem, por si sós, decisões autônomas a respeito de sua privacidade[260]. Em segundo lugar, buscou-se alcançar a adequação aos parâmetros internacionais a partir da inspiração manifesta na Diretiva 95/46/EC (que, em 2016, viria a ser substituída pelo RGPD).

Em terceiro lugar, sem prever vedações taxativas (como, por exemplo, proibir expressamente o comércio de dados pessoais, ou o seu compartilhamento com o intuito de obter vantagem negocial ou econômica), na linha do que preconiza o modelo das FIPs[261], o legislador

---

[259] Vale pontuar, desde logo, a pertinente crítica de Waldman (2021, p. 52): "A privacidade como controle continua dominante porque aqueles com poder sobre nossos dados – a indústria da informação – têm um forte interesse em definir a privacidade como controle. Isso pode parecer contraintuitivo. Como nos dar controle sobre nossos dados pode ajudar a indústria a extraí-los de nós? Fácil. O discurso do controle é o discurso da autogovernança. E a autogovernança é uma farsa." (Tradução nossa)

[260] "[Regimes de privacidade baseados em] direitos apresentam aos indivíduos um fardo infinito de tarefas. As pessoas recebem algo para fazer, então elas sentem que estão no controle. Infelizmente, esse controle é frequentemente ilusório. Os direitos são frequentemente difíceis e demorados de invocar, então eles podem ser eficazes para uso ocasional, mas não para lidar com as hordas de empresas que estão tratando os dados das pessoas." (Solove, 2023, p. 984, tradução nossa)

[261] "Os Fair Information Practice Principles (FIPs), desenvolvidos com contribuições de americanos e europeus, estabeleceram o modelo para a privacidade em ambos os lados do Atlântico. Esses princípios se concentram em direitos processuais como transparência, consentimento, salvaguardas, limitações de propósito e minimização de dados, a serviço da autodeterminação informacional e de um ambiente sustentável para o processamento de dados. Por enfatizarem a escolha e a autonomia individual, os regimes baseados em FIPs tendem a não ter

recorreu à fixação de normas procedimentais por meio das quais se pudesse atestar a legitimidade das atividades de tratamento, estabelecendo-se uma relação de causa e efeito entre a demonstração objetiva da adoção das salvaguardas e dos requisitos estabelecidos pela LGPD e a consequente observância de seus princípios e fundamentos.

O perfil de nossa Lei Geral de Proteção de Dados Pessoais, como se buscou tornar claro, é caracterizado pelo emprego do paradigma do controle - centrado na hipótese legal do consentimento[262] – como forma de endereçar assimetrias de poder entre indivíduos, de um lado, e empresas e governos, de outro. É, também, marcado por uma perspectiva procedimental, para a qual o cumprimento de requisitos previstos na norma evidencia, por si só, a legitimidade do tratamento (e, portanto, a preservação de direitos fundamentais como a liberdade, a privacidade e a autonomia).

Um último ponto merece ser observado, ainda à luz de nosso regime jurídico de proteção de dados pessoais. A autonomia é tanto um *pressuposto* do exercício do controle individual (e, consequentemente, da mitigação das disparidades de poder) quanto um *resultado* desejado pelo legislador. Afinal, se, por um lado, a tomada de decisão individual a respeito dos fluxos informacionais – ao menos idealmente – depende da conformação de um espaço deliberativo livre de interferências indevidas[263], por outro, a proteção de dados pessoais – posta em movimento pelo exercício do controle individual – é instrumental à tutela e à promoção dos direitos fundamentais de liberdade, de privacidade e, da mesma forma, da própria autonomia individual.

Destacar a função da autonomia individual, considerado o nosso objeto de investigação, parece-nos tarefa de fundamental importância na crítica ao paradigma do controle. Como dito, o legislador estabeleceu uma ampla cartilha de princípios e de direitos relacionados à titularidade e, consequentemente, impôs aos agentes de tratamento uma série de deveres

---

proibições substantivas sobre tipos específicos de práticas de dados." (Richards; Hartzog, 2020a, p. 1, tradução nossa)

[262] Como notam Mendes e Fonseca (2020, p. 509), "o consentimento tem figurado como instrumento regulatório central e núcleo de legitimidade prática desse regime protetivo. Ele é lido, ainda, como expressão da autonomia individual e do controle do titular dos dados em torno de seus direitos de personalidade [...], contudo, sem inviabilizar o livre fluxo desses dados, elemento relevante para uma série de atividades econômicas e até mesmo para a elaboração de políticas públicas [...]".

[263] "Nesse paradigma, o indivíduo se encontra no centro do processo decisório acerca do que é feito com seus dados pessoais. Entretanto, nos casos em que o tratamento não está explicitamente autorizado por alguma base normativa, na prática, o positivo ideal de empoderamento do titular resulta na obtenção de seu consentimento individual frente aos termos do tratamento, após previamente informado a respeito da finalidade da coleta (notice and consent)." (Mendes; Fonseca, 2020, p. 513)

necessários à sua materialização, *idealizando*, em boa medida, as reais potencialidades do controle individual[264].

Ao estruturar desse modo o desenho regulatório fundamental do regime jurídico de proteção de dados pessoais, muito embora *reconhecendo* a necessidade de "promover na população o conhecimento das normas [...] sobre proteção de dados pessoais" (art. 55-J, VI, da LGPD), o legislador brasileiro padeceu de um otimismo exacerbado. Daí a inquietante indagação de Hartzog (2018, p. 432):

> Se o tratamento de dados é tão perigoso que requer permissão formal, e as escolhas só podem ser feitas de forma significativa em ambientes [...] limitados com pré-condições como "dado livremente, específico, informado, retratável e inequívoco", então por que estamos permitindo que os controladores se envolvam no que parece uma ficção, mesmo sob condições ótimas? (Tradução nossa)

Por um lado, o legislador desconsidera as inúmeras e cotidianas interferências sobre a livre expressão da autonomia individual no exercício dos direitos relacionados à titularidade (o que põe em xeque o paradigma do controle), notadamente no contexto das plataformas digitais, como o próprio *design*[265]. Por outro, ignora que a imposição de limitações às atividades de tratamento, por meio de adequações procedimentais, não impede o aprofundamento vertiginoso das assimetrias de poder entre os indivíduos e as plataformas digitais (e, consequentemente, de seu potencial manipulativo). Proteger a autonomia (e, bem assim, a privacidade), afinal, envolve restringir o próprio poder, e não apenas requerer demonstrações de que os dados pessoais obtidos a partir do exercício desse mesmo poder (e cujo tratamento dará ainda mais poder às empresas) foram adequadamente tratados:

> Regimes de proteção de dados também não conseguem levar em conta externalidades causadas pelos dados, como danos ambientais, roubo de atenção e degradação da interação social. Isso é um problema porque estamos apenas começando a ver os custos humanos e sociais associados à escala massiva de tratamento de dados e domínio de plataforma. Além dos principais danos relacionados à privacidade associados à coleta e ao uso de dados, a fome insaciável das empresas por informações pessoais está afetando negativamente nossa atenção e como gastamos nosso tempo, como nos tornamos cidadãos educados e informados e como nos relacionamos uns com os outros. (Richards; Hartzog, 2020b, p. 1695, tradução nossa)

---

[264] "Os direitos muitas vezes dão às pessoas apenas um controle superficial, não um controle significativo. As pessoas recebem informações, avisos e algumas escolhas limitadas, como optar por não participar ou se opor. Mas elas muitas vezes são bastante impotentes para fazer algo sobre os julgamentos que estão sendo feitos sobre elas com base em seus dados." (Solove, 2023, p. 986, tradução nossa)

[265] "Ao tornar o processo de navegação por nossas escolhas de privacidade mais fácil ou mais difícil, os designers de plataforma podem interferir em com nossa propensão a compartilhar. Nossas publicações, então, não são manifestações de nossas decisões autônomas sobre nossa privacidade. Em vez disso, elas refletem respostas predeterminadas à manipulação da plataforma por *design*." (Waldman, 2021, p. 54, tradução nossa)

Ao pretender mais *legitimar* as atividades de tratamento (por meio da adequação formal) do que – atento aos elementos que compõem o quadro da relação *substancial* estabelecida entre usuários e plataformas digitais – buscar *proibir* práticas de tratamento de dados pessoais que têm relação direta com violações sistemáticas à privacidade, como a manipulação (a arquitetura dos ambientes digitais é um indiferente regulatório[266]) e a extração massiva de dados pessoais (que pode ser habilmente justificada por relatórios ou testes de balanceamento, demonstrando-se a adequação ao princípio da *necessidade*[267]), o legislador não protege nem promove a autonomia individual[268].

Considerando-se o contexto do capitalismo de vigilância em que estamos inseridos, proteger a privacidade, a autonomia e a liberdade por meio da atribuição de direitos individuais de controle equivale a armar os indivíduos com facas para que, sozinhos, sejam capazes de enfrentar exércitos inteiros[269]. Nessa perspectiva, importa-nos compreender melhor os contornos dogmáticos do paradigma do controle no subcapítulo seguinte.

3.2. Mitigando assimetrias: empoderamento por meio do controle individual

Como tivemos ocasião de referir no Capítulo 1, a gênese de um direito autônomo à proteção de dados, dogmaticamente desvinculado da tutela da privacidade, está associada ao desenvolvimento de tecnologias da informação e comunicação[270] que viabilizaram o surgimento de grandes repositórios eletrônicos de dados pessoais (*databases*) no período posterior à Segunda Guerra Mundial. Essas novas tecnologias tornaram, a um custo baixo,

---

[266] "Às vezes somos levados a compartilhar demais simplesmente pelo *design* de serviços online. As plataformas projetam sistemas para fazer o compartilhamento parecer bom, tal como para nos encorajar a manter uma 'sequência' no Snapchat ou nos cutucar para compartilhar postagens antigas ou parabenizar outras pessoas no Facebook. Além disso, as plataformas tornam o compartilhamento muito fácil." (Hartzog, 2018, p. 427, tradução nossa)

[267] "Na realidade, os controladores não pretendem restringir o tratamento de dados ao mínimo necessário. Além disso, devido às muitas normas abertas e difusas, eles podem facilmente argumentar que o que fazem é 'necessário' para os propósitos que eles próprios definem [...], até que, em casos raros, alguma autoridade supervisora os impeça." (Koops, 2014, p. 7, tradução nossa)

[268] Como bem destacam Richards e Hartzog (2020b, p. 1696): "Requisitos procedimentais como obrigações de obter o consentimento das pessoas para práticas de dados acabam normalizando os tipos de coleta de dados e danos de vigilância que eles supostamente mitigam. Eles são uma receita para empresas explorarem e manipularem pessoas a serviço de cada vez mais dados." (Tradução nossa)

[269] "Os direitos colocam muito do ônus sobre os indivíduos para lutar uma guerra que eles não podem vencer. Tentar usar os direitos de privacidade como uma forma primária de proteger a privacidade é semelhante a armar um indivíduo com uma adaga para lutar contra um exército inteiro." (Solove, 2023, p. 978, tradução nossa)

[270] Assim lecionam Mendes e Fonseca (2020, p. 512), a respeito das razões subjacentes ao surgimento da proteção de dados pessoais enquanto ramo autônomo: "De um lado, esse desdobramento histórico se deu em razão da necessidade de expansão e de 'atualização' das formas jurídicas de tutela da personalidade dos cidadãos frente às mudanças tecnológicas ocorridas. De outro, estabeleceu-se também enquanto vetor de integração econômica dos países envolvidos e das dinâmicas empresariais multinacionais."

facilmente acessíveis as informações a respeito de indivíduos, além de terem possibilitado o seu armazenamento por tempo indeterminado[271].

Efetivamente, o fenômeno dos bancos de dados desencadeou importantes preocupações e indagações a respeito da tutela da autonomia individual, na medida em que as tecnologias então em surgimento davam aos governos a capacidade de manter, na prática, réplicas (ou representações) virtuais dos indivíduos em repositórios de informações, o que abriu horizontes inéditos à vigilância estatal e tornou possível o exercício do controle em proporções até então desconhecidas. Ademais, a expansão do emprego dos bancos de dados para as atividades comerciais criaria um campo novo de possibilidades para que agentes privados pudessem coletar, armazenar, consultar e compartilhar informações pessoais no interesse da exploração de atividades econômicas.

Nesse cenário, tornou-se necessário cogitar de uma resposta normativa capaz de limitar tais atividades, de forma que ocorressem de modo seguro e sustentável (Richards; Hartzog, 2020a, p. 1). Como ensina Schwartz (1999, p. 1658), atribui-se a Alan Westin o papel de protagonismo nas formulações teóricas, ainda no final da década de 1960, a respeito da tutela da privacidade por meio do controle dos fluxos informacionais[272], em uma perspectiva que atribuía ênfase ao exercício da autonomia individual:

> Em 1967, no início da era dos computadores *mainframe*, *Privacidade e Liberdade* de Alan F. Westin forneceu uma formulação inicial e influente da privacidade-controle. Westin definiu a privacidade da informação como a reivindicação de "indivíduos, grupos ou instituições de determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros". Para Westin, esse interesse era um elemento essencial na preservação da liberdade humana. (Tradução nossa)

Com efeito, na segunda metade do século XX, o exercício do controle individual, enquanto abordagem paradigmática da tutela da privacidade, desfrutou de grande prestígio. À época em que foi articulado, o paradigma do controle era capaz de oferecer uma tutela significativa à luz do *estado da arte* das tecnologias então existentes. Como bem destaca Hirsch (2019, p. 15), à época em que Alan Westin concebeu a "abordagem do controle, a maioria dos tratamentos de dados pessoais atendia essas condições. As empresas geralmente coletavam

---

[271] "A história das regras de proteção de dados começa com o advento dos computadores. [...] As tecnologias elétricas e eletrônicas começaram a transformar a sociedade, rompendo expectativas estabelecidas sobre vigilância, privacidade e poder governamental e corporativo. Acadêmicos, autores populares, revistas e programas de notícias se concentraram nas ameaças à privacidade causadas por novas tecnologias de espionagem e a criação de 'bancos de dados' governamentais e corporativos, tentando entender essas mudanças e pedindo por reformas legais." (Richards; Hartzog, 2020b, p. 1699)

[272] A construção teórica inicial, cujas bases foram lançadas pela obra de Alan Westin, é denominada por Solove e Hartzog (2024, p. 1025) de "Modelo de Controle Individual". Nas palavras dos autores: "O Modelo de Controle Individual visa a capacitar indivíduos e dar a eles controle sobre seus dados pessoais." (Tradução nossa)

dados pessoais [...] para propósitos específicos. Os indivíduos podiam fazer uma escolha substancial sobre permitir isso ou não" (Tradução nossa).

A literatura em geral refere à primeira experiência de adoção institucional do paradigma do controle ao mencionar relatório emitido pelo Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos da América em 1973. No documento, intitulado *Records, Computers and the Rights of Citizens*[273], reconhecia-se o aumento de preocupações a respeito da multiplicação de sistemas de registro digital e reforçava-se a importância de que os indivíduos tivessem "o direito de participar na decisão sobre o conteúdo do registro, e que divulgação e que uso será feito da informação identificável nele" (Solove, 2023, p. 980, tradução nossa).

O relatório, em consonância com as preocupações por ele destacadas, propunha um conjunto de seis princípios fundamentais relacionados ao tratamento justo de dados pessoais, a partir dos quais se deveria balizar as estratégias para a proteção da privacidade no contexto das novas tecnologias de armazenamento eletrônico (Richards; Hartzog, 2020b, p. 1700). Trata-se das já mencionadas FIPs, conjunto influente de postulados normativos no contexto das abordagens iniciais a respeito da proteção de dados pessoais na segunda metade do século XX. De acordo com as FIPs, caberia aos agentes de tratamento garantir aos indivíduos – dentre outros – os direitos de acesso, de obtenção de informações a respeito dos usos e finalidades do tratamento de dados pessoais, e de correção de informações.

Como leciona Bioni (2020, p. 113), a OCDE, dada a sua vocação de estabelecer diretrizes para a cooperação multilateral entre seus países-membros, revisou o conteúdo das FIPs ao expedir, já na década de 1980, importantes orientações (*guidelines*) a seus países-membros a respeito da tutela da privacidade, diante da evolução das tecnologias de tratamento de dados pessoais[274]. Com efeito, a OCDE estruturou suas *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[275] largamente inspirada no modelo normativo proposto pelas FIPs, a partir de definições e princípios relacionados à concessão de *controles* aos indivíduos sobre as suas próprias informações.

Nota-se, a partir desse contexto histórico, as razões pelas quais o modelo de proteção de dados pessoais estruturado sobre as FIPs – e, consequentemente, a noção de controle individual – gozou de notável (e disseminada) aceitação no contexto das proposições normativas

---

[273] "Registros, computadores e os direitos dos cidadãos", em tradução livre.

[274] "Com inspiração nas Fair Information Practices (FIPs) [...], o referido documento assentou as definições gerais, os princípios básicos e a cooperação internacional sobre o tema no bojo dos países membros da OCDE." (Mendes; Fonseca, 2020, p. 512). No mesmo sentido, cf. Cate, 2006, p. 348.

[275] "Orientações sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais", em tradução livre.

internacionais a respeito da proteção de dados pessoais[276]. Como notam Richards e Hartzog (2020b, p. 1701), a partir da edição das *guidelines* pela OCDE, as FIPs "tornaram-se as pedras angulares para leis de proteção de dados ao redor do mundo" (tradução nossa). Da mesma forma, Mendes e Bioni (2019, p. 165) destacam:

> Ao longo do desenvolvimento da temática da proteção de dados pessoais, estabeleceu-se, por meio de instrumentos internacionais e transnacionais, um consenso em torno de um quadro básico de princípios que devem nortear a atividade de tratamento de dados. Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder de controle ao indivíduo sobre o fluxo de seus dados.

O exercício do controle individual enquanto elemento fundante do (então) novo regime de proteção de dados pessoais (traduzido, como lembra Rodotà, pela ideia de *control of information about oneself*[277]) estruturava-se sobre a noção fundamental de que **o exercício da autonomia individual conduziria a um equilíbrio de poderes entre os agentes de tratamento e os cidadãos**. Hartzog (2017, p. 953), a propósito, acertadamente observa que os regimes de proteção de dados inspirados nas FIPs "eram relativamente bem equipados para a primeira onda de computação pessoal" (tradução nossa).

O paradigma do controle, tanto à época de sua formulação inicial quanto atualmente, corresponde ao anseio de endereçar assimetrias de poderes entre titulares de dados pessoais e empresas ou governos por meio da criação de direitos inerentes à titularidade. Em tal perspectiva, a autonomia é compreendida, numa visão eminentemente liberal, como o próprio poder de decisão a ser exercido pelo indivíduo sobre seus dados pessoais (Schwartz, 1999, p. 1658), de sorte a equalizar as forças em disputa na arena da proteção de dados pessoais. De fato, é compreensível (e mesmo intuitiva[278]) a busca pela solução do problema a partir da criação de direitos e por meio da atribuição de controle (e, consequentemente, de poder) aos indivíduos. Como comenta Hartzog (2018, p. 429),

> O controle sobre informações pessoais é atraente isoladamente. Quem não gostaria de ter mais poder sobre coisas que afetam nossas vidas? Mas com esse poder, muitas vezes, vem uma obrigação prática. Se você não exercer esse controle, estará em risco. As empresas podem considerar sua inação como aquiescência. (Tradução nossa)

---

[276] "Não há dúvidas de que as *guidelines* foram bem-sucedidas. [...]. Existem agora mais de 100 países com leis de privacidade de dados e a maioria delas é construída sobre a maioria ou todas as práticas mínimas de informação justa especificadas pela OCDE." (Hartzog, 2017, p. 958, tradução nossa)

[277] "O sucesso das definições de privacidade baseadas no princípio do 'control of information about oneself' se explica justamente pelo fato de que elas colocavam em evidência a novidade representada pela atribuição aos interessados de um poder autônomo de controle." (Rodotà, 2008, p. 46)

[278] "Os indivíduos são frequentemente impotentes e vulneráveis em um mundo onde vastas quantidades de seus dados pessoais são coletadas e usadas de maneiras que afetam suas vidas. Portanto, parece intuitivo tentar dar aos indivíduos mais controle sobre seus dados pessoais com direitos de privacidade." (Solove, 2023, p. 993, tradução nossa)

A propósito, o paradigma do controle também manifesta íntima relação com o conceito de autodeterminação informativa, gestado na jurisprudência da Corte Constitucional Alemã, a que nos referimos no Capítulo 1. Afinal, a autodeterminação informativa decorre justamente da ideia de atribuir ao indivíduo o poder de interferir e de fazer escolhas a respeito de aspectos do tratamento de seus dados pessoais[279]. De acordo com Koops (2014, p. 3), trata-se da noção segundo a qual

> as pessoas devem poder exercer controle sobre o que acontece com seus dados pessoais; afinal, são seus dados. Isso implica, primeiro, que o consentimento livre e informado dos indivíduos é um fundamento importante para legitimar o tratamento de dados e, segundo, que os indivíduos têm vários direitos para exercer controle sobre os dados, como direitos de correção ou eliminação. (Tradução nossa)

Embora o desenvolvimento rápido e intenso das tecnologias de informação e comunicação, da década de 80 até o presente, tenha evidenciado a necessidade de adequação dos regimes de proteção de dados pessoais, para que endereçassem desafios contemporâneos (como as decisões tomadas a partir do tratamento automatizado de dados pessoais), o paradigma do controle manteve-se prevalente. Vale destacar, a propósito, o Considerando n. 7 do RGPD, segundo o qual "[a]s pessoas singulares deverão poder **controlar** a utilização que é feita dos seus dados pessoais" (grifo nosso).

Nessa mesma esteira, como vimos, a LGPD denominou as pessoas às quais se referem os dados pessoais de *titulares*, de sorte a reforçar a noção de controle sobre as informações que lhes digam respeito. A propósito, o texto de seu art. 17 é enfático: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei".

Muito embora a sua relevância no contexto da afirmação do direito autônomo à proteção de dados pessoais não deva ser menosprezada, as FIPs foram concebidas em um contexto completamente diverso do que ora vivenciamos, em que inúmeras atividades cotidianas passaram a ser mediadas por plataformas digitais e, portanto, transformadas em dados pessoais. Na acertada ponderação de Richards e Hartzog (2020a, p. 2), "a abordagem das FIPs nunca considerou que os futuros consumidores e cidadãos poderiam criar tantos dados e ter tantas

[279] Nesse mesmo sentido, Hartmann, Patz e Piaia (2021, p. 161) expressamente definem o direito à autodeterminação informativa como a "faculdade que toda pessoa tem de exercer, de algum modo, controle sobre seus dados pessoais, garantindo-lhe, em determinadas circunstâncias, decidir se a informação pode ser objeto de tratamento (coleta, uso, transferência) por terceiros, bem como acessar bancos de dados para exigir correção ou cancelamento de informações".

contas comerciais e governamentais que a autodeterminação informacional poderia se tornar impossível". (Tradução nossa)

Efetivamente, o controle individual enquanto elemento central dos regimes de proteção de dados pessoais mostrava-se consentâneo com uma época em que a computação não era sobremaneira disseminada como atualmente; além disso, àquela época nem sequer se poderia imaginar[280], salvo nas obras de ficção científica, a formação de um modelo econômico completamente estruturado sobre a extração massiva de dados pessoais, a ensejar a concepção de técnicas sofisticadas de obtenção de quantidades cada vez maiores de informações sobre as pessoas humanas. Segundo Hartzog (2017, p. 966):

> As FIPs foram desenvolvidas antes mesmo que a maioria das pessoas sequer imaginasse ter um computador pessoal. Elas foram projetadas para lidar com os problemas que resultavam da coleta e conversão de informações em bancos de dados armazenáveis e pesquisáveis. A realidade de todos terem um supercomputador, um dispositivo de vigilância e um beacon em seus bolsos com um universo digital acumulado de cerca de 44 trilhões de gigabytes (!) ainda estava muito distante. Mídias sociais, biometria, drones e robôs que interagiam regularmente com humanos ainda não tinham sido inventados. No entanto, aqui estamos nós, com um novo conjunto de problemas que os FIPs abordam apenas parcialmente. (Tradução nossa)

A abordagem pautada no controle, em teoria, protege e reforça a autonomia individual. Lembremo-nos, a propósito, da estreita relação entre autonomia e liberdade, explorada no Capítulo 2, e de como essa interação serviria aos propósitos de conter a vigilância e delimitar um âmbito de proteção da vida privada – consentâneo com as próprias escolhas individuais[281] – sobre o qual não seriam admitidas incursões de empresas ou governos.

Entretanto, tal perspectiva deve ser repensada à luz do contexto do capitalismo de vigilância, em que são extremamente limitadas as possibilidades de exercício de um controle efetivo sobre os dados pessoais. Mais do que isso, como lembra Hartzog (2018, p. 426), empresas que estruturam seus modelos de negócio sobre a extração massiva de tais informações têm incentivos para fazer com que os usuários de suas plataformas e sistemas digitais acreditem ter mais controle do que eles realmente têm.

---

[280] Richards e Hartzog assim apresentam o contexto do tratamento de dados pessoais nas décadas de 1960 e 1970: "Dados eletrônicos eram relativamente caros, escassos e administráveis. Os computadores ainda não tinham se tornado parte de nossas vidas diárias e a internet ainda não tinha sido democratizada. Como o processamento de dados parecia revolucionário, os legisladores abraçaram a justiça como uma meta que poderia equilibrar a privacidade e o bem-estar das pessoas com inovação e eficiência." (Richards; Hartzog, 2020b, p. 1733, tradução nossa)

[281] Como observa Rodotá (2008, p. 47), "como a inovação tecnológica progressivamente pôs em funcionamento instrumentos de comunicação de mão dupla, também a inovação institucional pode tornar efetivos sistemas de controle em mão dupla, que partam da coletividade em direção aos bancos de dados e não somente do alto em direção ao baixo".

Assim, se os desafios ao exercício do controle (e, portanto, da autodeterminação informativa) já não eram grandes o bastante à época em que o conceito foi cunhado, tornam-se cada vez maiores com as crescentes quantidades de dados coletados (dataficação da vida), com a sofisticação das técnicas de manipulação (padrões obscuros) e com o uso progressivamente mais disseminado e corrente de sistemas de inteligência artificial. Vale transcrever, no ponto, a precisa lição de Hartzog (2017, p. 953):

> [...] tecnologias automatizadas e quantidades exponencialmente maiores de dados levaram os princípios das FIPs, como minimização de dados, transparência, escolha e acesso ao limite. Avanços em robótica, genética, biometria e tomada de decisão algorítmica estão desafiando a ideia de que regras destinadas a garantir agregação justa de informações pessoais em bancos de dados são suficientes. O controle sobre as informações em bancos de dados não é mais nem a metade disso. (Tradução nossa)

A LGPD, como exposto, acolheu amplamente o controle enquanto resposta fundamental à assimetria de poderes que, à época de sua entrada em vigor, já se mostrava muito mais grave do que aquela causada pelas tecnologias de coleta e armazenamento existentes na década de 1970. Nesse sentido, aliás, uma das competências da ANPD é precisamente a de "estimular a adoção de padrões para serviços e produtos que facilitem *o exercício de controle dos titulares sobre seus dados pessoais*, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis" (art. 55-J, VIII).

E é nesse mesmo diapasão – orientado pelo paradigma do controle – que vem se formando a interpretação do órgão regulador a respeito do regime jurídico de proteção de dados pessoais. Como se verifica, por exemplo, da Nota Técnica 175/2023/CGF/ANPD, a Autoridade Nacional declara que "a autodeterminação informativa é fundamento previsto da LGPD e tem como objetivo assegurar certo controle do cidadão sobre informações que se referem a ele". Da mesma forma, em seu Guia Orientativo sobre *Cookies*, a Autoridade sugere, como solução de conformidade regulatória, a adoção de *banners* pelos agentes de tratamento, na medida em que tais técnicas forneceriam "ferramentas para que o usuário **possa ter maior controle** sobre o tratamento, como, por exemplo, permitindo que ele consinta ou não com determinados tipos de *cookies*" (ANPD, 2023, p. 28, grifo nosso).

Em suma, embora consentâneo com as circunstâncias históricas que ensejaram a sua concepção, como saída para a redução das assimetrias de poder diante das ameaças (à época) inéditas, representadas pelos bancos de dados, o paradigma do controle individual, hoje, encontra-se em crise[282]. É o que discutiremos no tópico seguinte.

---

[282] "O paradigma do controle funcionou relativamente bem para as atividades de coleta e processamento de informações para as quais foi inicialmente projetado na década de 1970. No entanto, como aconteceu com relação

3.3 Fragilidades da proteção de dados pessoais sob o paradigma do controle

O paradigma do controle se sustenta sobre uma equivocada compreensão de que o oferecimento de informações (ainda que claras, acessíveis e precisas) aos titulares de dados pessoais viabilizaria a tomada de decisão racional e *autônoma*, efetivando-se o princípio da autodeterminação informativa e, consequentemente, a tutela da privacidade, da liberdade e do livre desenvolvimento da personalidade[283]. Na linha de tal paradigma, a publicação de políticas de privacidade, a abertura de canais de exercício de direitos (como os de acesso e portabilidade) e a inserção de cláusulas contratuais destacadas a respeito do consentimento com o tratamento de dados pessoais são materializações do controle individual no regime jurídico de proteção de dados pessoais estabelecido pela LGPD.

Ademais, há uma lógica procedimental subjacente à LGPD, a que já nos referimos, pautada em um foco primordial no conceito de dado pessoal e nas demonstrações formais de cumprimento dos comandos legais. Esse enfoque eminentemente procedimental de nosso regime jurídico de proteção de dados pessoais enseja um perigoso *descolamento* entre a relação jurídica informacional e a relação jurídica substancial, comprometendo gravemente o potencial protetivo da LGPD.

Afinal, o foco na adequação formal das atividades de tratamento desvia o olhar do regulador daquilo que realmente importa: as assimetrias de poder e de informação, que ensejam graves perigos à autonomia individual, à privacidade, à liberdade, entre outros bens jurídicos de igual estatura. Ora, a proteção de dados pessoais importa não para garantir-se a mera conformação procedimental da relação jurídica informacional – como se ela fosse independente da relação substancial –, mas, sim, para que, ao reforçar a tutela da autonomia e da privacidade, contenha-se o poder sem precedentes que vem sendo acumulado por governos e por empresas cujo negócio principal está na extração massiva de dados pessoais a partir de incisivas e reiteradas invasões à privacidade individual. Importante, no ponto, recorrer ao magistério de Solove (2021, p. 38):

> A privacidade é um limite ao poder do governo e das empresas. Quando se trata de dados pessoais, conhecimento é poder. Dados pessoais estão envolvidos em muitas decisões muito importantes sobre a vida das pessoas. Dados pessoais podem ser facilmente usados para afetar reputações, moldar a

aos alimentos, medicamentos, moradia e tantas outras áreas, condições sociais cada vez mais complexas estão tornando impossível para os indivíduos fazerem escolhas significativas sobre a coleta e o uso de suas informações pessoais." (Hirsch, 2019, p. 7, tradução nossa)

[283] "Para que haja um livre desenvolvimento da personalidade, existe a necessidade de que o indivíduo crie suas próprias convicções, sem interferências alheias, sem que haja uma forma de repreensão social ou até mesmo estatal; que desenvolva suas ideias, seus modos de agir e interagir socialmente, os gostos, os credos dentre outras características que formam a personalidade do indivíduo." (Tateoki, 2021, p. 65)

> tomada de decisões e influenciar o comportamento. Nas mãos erradas, dados pessoais podem ser usados para causar grandes danos às pessoas. (Tradução nossa)

Ainda nesse particular, como bem destacam Richards e Hartzog (2020a, p. 4), é de se ressaltar que o tratamento *legítimo* – assim entendido aquele realizado de acordo com as balizas procedimentais – *não é* "em si mesmo, uma forma de mitigar o poder" (tradução nossa). Vale lembrar, ademais, que o *poder informacional* é volátil, de sorte que pode se transformar facilmente (de poder econômico a poder político; de poder político a poder bélico, e assim por diante[284]). Nessa perspectiva, reforça-se o papel das normas de proteção de dados pessoais, na medida em que, contendo efetivamente o aumento do poder informacional (e não apenas garantindo que seja exercido dentro de algumas balizas), podem evitar repercussões ainda mais graves em outros âmbitos da vida coletiva.

O paradigma do controle falha em considerar, ademais, que o próprio controle exercido pelos titulares ocorre dentro de um contexto mais amplo de poder estrutural. Como veremos a seguir, a crise do paradigma do controle se revela diante de um contexto marcado por relações cada vez mais *indispensáveis* e *assimétricas* com empresas que monitoram e controlam o que os titulares de dados pessoais veem e fazem, e que implementam sofisticadas técnicas de manipulação, seja para interferir cada vez mais eficazmente em seu comportamento, seja para prever padrões futuros[285], comercializando a própria *certeza* sobre interesses e necessidades individuais a parceiros comerciais ou governos.

Em síntese, a crise do paradigma do controle pode ser compreendida a partir de dois elementos essenciais: as dificuldades inerentes à efetivação do controle individual em um mundo hiperconectado (daí a se falar em *ilusão do controle*), notadamente o otimismo exacerbado[286] do legislador com relação às aptidões individuais para o exercício autônomo do controle (isto é, a crença na *racionalidade do titular*); e o modelo eminentemente procedimental

---

[284] "Existem diferentes tipos de poder: econômico, político, militar e assim por diante. Mas o poder pode ser entendido como uma analogia à energia: ele pode se transformar de um tipo em outro. Uma empresa com poder econômico pode valer-se de dinheiro pra ganhar poder político através de lobby, por exemplo. Uma pessoa politicamente poderosa pode valer-se de poder para ganhar dinheiro através da troca de favores com empresas privadas." (Véliz, 2021, p. 81)

[285] "A abordagem do controle não pode proteger as pessoas das ameaças que a análise preditiva representa. Ela não pode capacitar as pessoas a proteger sua privacidade porque, quando concordam em compartilhar dados, elas não sabem o que estão realmente revelando. Ela não pode permitir que as pessoas se protejam contra manipulação porque elas frequentemente não sabem quando estão revelando suas vulnerabilidades. Ela não pode proteger contra vieses porque, embora as empresas possam fornecer avisos de que usarão dados pessoais para fins analíticos, elas não dão acesso aos dados de treinamento ou ao algoritmo e, mesmo que o fizessem, a maioria das pessoas não saberia como avaliá-los." (Hirsch, 2019, p. 24, tradução nossa)

[286] Segundo Mendes e Fonseca (2020, p. 514), caso o titular "esteja munido de amplo conhecimento acerca do que é feito com seus dados pessoais, poderá sopesar os custos envolvidos para sua personalidade e contrapô-los em face dos benefícios trazidos, por exemplo, pela utilização de um serviço online".

sobre o qual se estrutura a LGPD, exigindo-se menos a redução de assimetrias de poder e extração massiva de dados pessoais do que a compatibilidade entre a relação jurídica informacional e os requisitos formais estabelecidos pela norma.

3.3.1 A ilusão do controle e o mito da racionalidade do titular

"Li e estou de acordo". "Sua privacidade é algo importante para nós". "Aceitar todos os *cookies*". Essas e outras expressões compõem a gramática contemporânea da proteção de dados pessoais, moldada pelo advento das plataformas digitais, disseminadas como mecanismos de mediação de inúmeras atividades do cotidiano, que há muito não se limitam à esfera comercial. O surgimento desse novo vocabulário está diretamente associado à afirmação do paradigma do controle como vetor epistemológico do regime jurídico de proteção de dados pessoais. Com a LGPD, nasce a necessidade de, por exemplo, *informar* os indivíduos por meio de políticas de privacidade, o que é um passo importante para a *legitimação* do tratamento de dados pessoais, independentemente do uso da base legal do consentimento.

Como vimos, o paradigma do controle mostrava-se apropriado a um contexto tecnológico e social existente há mais de meio século. Se, no contexto europeu – em que houve, de fato, um processo histórico de afirmação e de sedimentação do tema da proteção de dados pessoais no âmbito *social* – esse modo limitado de tutela da privacidade já enfrenta desafios, no delicado cenário brasileiro não é demasiado afirmar que a tutela da autonomia e da privacidade por meio da atribuição de controles individuais é, em verdade, uma missão fadada ao fracasso.

Nada obstante, a LGPD deve ser cumprida. Empresas e órgãos públicos estão obrigados a criar canais de comunicação, nomear encarregados, redigir políticas de privacidade claras e acessíveis, obter consentimentos livres, informados e inequívocos dos titulares de dados pessoais (quando for o caso), produzir relatórios sobre as operações de tratamento e conduzir testes de balanceamento antes de se utilizarem da hipótese legal do legítimo interesse. Titulares, por outro lado, podem requerer a anonimização de seus dados pessoais tratados em desconformidade com a LGPD ou obter informações sobre a "possibilidade de não fornecer consentimento e sobre as consequências da negativa" (nos termos do art. 18, VIII, da LGPD), direitos que – dentre outros – denotam o *controle* que podem exercer sobre seus próprios dados pessoais.

Esse controle que a LGPD busca atribuir aos titulares de dados pessoais é, em larga medida, *idealizado*. E assim o é porque o exercício do controle significativo, na atualidade, é

simplesmente impraticável. Isso se dá por quatro razões fundamentais, as quais passaremos a explorar nesse subtópico.

Em primeiro lugar, não consentir significa, essencialmente, não ter acesso às plataformas digitais (*take-it-or-leave-it*) que viabilizam não apenas o acesso à informação e a participação na dinâmica social no ciberespaço, mas também o acesso a bens e serviços de elevada importância para a vida cotidiana, tendo-se estabelecido verdadeira relação de dependência das plataformas digitais, sobre as quais discorremos no Capítulo 1. Esse *trade-off* entre dados pessoais e acesso plataformas (pretensamente gratuitas) deflui do usual modelo de negócios no mundo digital, em que dados pessoais são coletados, utilizados ou mesmo vendidos (Solove, 2023, p. 36), e no qual titulares de dados pessoais não têm qualquer poder de barganha efetivo[287].

Ora, se o uso de plataformas digitais é indispensável – ou, visto de outro modo, se a recusa ao tratamento de dados pessoais representa uma *renúncia brutal*, na expressão de Doneda (2021, p. 312)[288] – à utilização "de serviço/produto, que, muitas vezes, sob a perspectiva do indivíduo, é essencial para a sua sociabilidade ou acesso à informação na era digital" (Mendes; Fonseca, 2020, p. 516), o controle é, de fato, meramente ilusório. Confira-se, a respeito, a lição de Cate (2006, p. 366):

> Requerimentos de informação e consentimento geralmente criam a ilusão, mas não a realidade, de uma escolha significativa do consumidor. [...] se o consentimento for necessário como condição para abrir uma conta ou obter um serviço, uma alta taxa de resposta sempre pode ser obtida. Um exemplo útil são os termos de licença que os usuários de computador encontram ao baixar ou instalar um *software*. (Tradução nossa)

Em segundo lugar, avisos ou políticas de privacidade – elementos indispensáveis à obtenção válida do consentimento – *não são lidos*[289], e, mesmo se o fossem, demandariam, no mínimo, nivelamento conceitual elementar a respeito da proteção de dados pessoais, o que é

---

[287] "[...] como aponta Pasquale, não deixa de ser uma ficção achar que os consumidores podem e irão barganhar por privacidade ou simplesmente deixarem de contratar quando entenderem que seus direitos não estão sendo assegurados (o chamado *opt out*). Pelo contrário, em contextos de ausência de rivalidade e em que a aceitação da política de privacidade é condição *sine qua non* para o acesso ao serviço [...], a legitimidade do consentimento sempre será discutível, mesmo que ele tenha sido informado." (Frazão, 2019c, p. 124)

[288] "O confronto com situações reais revela que, em tais situações, a alternativa à não revelação dos dados pessoais pelo seu titular costuma ser uma – por vezes, brutal – renúncia a determinados bens ou serviços. A disparidade de meios e de poder entre a pessoa de quem é demandado o consentimento para utilização dos dados pessoais em contemplação da realização de um contrato e aquele que os pede faz com que a verdadeira opção que lhe reste seja, tantas vezes, a de 'tudo ou nada', 'pegar ou largar'." (Doneda, 2021, p. 312)

[289] "[...] estudos têm indicado que muitos usuários não leem esses termos e, quando leem, acabam por não os entender ou levam um tempo significativo para tanto [...]. Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja a de não desfrutar importantes produtos e serviços online." (Mendes; Fonseca, 2020, p. 508) No mesmo sentido, cf. Koops, 2014, p. 3.

difícil se imaginar em um país em que 3 a cada 4 cidadãos não têm habilidades digitais básicas. Na precisa observação de Waldman (2021, p. 52),

> avisos de privacidade são extremamente difíceis de analisar, escritos em linguagem que nem mesmo especialistas conseguem entender. Avisos devem nos dar as informações de que precisamos para tomar decisões informadas. Mas acadêmicos mostraram que levaria quase 244 horas por ano para ler as políticas de privacidade dos sites que visitamos apenas uma vez. Até mesmo especialistas têm dificuldade para entendê-las. Mesmo se pudéssemos encontrar alguma maneira de tornar os avisos de privacidade perfeitamente compreensíveis para não especialistas, as assimetrias estruturais entre a indústria da informação e os usuários permaneceriam. (Tradução nossa)

O modelo *notice-and-choice*[290], presente na tradição norte-americana[291], foi estruturado sobre a compreensão de uma racionalidade cartesiana dos indivíduos, que poderiam, se não concordassem com os termos das políticas de privacidade, simplesmente *escolher* recusar-se à coleta de seus dados pessoais (e, evidentemente, não utilizar o serviço, como consequência da recusa).

Já a experiência europeia[292], por outro lado, busca materializar o controle individual sobre os fluxos informacionais a partir do uso da hipótese legal do consentimento. O consentimento manifesta certo avanço com relação ao modelo *notice-and-choice*, na medida em que a regulamentação estabelecida pelo RGPD requer a obtenção de uma anuência *qualificada*, que apenas será considerada válida caso atenda a requisitos que assegurem que o consentimento manifeste autêntica expressão da autonomia individual. Por isso, como na LGPD, deve ser livre, informado e inequívoco.

Nada obstante, na hipercomplexidade inerente à sociedade da informação, a doutrina vem criticando as reais aptidões e potencialidades da manifestação do consentimento individual como mecanismo de proteção dos titulares de dados pessoais. Afinal, como lembram Richards e Hartzog (2019, p. 1484), "[s]omos muito otimistas; confiamos muito no passado e na experiência vivida em vez de dados confiáveis e generalizáveis; descontamos muito os custos

---

[290] Na crítica precisa de Richards e Hartzog (2019, p. 1471): "'aviso' pode significar uma descrição vaga, mas não falsa, de práticas de dados enterradas profundamente em uma longa política de privacidade e 'escolha' pode significar nada mais do que a escolha de usar o serviço em primeiro lugar (Apple, Android ou nenhum telefone, por exemplo)." (Tradução nossa)

[291] "Nos Estados Unidos, muitas leis buscaram implementar o Modelo de Controle Individual pela abordagem de aviso e escolha, onde empresas postavam avisos sobre suas práticas de privacidade e indivíduos podiam optar por não participar se se opusessem. Claro, as pessoas não leem avisos de privacidade e não têm ideia do que está sendo feito com seus dados. Ninguém realmente levou o aviso e escolha a sério; ele tem sido completa e continuamente criticada por comentaristas." (Solove; Hartzog, 2024, p. 1025, tradução nossa)

[292] "O RGPD exige um consentimento de alta qualidade, em paridade com decisões importantes da vida, como consentimento para tratamento médico. Em muitos contextos, os fardos que o RGPD coloca no consentimento tornam o consentimento impossível como mecanismo para tornar legítimos os usos de dados. Além disso, muitas regras no RGPD não são renunciáveis e continuam a se aplicar depois que alguém consentiu com o uso de dados." (Hoofnagle; der Sloot; Borgesius, 2019, p. 68, tradução nossa)

futuros; e achamos que a maneira como as coisas estão agora permanecerá assim" (Tradução nossa).

Nessa perspectiva, o controle individual – materializado pelo consentimento livre, inequívoco e informado com termos e condições de uso, ou com políticas de privacidade – pode até mesmo intensificar os agravos à autonomia e à privacidade. Afinal, pode representar a legitimação de atividades de tratamento que têm por finalidade a acumulação de poder, conhecimento e controle indireto sobre os titulares. Noutros termos, ao invés de proteger, o paradigma do controle pode tornar os indivíduos ainda menos protegidos, alocando sobre eles o ônus de consentir e de exercer proativamente seus direitos:

> Temos que fazer nossas escolhas de privacidade, site por site, aplicativo por aplicativo, às vezes muitas escolhas por plataforma. Somos responsáveis por ler as políticas de privacidade. Temos a tarefa de encontrar plataformas alternativas – se elas existirem – quando nos opomos às práticas de coleta de dados. Temos que navegar no processo de *opt-out* de uma plataforma. Direitos de acesso, correção e exclusão exigem trabalho de privacidade adicional, sem mencionar a capacidade de navegar no processo de aprovação, verificação e recurso contra uma empresa se eles rejeitarem nossas solicitações. E temos que fazer isso dentro de um ambiente projetado para extrair nossas informações. De fato, o ônus de proteger nossa privacidade está quase inteiramente sobre nossos ombros. (Waldman, 2021, p. 54, tradução nossa)

É diante desse problemático cenário que Solove e Hartzog (2024, p. 1024) afirmam que, embora os indivíduos estejam fragilizados, a resposta mais adequada não é empoderá-los com controle sobre seus dados. Ao invés de proteger os titulares de usos abusivos de seus dados pessoais, o emprego da base legal do consentimento, ao menos no contexto das plataformas digitais, se revela mais como uma espécie de *atalho regulatório*, na medida em que se constitui em um mecanismo pretensamente mais simples de se demonstrar a legitimidade do tratamento de dados pessoais.

Em terceiro lugar, o paradigma do controle não responde suficientemente às graves interferências estruturais, presentes no *design* das plataformas digitais, capazes de *condicionar* ou mesmo *fabricar* o próprio consentimento por meio da manipulação[293]. Empresas que exploram atividades econômicas a partir de plataformas digitais detêm completo domínio de sua arquitetura, além de concentrarem um manancial de informações a respeito dos titulares de dados pessoais, a partir das quais podem atribuir diferentes formas às interfaces digitais, moldadas de acordo com as vulnerabilidades e vieses cognitivos dos usuários.

---

[293] "As FIPs têm pouco a dizer sobre nossa suscetibilidade à manipulação. Interfaces de usuário podem ser projetadas para extrair nosso 'consentimento' ou para nos encorajar a postar de maneiras que nem percebemos." (Hartzog, 2017, p. 969)

Nesse sentido, truques de *design* de interface, técnicas de oferecimento de conteúdo que geram compulsão pelo uso do *smartphone*, inserção de padrões obscuros feitos para causar a *ilusão* do exercício de um controle significativo sobre os dados pessoais, exploração de vieses cognitivos a partir do perfilamento, dentre outros fatores, são componentes cuja existência não pode ser desprezada diante do objetivo de se proteger a privacidade e a autonomia no mundo digital. Todavia, os direitos relacionados ao controle individual pouco protegem os indivíduos contra esses riscos.

Aliás, a própria forma como políticas de privacidade são redigidas ou apresentadas pode servir ao propósito de manipular[294]. Mesmo que sejam viabilizados os controles para exercício de direitos exigidos pela LGPD, essas interfaces resultam, inevitavelmente, de escolhas feitas pelos arquitetos das plataformas digitais. Como bem observam Richards e Hartzog (2020b, p. 1734),

> Engenheiros projetam suas tecnologias para produzir resultados específicos. As escolhas humanas são limitadas pelo design das ferramentas que usam. As empresas decidem o tipo de caixas que as pessoas podem selecionar, botões que pressionam, os interruptores que ativam e desativam e outras configurações em que podem mexer. Ao apresentar escolhas limitadas como "mais opções" para os usuários, as empresas podem incutir nos usuários uma falsa sensação de controle, obscurecendo quem realmente está no controle da interação. (Tradução nossa)

Diante desse contexto é que Hartzog (2018, p. 426) defende, categoricamente, que o controle é *ilusório*[295]. Nada obstante, busca-se resolver o problema de *mais violações à privacidade* com *mais controle*[296]. Assim, se, na década de 1970, sequer se cogitava de decisões decorrentes do tratamento automatizado de dados pessoais, hoje a questão foi remediada com *controle* sobre o algoritmo utilizado para se decidir em um ou outro sentido (nesse sentido é o art. 20 da LGPD, que estabelece o direito à *revisão* de tais decisões, e o direito a obter informações sobre os critérios e procedimentos que as orientam, *se solicitadas*).

---

[294] "Muitas dessas leis exigem que as políticas de privacidade sejam suficientemente 'visíveis' para os usuários, e ainda assim as políticas de privacidade hoje são bagunças confusas de jargões jurídicos e vagas platitudes de *marketing* que [...] na verdade não informam. No entanto, elas nos fazem pensar nelas como compromissos juridicamente vinculativos, e são projetadas e apresentadas a nós para manipular intencionalmente nosso comportamento." (Waldman, 2021, p. 132, tradução nossa)

[295] No mesmo sentido é o entendimento de Cofone (2024, p. 16): "A economia da informação destrói a ideia de que as pessoas têm escolhas sobre o que acontece com suas informações. Além do objetivo insuficiente, mas não cumprido, de informar as pessoas como o principal meio de proteção, as pessoas raramente têm escolha genuína para fazer qualquer coisa além de concordar com elas." (Tradução nossa)

[296] "Direitos relacionados à privacidade não podem resolver o problema da fragilidade dos titulares. A capacidade dos indivíduos de exercer controle sobre seus dados pessoais é bastante limitada; há um teto para o controle individual. Os direitos podem dar às pessoas uma pequena quantidade de poder em algumas instâncias isoladas, mas esse poder é muito fragmentado e fortuito para ter um impacto significativo na proteção da privacidade." (Solove, 2023, p. 978, tradução nossa)

Em quarto lugar, além de terem atenção limitada – o que leva a doutrina a cogitar, com acerto, de uma *fadiga do consentimento*[297] num cenário em que *todas* as políticas de privacidade de plataformas digitais precisam ser lidas, por mais simplificadas que sejam, e no qual todas as plataformas precisem requerer[298], a todo o tempo, novos consentimentos para novas atividades de tratamento (como o uso de *cookies*) –, os indivíduos, ao contrário do que pressupõe o legislador, nem sempre tomam decisões racionais, como vimos no Capítulo 2. O paradigma do controle, a propósito, não endereça os *custos* envolvidos no exercício do controle individual. Segundo McDonald e Cranor (2008, p. 546),

> As políticas de privacidade deveriam ajudar a reduzir assimetrias de informação porque as empresas compartilham informações com seus clientes. No entanto, pesquisadores também observam que se o custo para ler as políticas de privacidade for muito alto, é improvável que as pessoas leiam as políticas. O tempo é um custo potencial, e o tempo necessário para ler as políticas pode ser uma barreira séria. Essa abordagem pressupõe que atores racionais realizem análises pessoais de custo-benefício, pelo menos em um nível implícito, para tomar decisões individuais de ler ou pular as políticas de privacidade. (Tradução nossa)

Além de nem sempre fazerem escolhas racionais e não terem as informações e elementos necessários a uma tomada de decisão significativa sobre o controle de seus dados (afinal, nem mesmo os programadores dos algoritmos sabem que usos podem ser feitos dos dados pessoais em futuro próximo ou distante[299]), os indivíduos, voluntariamente, instados pelo anseio de se integrar às tendências a que aderiu a coletividade já inserida no ambiente digital, acolhem, ávidos, tecnologias cada vez mais invasivas e prejudiciais à sua própria privacidade. Vê-se, nesse sentido, as dificuldades existentes em balancear benefícios imediatos e prejuízos futuros[300] na avaliação sobre o consentimento, especialmente mais grave em se tratando de crianças e adolescentes.

---

[297] "E como se não fosse difícil o bastante ler, analisar e integrar os avisos de, digamos, os cinquenta sites que visitamos em um dia, há outro problema além da fadiga da decisão. Existem centenas de sites que nunca vemos que nos rastreiam, monitoram nosso comportamento de navegação e compartilham nossas informações com outros. Essas plataformas podem ter postado políticas de privacidade em algum lugar, mas não podemos procurar por algo que não sabemos que está lá." (Waldman, 2021, p. 53, tradução nossa)

[298] "A partir do momento em que as pessoas inicializam um dispositivo, elas são presenteadas com 'controle' sobre as informações na forma de políticas de privacidade, termos de uso e banners em pop-up para cada site ou aplicativo que você visita ou usa. O ataque incessante é o suficiente para fazer os olhos de qualquer um ignorarem e clicarem em qualquer coisa que nos seja apresentada, apenas para que possamos finalmente usar o serviço." (Hartzog, 2017, p. 975, tradução nossa)

[299] "[...] informações pessoais são inferidas por agregação de dados; isto é, compilando diferentes tipos de informações fornecidas pelo titular dos dados, talvez para diferentes empresas, em diferentes momentos. Essas informações são subprotegidas por regras de propriedade. Isso ocorre porque os riscos de agregação são impossíveis de estimar, pois os efeitos de escala tornam a soma das divulgações desigual às partes constituintes das divulgações." (Cofone, 2021, p. 529, tradução nossa)

[300] "[...] seja pela escala em que a informação é processada, seja pela enorme capacidade de agregação da informação pelas novas tecnologias, é improvável que o indivíduo, no momento da coleta, gerencie plenamente algo que ocorrerá no futuro e que envolve inúmeras incertezas acerca de como todas as informações e dados

De fato, não apenas o *mito da* racionalidade (ou soberania[301]) do titular de dados pessoais, como também o crescente uso de técnicas de manipulação nos ambientes digitais – os quais são construídos e controlados pelos agentes econômicos que exploram o uso dos dados pessoais – demonstra que não se pode cogitar da capacidade plena dos indivíduos para tomar decisões efetivamente *livres* e *informadas* a respeito do tratamento de seus dados pessoais. Ao contrário, como afirmam Tepedino e Teffé (2020, p. 95), "ao invés de realmente concordar com o uso dos próprios dados, o que se verifica na prática é a obediência do titular à vontade das empresas, o que facilita práticas de controle e de uso indiscriminado de dados pessoais".

3.3.2 O "teatro da privacidade": a natureza procedimental e o desvirtuamento epistemológico do regime jurídico da proteção de dados pessoais

Tal como o regulamento europeu, a LGPD focaliza e estrutura seu sistema protetivo ao redor do conceito fundamental de dado pessoal[302]. Tamanha é a importância do dado pessoal para a incidência do regime jurídico de proteção de dados que a sua qualificação tem o condão de alterar a intensidade da proteção conferida a seus titulares, aumentando-a (como ocorre, por exemplo, com os dados pessoais *sensíveis*) ou mesmo afastando-a (tal como se dá no caso dos dados pessoais *anonimizados* ou utilizados para certas finalidades, como a jornalística ou artística – art. 4º, II, "a", da LGPD).

Para além disso, o tratamento legítimo de dados pessoais se revela por sua adequação formal ao procedimento estabelecido pela norma jurídica. Isso porque, em tal abordagem, as assimetrias de poder que a LGPD buscou combater são endereçadas de modo indireto. Assim, não se trata de estabelecer restrições duras ou vedações peremptórias sobre o tratamento de dados pessoais[303], considerados determinados contextos, hipóteses e finalidades, mas de legitimá-los. A LGPD, pelo contrário, ao compreender o tratamento de dados pessoais como

---

acerca de um indivíduo serão agregados, cruzados ou utilizados." (Mendes; Fonseca, 2020, p. 518) No mesmo sentido, cf. Solove, 2013, p. 1881; Solove, 2021, p. 43; Solove, 2023, p. 978; Marques; Mucelin, 2022, p. 18.

[301] Incidem perfeitamente sobre nosso objeto de estudo as pertinentes considerações formuladas por Frazão (2021) a respeito do mito da soberania do consumidor, no seguinte sentido: "entre o mundo ideal no qual o pressuposto da soberania do consumidor foi intelectualmente plasmado e o mundo real existe uma distância tão grande que, em muitos casos, falar em soberania do consumidor, mais do que uma falácia, pode ser uma verdadeira negação da realidade".

[302] "As estruturas tradicionais de proteção de dados são tão focadas nos dados de cada indivíduo que negligenciam importantes implicações sociais e de direitos civis decorrentes da coleta e tratamento de dados pessoais. Comunidades marginalizadas, particularmente comunidades de cor, arcam com um fardo desproporcional de abusos de privacidade". (Richards; Hartzog, 2020b, p. 1737, tradução nossa)

[303] Na lição de Richards (2022, p. 1523) a respeito do RGPD – aplicável à experiência brasileira –, a intenção da norma é a de "equilibrar os direitos de proteção de dados das pessoas humanas [...] com a realidade de que os fluxos de dados pessoais se tornaram uma marca registrada da economia e da sociedade europeias" (tradução nossa).

atividade imprescindível ao florescimento da inovação e ao desenvolvimento econômico, preocupa-se em incentivá-lo[304] e em *regulá-lo*, para que seja deferente aos direitos fundamentais dos titulares.

A opção do legislador revela uma lógica segundo a qual a observância de garantias, salvaguardas e obrigações asseguraria, por si só, o uso ético dos dados pessoais e, consequentemente, promoveria a privacidade, a autonomia individual, a liberdade, dentre outros bens jurídicos de igual estatura. Esse enfoque predominante nos requisitos procedimentais do tratamento de dados pessoais – inspirado pelas FIPs – enseja, no plano epistemológico, um *descolamento* entre a relação jurídica *substancial*, em que se encontram as assimetrias e demais elementos contextuais que informam (ou, no mínimo, interferem gravemente sobre) o contexto do tratamento, e a relação jurídica *informacional* de que cuida o regime jurídico de proteção de dados pessoais.

Em outras palavras, embora estabeleça princípios e direitos substantivos, a LGPD se estrutura sobre uma lógica procedimental para fazer com que sejam efetivados. Ao fazer isso, desdobra, no plano epistemológico, uma mesma relação em duas: a relação que chamamos *substancial*, marcada (no contexto das plataformas) pelas assimetrias, pelas técnicas de *design* da arquitetura digital, pela dependência dos titulares, e a relação *informacional*, que ocorreria num ambiente etéreo, ideal, em que as características da relação substancial – ainda que em alguma medida levadas em consideração na estruturação do procedimento – não são priorizadas ao se avaliar a legitimidade do tratamento. Nesse particular, Richards e Hartzog (2020b, p. 1724) bem observam que as FIPs "estabelecem as pré-condições para o processamento, mas, em última análise, não questionam as implicações do próprio processamento" (tradução nossa).

O foco sobre o procedimento promove um achatamento das relações de poder, na medida em que o conjunto de requisitos necessários a um tratamento legítimo não leva em consideração o fato de que nem todas as assimetrias de poder são iguais. De fato, embora o legislador reconheça tais disparidades entre titulares e agentes de tratamento, o caráter procedimental do regime jurídico de proteção de dados pessoais é *uniformizante*.

Não por outra razão, o mesmo conjunto de regras previsto pela LGPD se aplica tanto à Meta quanto a uma pequena imobiliária, muito embora os titulares estejam muito mais

---

[304] "O objetivo de regimes de proteção de dados como o RGPD sempre foi incentivar o tratamento justo de dados e equilibrar interesses conflitantes, em vez de impedir totalmente o tratamento de dados. Em outras palavras, todo o esforço da proteção de dados moderna baseada nas FIPs é construído em torno da ideia de que, desde que o tratamento de dados seja justo para o titular, a lei não deve apenas regulá-lo, mas sim criar uma estrutura legal para habilitá-lo." (Richards; Hartzog, 2020b, p. 1722, tradução nossa)

vulneráveis a uma gigantesca e bilionária multinacional cujo negócio predominante envolve a manipulação[305], a extração massiva de dados pessoais, o perfilamento e a venda dessas informações a anunciantes. A propósito, Solove (2023, p. 993) acertadamente afirma que o "maquinário gigantesco que Shoshana Zuboff chama de 'capitalismo de vigilância' é pouco afetado pelo número minúsculo de pessoas que ocasionalmente exercem um dos seus direitos de privacidade" (tradução nossa). No mesmo sentido, Richards e Hartzog (2021, p. 1008):

> Fingir que nosso relacionamento com empresas que oferecem serviços *online* ocorre em paridade de condições, como se fossem vendedores de cachorro-quente da esquina, é uma zombaria das estruturas legais postas em prática precisamente por se reconhecer que alguns relacionamentos são muito mais perigosos do que outros. Em tais situações, apenas a lealdade é especificamente adaptada para evitar toda a gama de comportamentos oportunistas que decorrem de um desequilíbrio de poder tão acentuado e da profunda exposição de nós mesmos aos caprichos daqueles que, de outra forma, nos rasgariam em partes. (Tradução nossa)

Por compreender que a adequação procedimental das atividades de tratamento aos parâmetros legais consubstancia, *per se*, o tratamento legítimo de dados pessoais, é possível que o regulador venha a reputar legítimas práticas de tratamento que aprofundam ainda mais as assimetrias de poder e a dependência com relação às plataformas, que estimulam o vício e, consequentemente, comprometem a autonomia individual. Afinal, a conformidade é atestada por demonstrações formais de adequação do tratamento, e não pelos *resultados* da adequação. A atividade fiscalizatória do regulador se encerra quando se identifica a regularidade formal do tratamento, por mais que, na prática, o agente de tratamento continue a explorar o poder que exerce sobre os indivíduos para dar curso a atividades econômicas que se nutrem da extração massiva de dados pessoais.

Daí por que Richards e Hartzog (2021, p. 982), valendo-se da expressão cunhada na crítica de Chris Soghoian, cogitam da formação de um "teatro da privacidade" (*privacy theater*), em que o consentimento, ao invés de representar verdadeira defesa individual contra o tratamento abusivo de dados pessoais, serve, na verdade, como o ponto de partida para o início de uma série de práticas manipulativas que aprofundam, ainda mais, as assimetrias de poder que a lei buscou combater:

---

[305] "Todos são vulneráveis à manipulação porque ninguém tem acesso direto à informação. Você não pode ser testemunha em primeira mão de tudo o que acontece em seu país e ao redor do mundo. Você toma conhecimento sobre candidatos e eventos políticos principalmente através de suas telas. Mas, muitas vezes, você não escolhe suas fontes. Você não vai à procura delas – elas vêm à sua procura. Elas aparecem em seus feeds do Twitter ou Facebook. E embora elas possam aparecer como por magia ou por coincidência, empresas como o Facebook estão fazendo uma curadoria cuidadosa desse conteúdo para você. Estão vendendo sua atenção para atores desconhecidos que querem influenciá-lo." (Véliz, 2021, p. 118)

> Os aspectos processuais dos regimes de proteção de dados que enfatizam a autodeterminação informacional não protegem contra o oportunismo. Na verdade, o maquinário é construído de forma a encorajá-lo. Pedidos de "consentimento" são o marco zero para comportamento desleal *online*. Eles servem como pouco mais do que fachada – um "teatro da privacidade" que dá às empresas permissão para se envolver em qualquer forma de manipulação para persuadir e extrair informações e fatiar e cortar os dados de nossas vidas de um milhão de maneiras diferentes. (Tradução nossa)

A LGPD, assim como demais leis herdeiras da tradição das *Fair Information Practices*, não olha diretamente para a higidez dos bens jurídicos que, ao fim e ao cabo, se presta a tutelar (como o uso da informação para minar a atenção e o bem-estar dos indivíduos[306]), mas sim para a comprovação da adoção das cautelas por ela exigidas. As fragilidades dessa abordagem legal-regulatória relacionam-se com a possibilidade de que agentes de tratamento apresentem demonstrações de conformidade, como relatórios de impacto à proteção de dados, de modo raso e superficial[307], suficiente apenas a satisfazer os critérios (também formais e procedimentais) da norma e do regulador.

Assim é que, segundo Waldman (2021, p. 132), as medidas de *compliance* podem ser (como de fato são) compreendidas como demonstrações meramente simbólicas, destinadas a evitar, na maior medida possível, alguma responsabilização do agente de tratamento. A conformidade procedimental, aliás, depende, em larga medida, da compreensão estabelecida pelas próprias empresas a respeito do que seja a proteção de dados pessoais[308]. No mesmo sentido, Cofone (2024, p. 99) bem observa que

> O foco na regra processual transforma a conformidade com a proteção de dados em exercícios de marcação de caixas. Quando a indústria de tecnologia pode interpretar e implementar a lei por meio de listas de verificação, registros e documentação (como avaliações de impacto de privacidade), as empresas encontram maneiras de minar a lei na prática. (Tradução nossa)

Nesse cenário, atividades de tratamento que possam *afetar significativamente* interesses e direitos fundamentais[309] podem continuar ocorrendo desde que, sob a ótica da relação

---

[306] "[...] a privacidade de dados diz respeito a direitos civis, liberdade de expressão, liberdade contra assédio, interesses de autonomia coletiva e como as informações pessoais são utilizadas para corroer nossa capacidade de atenção, nosso bem-estar mental e nossas instituições públicas." (Richards; Hartzog, 2020a, p. 4)

[307] "Por exemplo, os requisitos para realizar avaliações de impacto de privacidade e se implementar a proteção de dados por design e padrão não têm especificidade ou responsabilidade suficientes, permitindo que as empresas os façam de maneiras minimalistas e superficiais." (Solove; Hartzog, 2024, p. 1030)

[308] "Temo que, enquanto a proteção de dados não estiver nos corações e mentes dos controladores – e a lei até agora tem feito um mau trabalho em atingir esses corações e mentes [...] – as avaliações obrigatórias de impacto sobre a proteção de dados funcionarão como listas de verificação em papel que os controladores preenchem, marcam e arquivam para mostrar devidamente aos auditores ou autoridades de supervisão, se eles algum dia solicitarem. Procedimento seguido, problema resolvido." (Koops, 2014, p. 7, tradução nossa)

[309] Confira-se a definição prevista pelo art. 4º, § 2º, da Resolução CD/ANPD n. 2/2022: " O tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um

informacional, tenham sido atendidos requisitos objetivos previstos pelo legislador, como a condução de uma prévia análise de impacto. A visão procedimental é incompatível com a compreensão de que a proteção de dados é, na verdade, um mecanismo instrumental à proteção de direitos fundamentais como a igualdade, a autonomia, a dignidade e a própria democracia[310].

Especialmente no que concerne aos padrões obscuros e à tutela da autonomia individual, a perspectiva procedimental limita sobremaneira o olhar do regulador e o potencial protetivo da lei. Fundamental, no ponto, transcrever a precisa observação de Hartzog (2017, p. 969):

> Retórica visual, antropomorfismo e outras ferramentas psicológicas podem ser implantadas à sombra das FIPs, que exigem apenas transparência quanto à coleta de dados e práticas de uso. Dados coletados com nosso consentimento podem ser alavancados contra nós. As FIPs não articulam nenhum limite significativo sobre as empresas que usariam nossas próprias limitações cognitivas contra nós ou dão qualquer noção clara de quando as empresas terão cruzado uma linha ética ao usar nossos próprios dados para tentar nos persuadir a compartilhar mais, clicar em um anúncio ou fazer uma compra online. Dada a crescente eficácia do aprendizado de máquina e do *big data*, essa ameaça só continuará a crescer. (Tradução nossa)

Em suma, nosso regime jurídico não indaga *se* agentes de tratamento podem, por exemplo, desenvolver novas plataformas de conteúdo que extraiam dados pessoais, de todos os tipos e modos, a partir de interfaces viciantes[311]. Esse tipo de atividade, presumivelmente protegida pelo princípio da livre iniciativa, *pode* acontecer, por mais questionável que seja. O que a LGPD busca esclarecer é se o agente de tratamento ofereceu demonstração suficiente de que se cercou das cautelas necessárias a assegurar, por exemplo, o exercício dos direitos dos titulares, ou se formulou políticas de privacidade de modo suficientemente claro e acessível, mesmo que ninguém as leia.

Adequado, nesse particular, referir à lição de Richards e Hartzog (2020b, p. 1693), segundo a qual "regimes de proteção de dados procuram permitir uma vigilância e um processamento de dados mais éticos em detrimento de questões fundamentais sobre se essa vigilância e esse processamento devem ser permitidos em primeiro lugar" (tradução nossa). O

---

serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade."

[310] "Muitos dos elementos estruturais do RGPD não têm a mesma força e rigor que os elementos de controle individuais do RGPD. Por exemplo, os requisitos para realizar avaliações de impacto de privacidade e se envolver em proteção de dados por design e padrão não têm especificidade ou responsabilidade suficientes, permitindo que as empresas os façam de maneiras minimalistas e superficiais." (Solove; Hartzog, 2024, p. 1030, tradução nossa)

[311] "[...] os regimes de proteção de dados fazem pouco para mitigar muitos dos problemas das tecnologias que são projetadas para serem viciantes para maximizar a interação e a coleta de dados. Por exemplo, a pessoa média passa quatro horas olhando para seu telefone todos os dias. Nosso uso compulsivo da tecnologia está causando estragos em nosso bem-estar emocional e mental, especialmente para os jovens." (Richards; Hartzog, 2020b, p. 1725, tradução nossa)

modelo procedimental deixa de considerar que regular a privacidade – ainda que por meio da proteção de dados pessoais – é, essencialmente, regular o poder (Solove, 2023, p. 979), e não o mero fluxo burocrático de atividades de tratamento, a partir das quais devem ser produzidos relatórios, inventários e análises de impacto.

Nessa perspectiva, o foco no procedimento retira os holofotes das relações de poder e de suas assimetrias (e de seu consequente agravamento) e obscurece uma interpretação mais ampla sobre a própria justiça do tratamento de dados pessoais. Afinal, razão assiste a Cofone (2024, p. 99), ao afirmar que os abusos que a adequação pelo procedimento busca reprimir não consistem propriamente na realização de atividades proibidas, mas sim nas violações praticadas *dentro dos próprios limites* estabelecidos pelas normas procedimentais.

A lógica procedimental, todavia, não olha para as consequências do tratamento, e sim para as finalidades declaradas ao titular e ao regulador. Não se olha para a motivação do tratamento (porque amiúde acobertada pela figura do *segredo comercial*, prevista pelo art. 6º, V, da LGPD), mas sim para as metodologias e os resultados de testes de balanceamento feitos pelas próprias empresas, nos quais seus próprios interesses são confrontados com os direitos dos titulares. Na acertada crítica de Solove (2023, p. 1035):

> Com muita frequência, as leis de privacidade focam na superfície. Elas olham se os dados estão corretos em vez de se os dados levam a bons julgamentos sobre as pessoas. As leis olham se as formalidades foram seguidas, como fornecer informações às pessoas, em vez de se as pessoas são realmente informadas. As leis olham se as pessoas têm direitos para excluir e corrigir em vez de se as organizações estão realmente se envolvendo na minimização de dados e mantendo a qualidade dos dados. (Tradução nossa)

Nesse particular, vale ilustrar o argumento a partir da menção – no contexto da hipótese legal do legítimo interesse – ao *teste de balanceamento de interesses legítimos*, que, segundo a Autoridade Nacional, consiste em "uma avaliação de proporcionalidade realizada com base no contexto e nas circunstâncias específicas do tratamento de dados, levando em consideração os impactos e os riscos aos direitos e liberdades dos titulares" (ANPD, 2024, p. 29).

No caso concreto envolvendo o uso, pela Meta, de dados pessoais para o treinamento de algoritmos de IA Generativa (ao qual já nos referimos no Capítulo 2), o regulador suscitou a inadequação da base legal do legítimo interesse, na medida em que as atividades envolviam o tratamento de dados pessoais sensíveis. Além disso, embora a base legal do legítimo interesse possa justificar o tratamento de dados pessoais de crianças e adolescentes, é necessário que, em qualquer caso, prevaleça o seu melhor interesse (circunstância que presumivelmente não se constata quando o tratamento de dados pessoais tem por finalidade o treinamento de algoritmos de IA Generativa daquela *big tech*).

Nada obstante, mesmo consignando que *o seu próprio voto* "e a situação em análise não necessariamente levam à legitimação conclusiva do uso da hipótese legal do legítimo interesse", decidiu o Diretor Relator – no que foi seguido, à unanimidade, pelo Conselho Diretor da ANPD – pela suspensão da medida preventiva, na medida em que a Meta "apresentou toda a documentação exigida, incluindo o teste de balanceamento" (Voto n. 23/2024/DIR-JR/CD).

A postura do regulador, no caso da Meta, revela e reforça o aspecto preponderantemente procedimental das normas conformadoras do regime jurídico de proteção de dados, além da consentânea interpretação da ANPD. Longe de estabelecer vedações substanciais, proibindo o tratamento de dados pessoais na forma e para as finalidades indicadas – e por mais imprevisíveis e perigosas que fossem as suas consequências – o regulador entendeu suficientemente demonstrado (ao menos a ponto de suspender a medida de urgência), a partir do *teste de balanceamento* apresentado, o respeito aos interesses e direitos fundamentais dos milhões de usuários brasileiros.

Considerando-se esse cenário, é possível afirmar, do ponto de vista da proteção da autonomia individual, que o paradigma do controle é eficiente? No Brasil, o exercício dos direitos previstos na LGPD pelos titulares de dados pessoais tem de fato reduzido assimetrias de poder e promovido (por exemplo) o respeito à privacidade?

A discussão a respeito dos contornos dogmáticos e das implicações epistemológicas do paradigma do controle nos revela que não. O caso da Meta, no plano prático, também. Verifica-se ter acerto, afinal, a observação de Cofone (2024, p. 98), para quem a principal pergunta, no modelo procedimental de proteção de dados pessoais, "não é se uma prática envolvendo dados pessoais é *danosa*, mas sim se alguém usou informações pessoais de um modo proibido – geralmente sem usar uma base legal, como o consentimento" (tradução nossa).

4 O PARADIGMA DA CONFIANÇA NA PROTEÇÃO DE DADOS PESSOAIS: UM PASSO ADIANTE NA PROTEÇÃO DA AUTONOMIA INDIVIDUAL

Verificamos, na presente investigação, que a proteção de dados pessoais nasce como decorrência do advento de tecnologias que permitiram a coleta e o armazenamento de dados em meios eletrônicos, abrindo limiares completamente novos ao tratamento das informações a respeito das pessoas humanas. O incremento progressivo das tecnologias de informação e comunicação – ao longo dos últimos 50 anos – trouxe consigo novos desafios à proteção da privacidade e da autonomia, requerendo da dogmática jurídica adaptações adequadas a tornar o Direito apropriado a seu tempo, a fim de servir à precípua finalidade de proteger os indivíduos contra abusos, arbitrariedades e perseguições.

Se o surgimento de uma disciplina autônoma da proteção de dados pessoais decorre justamente da realidade imposta pelos implacáveis avanços da ciência e da tecnologia, deve ela ser – porque assim o foi desde o início – condizente com a quadra histórica em que se situe. Há muito o cenário do tratamento de dados pessoais deixou de se caracterizar por computadores que ocupam o espaço de uma sala inteira e por um fluxo limitado de informações pessoais.

É por esta fundamental razão que se propõe uma **mudança de paradigma** para o regime jurídico de tutela dos dados pessoais: como também abordado na presente pesquisa, não basta que as ferramentas colocadas pelo legislador à disposição da defesa da privacidade e da autonomia sejam apropriadas ao estado da arte das *tecnologias* que permeiam o fluxo perene de dados pessoais, em atenção aos riscos por elas gerados. Demais disso, necessário, também, que esse ferramental normativo seja condizente com a *realidade social* subjacente à aplicação da norma, sob pena de *inefetividade*.

Necessário cogitar, portanto, de uma epistemologia da proteção de dados pessoais – se se pretende seja efetiva – apropriada às características da sociedade brasileira, no que importa, especialmente, à *relação*[312] dos indivíduos com as tecnologias de informação e comunicação, de que tratamos no Capítulo 3. Num país de graves desigualdades socioeconômicas, de passado colonial, de elevado analfabetismo e de pronunciada falta de compreensão a respeito do manejo

[312] "[...] deveres relacionais são extremamente sensíveis às disparidades de poder dentro de relacionamentos de informação. [...]. Deveres de lealdade protegem contra comportamentos oportunistas, enquanto deveres relacionados de cuidado aplicados a relacionamentos protegem contra comportamentos perigosos e riscos de dano. Quanto maior o desequilíbrio de poder e mais vulneráveis as pessoas são pela exposição, maior deve ser o dever atribuído à parte em quem se confiou." (Richards; Hartzog, 2022a, p. 360, tradução nossa)

(e dos riscos) de tecnologias digitais[313], bem como da proteção dos dados pessoais e de sua importância para a tutela de liberdades fundamentais[314], não é apropriado reduzir a proteção de dados pessoais à noção de *controle* individual.

Nesse sentido, em interessante pesquisa empírica conduzida por Schedeloski (2024), e cujos resultados foram relatados em sua tese de doutoramento, buscou-se dimensionar a extensão do conhecimento dos brasileiros a respeito do tema da proteção de dados pessoais. Um dos critérios de investigação, por exemplo foi a compreensão dos entrevistados a respeito da *destinação* dos dados pessoais coletados no contexto de relações de consumo: enquanto 24% das pessoas afirmaram acreditar saber o que seria feito com seus dados pessoais, 76% afirmaram não saber. Na análise da autora (2024, p. 97):

> Isso evidencia como o consentimento informado ainda não ocorre no país: **as informações são coletadas, no entanto os titulares não têm conhecimento sobre o que é feito com elas**.
>
> Tal fato pode ter-se dado pelo índice de amabilidade (*agreeableness*) de brasileiros ser maior do que o de outras nacionalidades. Isto é, **brasileiros não costumam discordar de outras pessoas e evitam tensões sociais**. Isso pode gerar a transmissão de informações mesmo em hipóteses com as quais não concordem ou das quais não tenham total conhecimento. [...].
>
> Daqueles que não possuíam conhecimento da LGPD [...], 84% falaram que não tinham conhecimento sobre o que estava sendo feito com seus dados; entre as pessoas com conhecimento iniciante, 73% não tinham conhecimento; com conhecimento médio, 66% das pessoas não sabiam; e com conhecimento avançado, 58% não tinham conhecimento. (grifo nosso)

Da mesma forma, a perspectiva *procedimental* – também à luz da realidade do único país que aprovou uma lei geral de proteção de dados sem ter criado, ao mesmo tempo, uma autoridade reguladora – limita o âmbito da tutela protetiva do regime jurídico centralizado pela LGPD (em que o único valor *substantivo* é a prevenção de danos[315]), na medida em que falha ao considerar a proteção de dados pessoais sob a perspectiva mais ampla (e primordial) da

---

[313] "[...] quem cresce em ambiente pobre de recursos, e é informado sobre indícios de mortalidade, está mais propenso a valorizar recompensas imediatas a recompensas adiadas, em comparação àqueles que são similarmente informados e crescem em ambientes ricos em recursos. Jovens brasileiros que vivem em favelas descontam recompensas futuras com mais frequência do que estudantes universitários da mesma idade." (Lembke, 2024, p. 103)

[314] "Geralmente, **a ANPD ainda não é percebida como um espaço de interação para esse tema [direitos relacionados à proteção de dados pessoais] entre os usuários de Internet**. Nesse sentido, estratégias de divulgação de atribuições e atividades dessas diferentes organizações podem orientar os cidadãos quanto à entidade mais adequada para tratar de solicitações referentes ao tema, a fim de trazer maior segurança quanto aos canais voltados para a garantia desses direitos." (Oyadomari; Costa; Ribeiro, 2023, p. 9, grifo nosso)

[315] "[...] as leis de privacidade modernas são incompletas porque, desde o seu início, falharam ao levar em conta a importância da confiança. Essa lacuna tem enviesado o direito à privacidade e as normas em direção a um processualismo pessimista no qual a prevenção de danos é o único valor substantivo. A confiança, nas relações informacionais, é necessária para que a economia digital não apenas funcione, mas floresça. Agindo juntas, privacidade e confiança podem fazer mais do que evitar danos, mas podem criar valor." (Richards; Hartzog, 2016, p. 435, tradução nossa)

contenção da acumulação do poder – e de suas repercussões danosas a liberdades fundamentais – em proporções inimagináveis nas mãos de alguns poucos agentes econômicos. Como vimos, se informação é poder, a regulação do trânsito informacional, com vistas à proteção da privacidade, da liberdade e da autonomia, não pode prescindir da consideração das dinâmicas e instrumentos de perpetuação de poder que subjazem à lógica da extração massiva (e à comercialização) de dados pessoais[316].

O regime procedimental inspirado no modelo europeu identifica uma virtude intrínseca no tratamento de dados pessoais, reconhecendo-se, de fato, que a informação se tornou indispensável à manutenção de uma miríade de atividades econômicas e mesmo à prestação eficiente de serviços públicos. O objetivo do RGPD (e, consequentemente, também da LGPD) não é conter a acumulação do poder por meio da proibição do tratamento de dados pessoais sob certas circunstâncias, mas, sim, viabilizá-lo e mesmo incentivá-lo, *desde que* ocorram em parâmetros considerados adequados (*legitimidade* do tratamento)[317].

Ao assim fazer, contudo, o RGPD direciona seus holofotes não sobre técnicas de perfilamento e de manipulação diluídas em ambientes digitais inteiramente desenhados e operados por grandes conglomerados digitais (por exemplo), mas, sim, sobre o que deve ser o tratamento *legítimo*, assim entendido aquele que cumpre os requisitos formais da norma. Consequentemente, conformidade formal e violação substancial podem coexistir. Como bem pontuam Richards e Hartzog (2021, p. 982),

> Podemos ser tentados a pensar que o RGPD e regimes de proteção de dados semelhantes ao redor do mundo podem ser suficientes para impedir que as empresas ajam de forma oportunista. Mas os regimes de proteção de dados podem, na verdade, facilitar o comportamento oportunista porque o RGPD e seus semelhantes são focados em dados e não nas disparidades dentro das relações informacionais. Os modelos de proteção de dados focam em dados pessoais identificáveis e como tratá-los legitimamente, em vez de focar na dinâmica de poder nas relações. Este é um enfoque primordialmente processual porque especifica o que é necessário para tratar dados (se o consentimento ou a notificação são necessários, etc.), em vez de colocar limites substantivos em tipos ou propósitos de tratamento. Como resultado, os modelos de proteção de dados podem ignorar abusos que não envolvem tratamento de dados pessoais, como padrões obscuros para *nudges* ou o uso

[316] "O poder das empresas de tecnologia é constituído, por um lado, pelo controle exclusivo de nossos dados e, por outro, pela capacidade de prever cada movimento nosso, o que, por sua vez, lhes dá oportunidades de influenciar nosso comportamento e vender essa influência a outros – incluindo governos." (Véliz, 2021, p. 85)

[317] "Regimes de proteção de dados baseados em FIPs são resistentes à imposição de limites de coleta diretos e inflexíveis porque os FIPs são projetados para facilitar, e não para restringir o tratamento. [...]. Mas os dados distribuem poder a quem os coleta. Limitar a coleta pode ajudar a restaurar o equilíbrio. No entanto, pontualmente, se os legisladores quiserem limitar significativamente a coleta, eles terão que aceitar e ser claros sobre os custos financeiros de fazê-lo, e se preparar para defender que tais custos são necessários para o tipo de inovação que é sustentável e realmente promove os valores humanos e o florescimento humano." (Richards; Hartzog, 2020b, p. 1753, tradução nossa)

> de conhecimento obtido de dados agregados de outras pessoas para nos manipular. (Tradução nossa)

É necessário, portanto, refletir sobre a tutela substancial a que se presta a proteção de dados pessoais a partir de uma perspectiva, igualmente, substancial. Para tanto, importa trazer à baila um conhecido – porém nem sempre percebido[318] – elemento especialmente relevante para as relações jurídicas marcadas por dependência de uma parte em relação à outra e por assimetrias de poder informacional: a **confiança**.

Cumpre observar, desde logo, que a confiança – expressamente mencionada apenas uma vez no texto da LGPD (quando se estabelece, como *faculdade* do controlador, a criação de programa de governança que tenha o objetivo de estabelecer relação de confiança com o titular – art. 50, § 2º, I, "e") – é um elemento fundamental às relações estabelecidas, de modo geral, na esfera civil[319]. Assim, a confiança, plasmada no princípio da boa-fé, envolve em boa medida a expectativa, nutrida de parte a parte de uma dada relação jurídica, de que todos procederão de modo honesto, íntegro e leal (art. 422 do Código Civil). Na lição autorizada[320] de Martins-Costa (2024, p. 225):

> Há evidente e intensa ligação entre boa-fé e confiança. Antes de mais, há uma comum raiz, a *fides* que está no núcleo de ambos. Essa ligação é por vezes de superposição, por outras de diferenciação: pelo primeiro viés (superposição), a boa-fé abrange a tutela das legítimas expectativas, sobrepondo-se ao princípio da confiança (*bona fides – cum fide*s). No proteger as legítimas expectativas, cabe falar em uma confiança objetivada, que não se reduz ao estado de fato característico da boa-fé subjetiva, ou "boa-fé crença", mas é pautada pelo que comumente acontece (*id quod plerumque accidit*) em certo setor ou situação da vida).

Portanto, aquele que paga confia em que a parte contratada prestará o serviço, e que o fará na forma avençada em contrato. Aquele que institui o fideicomisso deposita no fiduciário

---

[318] "A confiança está em todo lugar, mesmo que não seja óbvia. Confiamos que arquitetos e construtores criaram pontes que nos suportarão quando as cruzarmos. Confiamos que os comerciantes aceitarão os pequenos pedaços verdes de papel (ou código digital) que nós ganhamos em troca de bens e serviços. Confiamos que os aviões chegarão com segurança e ao aeroporto correto. Confiamos que os profissionais a nosso serviço agirão em nosso melhor interesse e confiamos que nossos amigos nos apoiarão e cuidarão de nós. Sem confiança, nossos sistemas modernos de governo, comércio e a própria sociedade ruiriam." (Richards; Hartzog, 2016, p. 433, tradução nossa)

[319] "A confiança nos permite correr riscos, cooperar com os outros, tomar decisões apesar da complexidade, e criar ordem no caos, entre tantas outras funções cotidianas. A confiança também encoraja o compartilhamento terapêutico ao dar a todos os indivíduos, desde alcoólatras e aqueles que sofrem de depressão até amigos próximos, a confiança de que precisam para revelar informações pessoais e talvez estigmatizantes. Nessas situações, as normas que esperamos que os outros sigam – confidencialidade e discrição – são essenciais para criar as circunstâncias necessárias para o compartilhamento em primeiro lugar." (Waldman, 2018, p. 74, tradução nossa)

[320] No mesmo sentido, Tomasevicius Filho (2020, p. 168) pondera: "Como afirmou Mota Pinto, uma das funções essenciais do direito é, sem dúvida, assegurar expectativas, para dar estabilidade e previsibilidade às ações. Daí surgir a necessidade de proteção da confiança despertada pela expectativa, pois esta reduz a complexidade social. Ao confiar, a pessoa não precisa buscar mais informações destinadas a reduzir os custos de transação na tomada de determinada decisão."

a confiança de que, para depois da abertura da sucessão, o legado ou herança serão transmitidos ao fideicomissário, após implementado determinado termo ou condição (art. 1.951 do Código Civil). A teoria dos atos próprios, da mesma forma, reporta-se a atos praticados com abuso de direito, em desconformidade com o princípio da boa-fé objetiva, como o comportamento contraditório[321] (*venire contra factum proprium*) e a surpresa por conduta inesperada (*tu quoque*).

Ao mesmo tempo, a confiança pressupõe, com maior ou menor intensidade, a *vulnerabilidade* (e, bem assim, a dependência) à ação de outrem, bem como a incerteza a seu respeito, o que traz à evidência a *dinâmica de poder* natural a tais relações. Como bem elucida Heimer (2001, p. 43),

> incerteza e vulnerabilidade são os elementos centrais das relações de confiança. A forma que a incerteza e a vulnerabilidade assumem varia muito de acordo com a substância do relacionamento. E embora as estratégias canônicas envolvam a diminuição da incerteza ou a redução da vulnerabilidade, as escolhas dos participantes sobre qual estratégia ou conjunto de estratégias adotar normalmente são limitadas pelas características de seus mundos sociais. Além disso, é crucial reconhecer que a confiança é dinâmica. Embora os participantes possam optar por estratégias de desconfiança em um ponto no tempo, ao facilitar interações que de outra forma seriam muito custosas, as estratégias de desconfiança permitem que os primeiros movimentos provisórios de relacionamentos, trocas de informações, adaptação mútua e, às vezes, eventualmente, confiança, se desenvolvam. (Tradução nossa)

No âmbito das relações informacionais – nas quais a informação desempenha um papel fundamental no contexto do negócio jurídico celebrado, pois a partir dela é que se viabilizará a execução contratual –, esse aspecto é particularmente relevante, na medida em que os danos causados pelo inadimplemento extrapolam a esfera patrimonial, podendo atingir[322] direitos inerentes à própria personalidade, como a inviolabilidade da vida privada (art. 21 do Código Civil). Assim esclarecem Richards e Hartzog (2021, p. 986):

> Em relações de confiança, a parte que confia se torna vulnerável ao poder da pessoa em quem se confia. No caso particular de uma relação informacional, o poder é conferido por meio da exposição de informações pessoais e da

[321] "Em se tratando da proibição de vir contra os próprios atos, podem-se observar os efeitos provocados pelo estado de informação assimétrica e pelos custos de transação, cabendo, por meio do princípio da boa-fé, reduzi-los ou eliminá-los. A situação de incerteza decorre do próprio contrato social, o que gera incerteza e risco. Ao mesmo tempo em que há este risco, naturalmente instala-se o processo de comunicação, por meio do qual haverá troca de informações entre si acerca das condutas futuras, seja pelo diálogo ou pela interpretação do comportamento adotado, concluindo-se, portanto, que se agirá de determinada maneira." (Tomasevicius Filho, 2020, p. 180)

[322] "[...] vulnerabilidade pode incluir risco aumentado de uso indevido de informações, divulgação não autorizada, manipulação ou perda de autonomia. [...]. As possibilidades de divulgação, dano ou manipulação em tais casos são limitadas apenas pelo potencial humano para inovação. Uma vez que as informações de uma pessoa são divulgadas, ela não tem mais controle exclusivo sobre seu uso e disseminação. Ela é exposta e fica à mercê da parte em quem confiou." (Richards; Hartzog, 2016, p. 450, tradução nossa)

> submissão da agência. Esse poder é aumentado quando as partes lidam entre si em ambientes mediados tecnologicamente, como interfaces de aplicativos [...] ou redes sociais. O poder dado às partes "confiadas" permite que elas tomem decisões que afetarão o bem-estar da parte "confiante". (Tradução nossa)

Nessa perspectiva, a confiança é um elemento essencial à divulgação (*disclosure*) de dados pessoais, na medida em que o fornecimento de informações pessoais (seja a pessoa física, seja a pessoa jurídica) envolve, de fato, uma suscetibilidade – sensível ao contexto – à ação da parte que passa a deter ditas informações. Quem detém conhecimento sobre alguém detém, da mesma forma, o potencial de exercer poder sobre a pessoa cujas informações são conhecidas.

A intensidade do fluxo informacional, bem como a natureza da informação compartilhada, varia de acordo com o contexto da relação[323]. Revelamos nossos segredos mais íntimos a parceiros amorosos; compartilhamos relatos ou informações embaraçosas com amigos próximos; intercambiamos registros fotográficos e audiovisuais que podem ir desde a nudez do corpo a momentos de convívio familiar. Da mesma forma, no âmbito das relações comerciais, a execução contratual envolve, amiúde, o fornecimento de dados pessoais consentâneos com o objeto do contrato.

Longe de meros truísmos, tais constatações se afiguram úteis à compreensão do fenômeno da intrincada relação entre privacidade, confiança e vulnerabilidade no vasto âmbito das relações humanas. Afinal, são esses três elementos essenciais ao florescimento de relações informacionais sustentáveis e de longo prazo (Richards; Hartzog, 2017, p. 1213). Nessa interação, a privacidade conforma um âmbito de defesa do indivíduo contra condutas antijurídicas perpetradas a partir do acesso a informações pessoais, seja pela obtenção indevida ou enganosa[324], seja pelo uso antiético daquelas a que a outra parte teve acesso em razão da relação jurídica estabelecida.

Embora, nessa perspectiva, a privacidade assuma pronunciada dimensão estática (remetendo-nos ao *right to be let alone*, proposto por Warren e Brandeis), o âmbito protetivo da privacidade se alarga, na sociedade da informação, considerando-se a indispensabilidade do

---

[323] Assim ensina Waldman (2018, p. 61): "A confiança, seja desenvolvida a partir de interação repetida [...], reciprocidade ou transferência, está no cerne de nossas decisões contextuais de compartilhar informações pessoais com outros. Nós a vemos na vida real, de jogos de confiança a redes sociais online, de interação familiar entre amigos a trocas limitadas entre estranhos online. A confiança nos dá a convicção e a disposição para compartilhar porque ela atenua as vulnerabilidades inerentes à exposição." (Tradução nossa)

[324] "As empresas às quais confiamos os nossos dados envolvem-se na coleta clandestina de dados, criam perfis e classificam-nos, incitam-nos a agir de formas que as beneficiam desproporcionalmente, partilham os nossos dados com redes obscuras de terceiros e empregam práticas de segurança de dados pouco rigorosas que nos expõem a riscos de danos futuros." (Richards; Hartzog; Francis, 2023, p. 1341, tradução nossa)

trânsito informacional para a própria participação[325] em espaços públicos de deliberação intermediados (ou inteiramente formados) por tecnologias digitais. Assim, a dependência do uso de plataformas digitais atribui novas nuances à privacidade, cuja dogmática passa a ser reconstruída com apoio no pressuposto de que a constante exposição de informações pessoais não é mais uma mera faculdade individual, mas uma necessidade[326].

A privacidade, que não se exaure no momento da coleta do dado pessoal, deve ser observada ao longo do fluxo informacional, em toda a sua complexidade (dotando-se, portanto, de expressão dinâmica). Proteger a privacidade é, na sociedade da informação, proteger a vulnerabilidade inescapável dos indivíduos, salvaguardando os seus melhores interesses contra condutas oportunistas e, por isso mesmo, desleais[327].

Esse deve ser, à luz do paradigma da confiança, o cerne da regulação do tratamento de dados pessoais, que servem, como notamos no primeiro capítulo deste trabalho, à prestação (ou ao aprimoramento) dos serviços intermediados pelas plataformas digitais. Como resultado, as atividades de tratamento mantêm em movimento as engrenagens da acumulação de poder (e, consequentemente, do aprofundamento de assimetrias[328]) que caracteriza o capitalismo de vigilância, ampliando o (já vasto) plexo de possibilidades de violações à privacidade e de interferências sobre a autonomia individual. Se **violações à privacidade e à autonomia** são causadas por comportamentos desleais e oportunistas, nos quais as vulnerabilidades reveladas pelos dados pessoais são exploradas em detrimento de seus titulares, a proteção de tais liberdades não prescinde da tutela da confiança[329].

---

[325] "[...] dependemos de empresas de dados para nos comunicar e buscar informações. É extremamente difícil navegar em nossas mais importantes necessidades sociais e de informação sem que elas sejam mediadas por empresas que ganham dinheiro com nossos dados." (Jones; Rubel; LeClere, 2019, p. 12, tradução nossa)

[326] "Essa exposição é necessária para participar de uma sociedade digital em rede na qual nossas finanças, nossas comunicações, nossos segredos e, de fato, nossas vidas pessoais, sociais, econômicas e políticas são mediadas por entidades às quais não temos outra escolha senão nos expor." (Richards; Hartzog, 2021, p. 969, tradução nossa)

[327] Segundo Richards e Hartzog (2020b, p. 1750), atos desleais caracterizam-se por serem "tentativas intencionais de usar tanto o design quanto os insights da economia comportamental para privilegiar os interesses de uma empresa na coleta de dados e na captação de atenção em detrimento da autonomia e dos interesses de privacidade do usuário" (tradução nossa).

[328] "[...] as relações dos usuários finais com muitos provedores de serviços online. Envolvem uma vulnerabilidade significativa, porque os provedores de serviços online têm experiência e conhecimento consideráveis e os usuários finais geralmente não têm. Os provedores de serviços online têm muitas informações sobre nós, e nós temos muito pouca informação sobre eles ou sobre o que eles podem fazer com as informações que coletaram. É fácil para os provedores de serviços online monitorar o que fazemos, especialmente porque eles coletam quantidades (e tipos) crescentes de dados sobre nós. Mas geralmente é muito difícil para nós monitorar suas operações e impedi-los de agir contra nossos interesses ou de trair nossa confiança." (Balkin, 2016, p. 1222, tradução nossa)

[329] "De fato, a confiança funciona como um contrapeso à vulnerabilidade e perda de poder inerentes à exposição. Ela forma a estrutura social de fundo que permite que o compartilhamento ocorra em primeiro lugar. E nós vivenciamos invasões de privacidade no momento em que essas normas de confiança são quebradas, não depois.

Como discutiremos no presente capítulo, a proteção de dados pessoais pautada no paradigma da confiança – que obsta, em última análise, o uso oportunista dos dados pessoais dos titulares, a partir da exploração sub-reptícia de suas vulnerabilidades, visando ao atingimento de finalidades que beneficiem exclusivamente o agente de tratamento – é capaz de abrir **campo fértil ao exercício e ao desenvolvimento da autonomia individual no ambiente das plataformas digitais**.

Ao estabelecer vedações substanciais ao tratamento de dados pessoais, voltadas à proteção da confiança dos titulares (e, consequentemente, de suas vulnerabilidades), o paradigma da confiança, por um lado, ressignifica os deveres de transparência, de confidencialidade e de segurança[330] incidentes sobre o tratamento de dados pessoais (reconhecidos pela teoria dos *deveres fiduciários* aplicados às relações informacionais, de que nos ocuparemos adiante), e, por outro, impõe aos agentes de tratamento a observância de um dever fundamental de lealdade, que implica, ao fim e ao cabo, a não utilização de dados pessoais na implementação de técnicas de manipulação, tais como os padrões obscuros, em interfaces digitais.

4.1 O papel fundamental da confiança na construção da privacidade

No presente trabalho, buscamos refletir – com especial ênfase sobre o fenômeno das plataformas digitais – sobre as características que marcam a relação (hoje, simbiótica) entre indivíduos e tecnologias digitais. A disseminação do acesso à Internet, em seus anos iniciais, veio acompanhada de um discurso otimista a respeito da formação de um espaço de livre criação e difusão do conhecimento; a respeito, também, de um marco fundador de uma nova era em que seriam encurtadas as distâncias entre indivíduos e sobremaneira incrementadas as potencialidades do intercâmbio de informações, os ganhos de eficiência em atividades econômicas, e a democratização do acesso ao conhecimento.

Isso é tão verdadeiro em contextos interpessoais quanto online. [...] essa maneira de entender a privacidade é diferente de muitas abordagens tradicionais baseadas em direitos. Esse contraste é colocado em grande relevo no contexto do uso de plataformas de 'big data' para segmentação comportamental, análise preditiva e tomada de decisão automatizada." (Waldman, 2018, p. 62, tradução nossa)

330 "Substituir as FIPs inteiramente seria uma tarefa assustadora. Mas, felizmente, o que é necessário não é a substituição das FIPs, mas sim seu rejuvenescimento, de um meio processual de fabricação de consentimento, em um sistema substantivo de regulamentação do tratamento de dados pessoais no interesse de todos. A confiança pode ser a fonte desse rejuvenescimento, permitindo-nos repensar as FIPs de maneiras que sejam positivas, substantivas e inspiradoras [...]." (Richards; Hartzog, 2016, p. 458, tradução nossa)

Esse contexto, sobretudo após o advento do capitalismo de vigilância, sofreu notáveis modificações[331]. Hoje, o acesso à Internet já não mais se limita a alguns escassos momentos nos dias (ou semanas) dos indivíduos. Estamos sempre conectados e, portanto, sempre expostos à vigilância e sujeitos à manipulação. A revolução da Internet móvel permitiu o rastreamento de (e por) dispositivos variados, para muito além do computador pessoal. A percepção do excedente comportamental (*behavioral surplus*), de que nos fala Shoshana Zuboff, como matéria-prima para a comodificação do comportamento humano, aliada à falta de regulação apropriada da utilização da informação relativa à pessoa humana, desvelou às empresas de tecnologia uma verdadeira *mina de petróleo*[332]. Essa dinâmica é bem sintetizada por Richards e Hartzog (2021, p. 972), nos seguintes termos:

> as pessoas não são mais a parte a ser servida, e sim se tornam grãos para os moinhos do comportamento e da atenção. Clientes humanos que confiam em empresas de tecnologia se transformam em fontes de matéria-prima de excedente comportamental, que é então usado para manipular esses mesmos clientes, para o benefício da plataforma capitalista de vigilância e de seus clientes reais, os anunciantes. (Tradução nossa)

O novo modelo econômico é marcado pela *instrumentalização*[333] da superioridade estrutural e informacional das empresas digitais em favor da exploração (e da própria formação) de vulnerabilidades individuais dos usuários que a elas confiam seus dados, dinâmicas não consideradas adequadamente na concepção do regime jurídico de proteção de dados pessoais de matriz europeia (Richards; Hartzog, 2021, p. 978). Como vimos, os agentes econômicos a que nos referimos são incentivados a maximizar[334] a extração de dados pessoais, utilizando-se, não raro, de comportamentos oportunistas, assim percebidos exatamente porque se estruturam

---

[331] "A internet da década de 2020 certamente fornece muitos serviços úteis, mas também se tornou o maior conjunto de vigilância corporativa e governamental da história da humanidade. [...]. E onde a internet prometia empoderamento humano, com muita frequência as ferramentas da ciência de dados e da ciência comportamental foram usadas para estimular o comportamento e fabricar consentimento para termos padronizados que ninguém lê." (Richards; Hartzog, 2021, p. 964, tradução nossa)

[332] "Diversos autores apontam a capacidade de orientar, modular ou modificar o comportamento do usuário que utiliza uma tecnologia como o objetivo final e o verdadeiro ouro negro no processo da coleta e análise de dados. Se os dados são o novo petróleo, a modulação do comportamento humano seria o produto de luxo, feito sob medida, já na ponta final da cadeia de produção." (Machado, 2021, p. 50)

[333] "[...] essas empresas de tecnologia altamente capitalizadas não agiram como os benevolentes 'arquitetos de escolha' que alguns esperavam que pudessem se tornar. As tecnologias – e a arquitetura de escolha – anunciadas como servindo aos consumidores tornaram-se, em vez disso, instrumentalizadas, servindo consumidores mercantilizados às empresas e seus clientes anunciantes comerciais e políticos." (Richards; Hartzog, 2021, p. 967, tradução nossa)

[334] "[...] empresas que coletam enormes quantidades de dados sobre indivíduos têm uma vantagem estratégica sobre seus clientes devido ao fato de que são confiadas com informações confidenciais do usuário, além do conhecimento superior e especializado, falta de transparência, e a confiança de seus usuários nos serviços especializados fornecidos. Dado um mercado altamente consolidado e o baixo risco [...] para a lucratividade, as empresas têm todos os incentivos do mundo para alavancar essa assimetria a seu favor, e muitas vezes o fazem." (Barrett, 2019, p. 1087, tradução nossa)

sobre as imensas assimetrias de poder (bem como da dependência) havidas com relação aos usuários de plataformas digitais.

Técnicas como o *profiling*, o microdirecionamento e a manipulação nutrem-se da extração massiva de dados pessoais (e também se potencializam a partir das disparidades de poder) para manter – e incrementar – o fluxo informacional, com consequências perigosas para os titulares de tais informações, a partir do que Balkin denomina de "incômodo algorítmico" (*algorithmic nuisance*)[335]. Como discutido no Capítulo 2, a implementação de interfaces maliciosas[336] subverte a autonomia individual para não apenas dar aos usuários de plataformas digitais a impressão de estarem no controle de sua própria privacidade, mas também se socorre de técnicas de *design* para catalisar a extração de dados pessoais.

Diante desse cenário, como se deve compreender a privacidade? A que serve a privacidade (ou a que deve servir) em uma quadra da História na qual a vida humana passa a implicar, em larga medida, o uso de plataformas digitais? Na medida em que a divulgação de dados pessoais (notadamente aqueles que revelam aspectos do comportamento e da mentalidade humana) envolve, de um lado, a *vulnerabilização* à ação de outrem e, de outro, a expectativa do tratamento ético, alheio a comportamentos oportunistas, a privacidade deve ostentar o papel primordial de se dirigir à tutela da *confiança* depositada[337] pelos titulares de tais informações nos agentes de tratamento. Na definição de Richards e Hartzog (2017, p. 1185),

> Devemos pensar na privacidade como as regras que governam as informações pessoais e levam em conta contextos sociais mais complexos, a importância crescente das relações informacionais na era digital e nossa necessidade de confiar em (e compartilhar informações com) outras pessoas e instituições para viver nossas vidas. [...]. Se a privacidade é cada vez mais sobre essas relações informacionais, também é cada vez mais sobre a confiança necessária para que elas prosperem, sejam essas relações com outros humanos, governos ou empresas. (Tradução nossa)

Nessa perspectiva, tem-se que, na sociedade da informação, privacidade, confiança e vulnerabilidade devem ser compreendidas como vetores centrais de uma epistemologia pautada

---

[335] "O conceito de incômodo algorítmico decorre do fato de que as empresas coletam dados sobre pessoas de várias fontes e usam algoritmos para tomar decisões sobre as pessoas. Por meio desse processo, as empresas fazem mais do que simplesmente tomar decisões. Elas também constroem identidades, características e associações digitais das pessoas, o que, por sua vez, constrói (e restringe) suas oportunidades futuras." (Balkin, 2017, p. 17, tradução nossa)

[336] "Designers agem de forma desleal quando empregam elementos maliciosos de interface do usuário (às vezes chamados de 'padrões obscuros') de maneiras que visam a influenciar o comportamento de um titular de dados pessoais contra seus melhores interesses." (Richards; Hartzog; Francis, 2023, p. 1356, tradução nossa)

[337] "Em termos simples, a privacidade importa porque permite a confiança. As regras de privacidade podem governar os usos de informações nas relações, e essas regras podem construir confiança. As regras de privacidade que promovem a confiança permitem que as pessoas divulguem com segurança informações pessoais de maneiras que beneficiem não apenas os indivíduos, mas também as entidades com as quais compartilham seus dados." (Richards; Hartzog, 2016, p. 447, tradução nossa)

na **proteção da autonomia individual contra as ameaças do capitalismo de vigilância**. A confiança, entendida, no contexto das relações informacionais, como "a propensão a se tornar vulnerável a uma pessoa ou empresa ao revelar informações pessoais" (Richards; Hartzog, 2016, p. 449), mostrar-se-á malferida sempre que agentes de tratamento deixarem de proceder com lealdade relativamente aos titulares de dados pessoais. Isso poderá ocorrer, por exemplo, quando, prevalecendo-se da vulnerabilidade dos indivíduos, lancem mão de técnicas de manipulação a partir do *design*, de sorte a facilitar a *extração* de dados pessoais e frustrar o *exercício* de direitos[338].

O paradigma da confiança propõe, portanto, **uma tutela *substancial*** das relações informacionais, nos quais o eixo epistemológico se *desloca* do dado pessoal (e da adequação formal de seu tratamento) em direção às dinâmicas de poder e às assimetrias subjacentes a tais relações, marcadas, sobretudo, pela confiança identificada na relação havida entre titulares e agentes de tratamento.

O reforço à proteção da confiança no contexto de relações informacionais auxilia, por um lado, na tutela substancial das vulnerabilidades individuais (o que, no paradigma do controle, se faz por meio da atribuição de direitos a serem exercidos pelos próprios titulares, como vimos) e, por outro, permite vislumbrar novos horizontes para as atividades econômicas pautadas na circulação de dados pessoais, na medida em que a confiança é um componente fundamental para o desenvolvimento de relações negociais éticas e sustentáveis[339].

No ambiente da proteção de dados pessoais, a incidência do paradigma da confiança envolve uma *filtragem epistemológica* de vetores dogmáticos centrais para regimes jurídicos de proteção de dados calcados no paradigma do controle. Em outros termos, são ressignificados, à luz da proteção da confiança, os pilares de confidencialidade, de transparência e de segurança, que passam a ser compreendidos, respectivamente, pelas noções de discrição, de honestidade e de proteção. Na proposta teórica formulada por Richards e Hartzog (2017, p. 1217),

> Incentivos legais significativos para ser honestas (em termos de melhor notificação de práticas de dados e violações de dados), discretas (em termos de nunca vender dados a terceiros, ao menos por padrão) e seguras (maior

[338] "[...] em nossa abordagem, a lealdade se manifestaria principalmente como uma proibição de projetar ferramentas digitais e tratar dados de uma forma que conflite com os melhores interesses do titular. Os coletores de dados vinculados a tal dever de lealdade seriam obrigados a agir no melhor interesse das pessoas que expõem seus dados e se envolvem em experiências online, mas apenas na extensão de sua exposição." (Richards; Hartzog, 2021, p. 966, tradução nossa)

[339] "Como a confiança é boa para os negócios, as empresas devem competir para serem as mais confiáveis. As empresas que ganham a confiança de seus usuários obterão mais informações e vendas. Os consumidores que confiam nas empresas terão menos motivos para fugir para concorrentes que podem ser menos confiáveis. O resultado final é que a economia da informação pode florescer enquanto ainda protege os consumidores. Todos ganham, exceto os não confiáveis". (Richards; Hartzog, 2016, p. 465, tradução nossa)

> responsabilidade por violações de dados) podem gerar maior confiança do que os sentimentos mistos que muitos indivíduos têm sobre grandes empresas de tecnologia. Mas a verdadeira virtude da teoria da confiança é o dever de lealdade, colocando os interesses do usuário humano em primeiro lugar sobre os interesses de curto e médio prazo da empresa, para que tanto o usuário quanto a empresa se beneficiem a longo prazo. (Tradução nossa)

Mais especificamente, a confidencialidade, compreendida em termos formais como o dever de não divulgar informações, dá lugar ao conceito mais amplo de *discrição*, que se contrapõe à ótica da proteção individual a partir de uma lógica essencialmente binária, consistente na dicotomia informação pública *versus* informação privada[340]. A discrição, em uma perspectiva contextual, centra-se mais na *eticidade* – e, consequentemente, na deferência à confiança do titular de dados pessoais – no compartilhamento de dados pessoais.

A transparência (art. 6º, VI, da LGPD), reduzida ao dever de divulgação de informações sobre as atividades de tratamento de modo claro e acessível – independentemente da efetiva compreensão do titular[341] – é relida, a partir do paradigma da confiança, como *honestidade*. Afinal, nessa perspectiva, o que se espera do agente a quem se confiam os dados pessoais é a exposição de informações ao titular de acordo com os fatos, sem jogos de palavras ou uso de expressões vagas e genéricas (que poderiam, numa perspectiva formal, atender ao princípio da transparência).

Espera-se que o agente exponha ao titular a realidade das práticas de tratamento que serão por ele implementadas, de sorte a informá-lo de modo *significativo* sobre as consequências do uso de sua plataforma digital. Aqui, portanto, o eixo se desloca do mero dever de *informação*, verificado a partir da disponibilização de informações claras sobre o tratamento, para o dever de *honestidade*, que envolve uma postura mais proativa do agente[342], no sentido de se expor até mesmo as *verdades inconvenientes* sobre as consequências do uso dessa ou daquela tecnologia. Como esclarecem Richards e Hartzog (2016, p. 464),

---

[340] "Normas sobre privacidade deveriam adotar a discrição, que reflete as linhas nebulosas e contextuais entre 'público' e 'privado'. Reguladores, legisladores e juízes devem criar algum tipo de obrigação para os agentes de tratamento de ofuscar as informações reveladas de modo que o público em geral ou partes especificamente não autorizadas dificilmente as encontrem ou entendam, mesmo quando a relação informacional não for estritamente confidencial." (Richards; Hartzog, 2016, p. 461, tradução nossa)

[341] "A ideia é que se as empresas forem transparentes, as pessoas estarão cientes dos riscos de exposição e interação no mundo digital. Mas é claro que esse *ethos* é usado com muita frequência em políticas de privacidade densas como uma ficção para explorar as pessoas sob um fino verniz de conformidade de uma forma que pouco faz para mantê-las seguras ou realmente notificadas. Se as empresas devem manter a confiança que receberam, não basta serem meramente e passivamente 'abertas' ou 'transparentes'". (Richards; Hartzog, 2020b, p. 1747, tradução nossa)

[342] Como lembram Richards e Hartzog (2017, p. 1214), agentes de tratamento "confiáveis são honestos porque nos explicam os termos sob os quais eles mantêm e usam nossos dados. A honestidade coloca a obrigação de ser compreendido no controlador, em vez de em nossa capacidade de examinar a linguagem densa, vaga e multifacetada das políticas de privacidade e termos de serviço" (tradução nossa).

> Um foco na confiança pode remediar os problemas com políticas de privacidade como ferramentas para consumidores. Embora seja uma coisa para uma empresa estar obrigada a listar nas letras miúdas as maneiras pelas quais coletar e compartilhar informações das pessoas, outra completamente diferente para uma empresa é ser obrigada a admitir: "Você não pode confiar que seremos discretos, honestos, leais ou protetores". Indicações de confiança são mais intuitivas e úteis para os consumidores do que recitações secas de quais tipos de informações são coletadas e garantias vagas de que informações pessoais serão divulgadas apenas para "afiliados de terceiros".

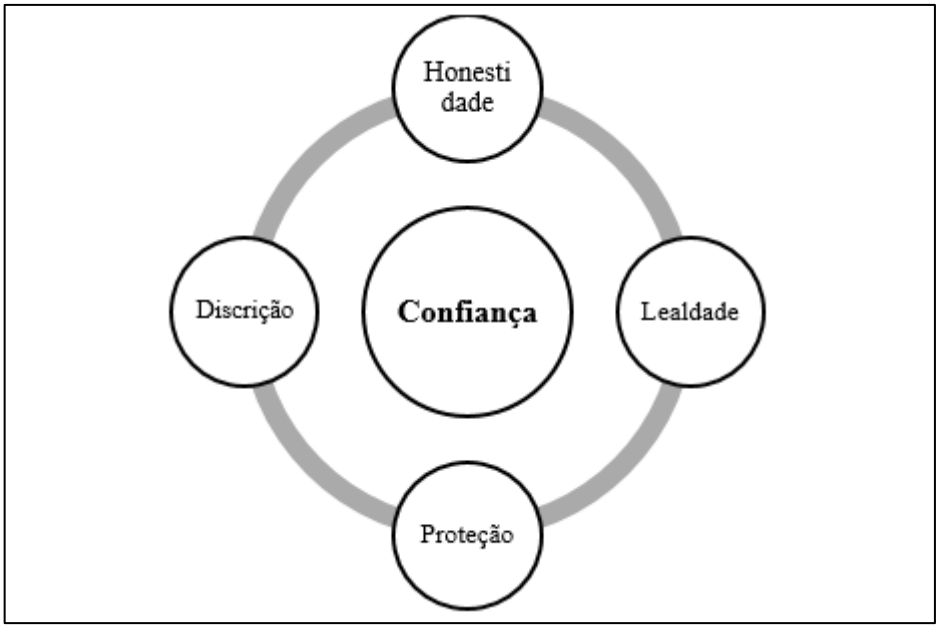
Em terceiro lugar, o paradigma da confiança impõe a releitura da segurança (art. 6º, VII, da LGPD) como *proteção*, impondo-se não a mera demonstração objetiva da adoção de cautelas técnicas e operacionais contra incidentes de segurança da informação, mas, sim, a adoção de uma postura de *guardião* dos dados pessoais (Richards; Hartzog, 2016, p. 466), além se conceber o dever dos agentes de tratamento para além da ocorrência de incidentes de segurança ("acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão", nos termos do art. 6º, VII, da LGPD), estendendo-se para situações em que os danos atinjam diretamente a pessoa humana, individual ou coletivamente, e não apenas seus dados pessoais (Richards; Hartzog, 2020, p. 1749).

O paradigma da confiança impõe, ainda, um dever explícito de *lealdade* aos agentes de tratamento, caracterizado, em síntese, pela vedação à implementação de tecnologias e ao tratamento de dados pessoais de modo conflitante com o *melhor interesse* dos titulares de dados pessoais, nos limites do relacionamento estabelecido entre as partes.

Em outras palavras, o dever de lealdade caracteriza-se pela **proibição de comportamentos oportunistas à custa dos titulares de dados pessoais** (*dimensão negativa*) e pelo mandamento de atuação dos agentes de tratamento em favor da **promoção de seu melhor interesse** (*dimensão positiva*). A propósito, na lição de Mattietto (2021, p. 143), "[a] lealdade sintetiza todo um conjunto de qualidades positivas (probidade, veracidade, honestidade, fidelidade, comprometimento, responsabilidade), que reconduzem ao padrão médio tido como correto na vida em sociedade e saudável para o tráfego negocial".

A fim de bem sistematizar a noção de confiança no paradigma ora proposto, interessante recorrer ao diagrama abaixo, que evidencia os deveres que gravitam em torno do conceito central de que se cogita:

Figura 1 – Deveres anexos estruturantes do dever geral de confiança nas relações informacionais



Fonte: elaborado pelo autor.

Dada a sua destacada relevância para a tutela substancial das partes vulneráveis nas relações informacionais (os titulares de dados pessoais), trataremos do princípio da lealdade, com maior detalhamento, no item a seguir.

4.2 O dever de lealdade dos agentes de tratamento: a proteção de dados pessoais enquanto tutela substancial (e não procedimental) da privacidade e da autonomia individual

Situar dogmaticamente a confiança no centro da proteção à privacidade enseja a identificação de *deveres* relacionados à tutela dos interesses da parte que divulga suas informações pessoais (e, portanto, deposita em outrem a confiança de que suas informações não serão utilizadas de modo oportunista). Tais deveres serão tão mais intensos quanto maior seja o dano potencialmente causado pela divulgação – ou pelo uso indevido, em termos mais amplos – da informação confiada.

Nessa ordem de ideias, a consideração de *assimetrias* informacionais[343] e de poder nas relações informacionais, bem como o reconhecimento de uma *dependência* do titular com

[343] "O direito fiduciário tem tradicionalmente trabalhado para permitir a confiança em relações caracterizadas por desequilíbrios de poder, conhecimento e controle, protegendo os indivíduos da exploração e fornecendo-lhes mecanismos legais para impor a confiança que depositam em seus fiduciários. Com algumas adaptações, acreditamos que ele pode desempenhar um papel semelhante na moderna economia da informação." (Filler; Haendler; Fischer, 2021, p. 6, tradução nossa)

relação ao agente de tratamento[344] (perspectiva substancial), atraem para o campo da proteção de dados pessoais a noção de *deveres fiduciários*[345].

Trata-se, de modo geral, de deveres inerentes à boa-fé com que deve se conduzir o fiduciário (neste caso, o agente de tratamento), considerando-se a confiança nele depositada pelo fiduciante (isto é, o titular de dados pessoais). Tal plexo de deveres pode ser resumido ao mandamento geral de que o fiduciário não se prevaleça da posição privilegiada que ostenta na relação jurídica para agir contra os interesses daquele que nele confiou. Espera-se, assim, que tais deveres cumpram a função precípua de colocar o fiduciante a salvo de possíveis comportamentos oportunistas (Brennan-Marquez, 2015, p. 651) que venham a ser praticados pelo agente fiduciário, bem como de estabelecer padrões éticos de conduta pelas partes de uma determinada relação informacional na qual haja assimetrias de poder.

Considerado o papel preponderante da informação na relação advogado-cliente, a doutrina menciona, como exemplo de *fiduciários informacionais*, os advogados, que têm acesso, por força da execução de um contrato (seja de representação em juízo, seja de prestação de atividade consultiva), a informações sobre seus clientes. Não raro, tais informações revelam vulnerabilidades que permitem o exercício indevido de poder (como a coação, por exemplo) sobre seu titular[346]. Além da vulnerabilidade inerente ao risco de lesão decorrente do uso desleal de tais informações, o cliente mantém com o advogado uma relação de dependência, na medida em que a este compete – no mais das vezes – o manejo das técnicas necessárias para o bom desempenho de seu mister.

A assimetria, portanto, não se revela apenas pelo conhecimento de informações pessoais cuja utilização desleal possa causar lesões ao cliente, mas, também, pelo domínio do conhecimento técnico por apenas uma das partes da relação informacional. O mesmo se pode

---

344 "[...] as pessoas dependem cada vez mais de uma ampla gama de serviços digitais que as observam e coletam dados sobre elas. Isso torna as pessoas cada vez mais vulneráveis a essas empresas. Como as operações das empresas não são transparentes, as pessoas precisam confiar que esses serviços não as trairão ou as manipularão para seus próprios fins. As empresas digitais que criam e mantêm essa dependência e vulnerabilidade devem ser consideradas fiduciárias informacionais em relação aos seus usuários finais." (Balkin, 2018, p. 12, tradução nossa)

345 "[...] o objetivo central dos deveres fiduciários é proteger contra a exploração de uma vulnerabilidade criada pela confiança em outrem. Dessa perspectiva, as relações fiduciárias são o caso paradigmático para o direito que permite a confiança ao impor deveres como cuidado, lealdade e confidencialidade. Portanto, não deve ser surpresa que a maioria, se não todas as relações fiduciárias, também se encaixem na categoria maior que temos chamado de "relações informacionais." (Richards; Hartzog, 2016, p. 457)

346 "Essas relações são marcadas pelo cliente confiando no fiduciário com informações sensíveis, de modo que o fiduciário pode fornecer um serviço que requer habilidades ou conhecimento especializado, e que o cliente geralmente não pode executar por si mesmo. A dificuldade resultante de supervisão cria um incentivo para o fiduciário abusar da confiança do cliente." (Barrett, 2019, p. 1060, tradução nossa)

cogitar, por exemplo, da relação médico-paciente[347], ou da relação psicólogo-paciente. Em cada um desses casos, a atribuição de deveres fiduciários informacionais busca reequilibrar assimetrias de poder (e proteger a parte vulnerável) exatamente pela proteção da confiança. À vista disso, códigos de ética profissional estabelecem deveres de não utilização das informações a que tais profissionais tenham acesso em detrimento dos interesses de seus clientes.

Pode-se citar, nesse particular, o art. 2º, parágrafo único, VIII, "a", do Código de Ética e Disciplina da Ordem dos Advogados do Brasil, que impõe aos advogados o dever de se abster de "utilizar de influência indevida, em seu benefício ou do cliente". Nesse mesmo sentido, o art. 15 estabelece, expressamente, ao advogado, o dever de exercer o mandato judicial ou extrajudicial "no interesse do cliente". Relações informacionais marcadas pela existência de deveres fiduciários ensejam, portanto, a assunção de deveres de lealdade, de confidencialidade e de cuidado[348], na medida em que a utilização da informação deve, sempre, ocorrer em benefício de seu titular.

A doutrina dos deveres fiduciários aplicados às relações informacionais surge da literatura norte-americana, a partir de um cenário caracterizado não apenas pela inexistência de uma lei geral a respeito do tema da proteção de dados pessoais, mas pela perspectiva, marcadamente liberal, do livre tratamento de dados pessoais no contexto de atividades econômicas, salvo quando houver disposição expressa em sentido contrário. A fim de conter abusos decorrentes das graves disparidades de poder, sobretudo no contexto das plataformas digitais, foi necessário cogitar de instrumentos já consagrados na tradição jurídica norte-americana, como os deveres fiduciários.

Além da teoria dos deveres fiduciários informacionais, outras possíveis abordagens focadas nas assimetrias de poder foram articuladas pela doutrina norte-americana, valendo citar, também, as "cláusulas-padrão fiduciárias" (*fiduciary boilerplates*), propostas por Lauren

---

[347] "Os exemplos clássicos de fiduciários informacionais são médicos e advogados. Ambos coletam muitas informações pessoais sobre seus clientes; suas operações não são transparentes para clientes relativamente destreinados, e a capacidade dos clientes de monitorar profissionais é limitada por sua falta de treinamento. Os clientes divulgam informações sensíveis porque precisam de serviços e, como resultado, devem confiar em médicos e advogados. Médicos e advogados, por sua vez, têm obrigações de não criar conflitos de interesse com seus pacientes, zelar por seus interesses e não divulgar informações sobre eles que possam ser usadas em desvantagem do cliente. Acima de tudo, fiduciários profissionais devem agir de boa-fé em relação a seus clientes." (Balkin, 2017, p. 13, tradução nossa)

[348] "Os fiduciários informacionais têm três deveres básicos para com as pessoas cujos dados eles coletam: um dever de cuidado, um dever de confidencialidade e um dever de lealdade. [...] o objetivo de um modelo fiduciário é mudar a forma como as empresas digitais, incluindo empresas de mídia social, pensam sobre seus usuários finais e suas obrigações para com eles. Atualmente, os usuários finais são tratados como um produto ou uma mercadoria vendida a anunciantes. O objetivo do modelo fiduciário é fazer com que as empresas parem de ver seus usuários finais como objetos de manipulação [...]." (Balkin, 2021, p. 93, tradução nossa)

Scholz (2020); a "integridade contextual" (*contextual integrity*), de que tratam Helen Nissenbaum e Solon Barocas (2014); a regulação da privacidade a partir de normas de devido processo, sugerida por Danielle Citron e Frank Pasquale (2014) e, também, por Kate Crawford e Jason Schultz (2014); o "pragmatismo da privacidade" (*privacy pragmatism*), articulado por Fred Cate, Victor Mayer-Schönberger e Peter Cullen (2014); ou, ainda, a epistemologia da privacidade enquanto confiança (*privacy-as-trust*), de Neil Richards e Woodrow Hartzog, de que decorre a afirmação do dever de lealdade aos agentes de tratamento.

Tais abordagens, ainda que guardem entre si distinções conceituais, erigem-se, todas[349], sobre a consideração de aspectos *substanciais* das relações informacionais, situando a confiança dos titulares de dados pessoais como elemento central de uma dogmática mais consentânea com os desafios impostos pelo capitalismo de vigilância[350], em oposição ao modelo baseado em controle. Todavia, a opção pelo marco teórico proposto por Richards e Hartzog se justifica pela constatação de que o fluxo informacional é, de fato, importante para a manutenção e o desenvolvimento da economia digital, e que a incidência[351] de todo um plexo de obrigações fiduciárias aos agentes de tratamento pode se revelar oneroso e ineficiente.

Com efeito, não podem ser negligenciados os benefícios (e os ganhos de eficiência) decorrentes da incorporação de plataformas digitais à vida cotidiana – evidenciados, sobretudo, no período em que se abateu sobre o mundo a pandemia causada pelo vírus SARS-CoV-2 –, ao mesmo tempo em que não pode ser desconsiderada a *efetividade* da proteção de liberdades fundamentais da mais alta relevância para democracias liberais, diante dos riscos presentes no contexto das plataformas, não suficientemente endereçados pelo paradigma do controle.

Assim, têm razão Richards e Hartzog ao ponderarem, por um lado, que a imposição de deveres fiduciários pode "tornar a capacidade de uma empresa de coletar e usar dados pessoais

---

[349] "Este conjunto de trabalhos não é frequentemente mencionado na mesma frase. Mas deveria ser. Cada um desses autores reconhece que o paradigma do controle do direito à privacidade não pode proteger adequadamente as pessoas na economia digital de hoje. Cada um sugere uma maneira de preencher essa lacuna. Sua busca coletiva por um novo paradigma regulatório para lidar com as ameaças que a análise preditiva representa é uma das áreas mais empolgantes da doutrina sobre direito e política de privacidade hoje." (Hirsch, 2019, p. 27, tradução nossa)

[350] Como esclarece Haupt (2020, p. 34), o modelo fiduciário proposto por Balkin remove o foco do conteúdo da informação, posicionando-o sobre as relações sociais entre as plataformas e seus usuários.

[351] Para a teoria dos deveres fiduciários aplicados às relações informacionais, a incidência dos deveres fiduciários é estanque. É dizer: ou está caracterizada a relação de fidúcia e, portanto, far-se-á exigível o cumprimento de todas as obrigações a ela inerentes, ou não está, razão pela qual não haveria que se cogitar da incidência dos deveres de lealdade, confidencialidade e cuidado. Como pontuam Richards e Hartzog (2020b, p. 1746), "[...] as regras de confiança que estamos propondo têm uma aplicação mais ampla, para além da estrutura formalizada de fiduciários informacionais. Normas de confiança são certamente relacionais por natureza, mas não são necessariamente dependentes de relacionamentos formais para incidirem, muito menos da estrutura completa de deveres fiduciários." (tradução nossa)

bastante custosa, particularmente em escala" (2021, p. 966, tradução nossa) e, por outro, que "a lei não precisa enfrentar a escolha binária entre tratar relações informacionais como 'fiduciárias' ou 'desprotegidas'" (2016, p. 457, tradução nossa), na medida em que *todas* as relações informacionais pressupõem confiança, muito embora os deveres dela decorrente sejam variáveis, porque dependentes do contexto em que ocorrem.

Pode-se *promover* a confiança nas relações informacionais não pela imposição de deveres fiduciários, mas considerando-se a lealdade como um conceito fundamental à dogmática da proteção da privacidade (Richards; Hartzog, 2016, p. 458). Como já reconhecido pela própria ANPD – embora no âmbito da análise de hipótese legal específica[352] –, o dever de lealdade é fundamental à promoção da confiança significativa entre as partes de uma relação jurídica informacional, por meio, essencialmente, da prevenção contra comportamentos oportunistas (antiéticos, portanto) da parte mais poderosa, particularmente aqueles relacionados ao desenvolvimento e ao *design* de interfaces maliciosas e ao tratamento de dados pessoais confiados pelos titulares de dados pessoais (Richards; Hartzog, 2021, p. 969).

Os padrões obscuros, objetos de nossa investigação, revelam-se como exemplos claros de condutas desleais, lesivas à autonomia individual, no âmbito de relações informacionais. São, também, demonstrações eloquentes de aspectos não adequadamente endereçados pelo regime jurídico da proteção de dados pautado no paradigma do controle. É precisamente esse o ponto de Hartzog, Selinger e Hunawan (2024, p. 784):

> É um erro dos legisladores ignorarem o design das tecnologias da informação. Woodrow Hartzog argumentou que "[o] design está em todo lugar. Design é poder. Design é político." Quando os legisladores ignoram o design das tecnologias da informação, eles permitem que as empresas escapem da responsabilização por decisões de design maliciosas e negligentes que incentivam danos à privacidade e uma degradação geral da privacidade. (Tradução nossa)

Nesse sentido, considerando-se que o *design* de plataformas digitais pode ser moldado de forma a facilitar, por diversas maneiras (como no emprego de manipulação), a extração de dados pessoais, trata-se de expediente que revela o prevalecimento oportunista da confiança do titular, bem como da superioridade técnica, para que sejam atingidos interesses próprios, a partir da exploração de vulnerabilidades.

---

[352] "Em decorrência dos **padrões éticos** vigentes e do princípio da boa-fé previsto na LGPD, o tratamento de dados pessoais para fins de estudos e pesquisas deve sempre se pautar por parâmetros de transparência, correção e **lealdade, com a devida proteção à confiança** e às legítimas expectativas dos titulares." (ANPD, 2023, p. 56, grifo nosso)

Embora a lealdade – como preceito geral da proteção de dados pessoais sob o paradigma da confiança – possa ensejar a criação de variados deveres específicos, apropriados a cada contexto, ela se refere a deveres que, essencialmente, obstam o comportamento oportunista em prejuízo da parte vulnerável. Segundo Richards e Hartzog (2022, p. 365) os deveres de lealdade "estão de acordo com noções básicas de justiça e decência – se você tem poder sobre alguém que confia em você, não deve traí-lo ou manipulá-lo para servir aos seus próprios interesses" (tradução nossa).

Como também esclarecem os mencionados autores (2021, p. 990), "fatores como o propósito da relação, incluindo a razão pela qual a confiança é depositada; o que especificamente é confiado; os objetivos da parte que confia; e a discrição e o poder da parte confiada" (tradução nossa) ajudarão a compreender o que significa ser leal em um ou outro contexto[353]. De todo modo, a norma jurídica deve considerar que, quanto mais intensa a posição de vulnerabilidade em que se encontre o titular de dados pessoais, mais rígidos devem ser os deveres inerentes à lealdade que se espera das partes em que se confiou (Richards; Hartzog, 2021, p. 1006).

Nessa perspectiva, pode-se compreender que a **base de incidência** do dever de lealdade seria caracterizada por três elementos centrais (Richards; Hartzog, 2021, p. 968). Em síntese, sob o paradigma da confiança, o dever de lealdade recairá sobre os agentes de tratamento quando (i) haja um convite à confiança no contexto de uma relação informacional, (ii) feito pela parte que tenha controle sobre a mediação da agência (e sobre os dados pessoais) da parte vulnerável no ambiente digital, e quando (iii) a parte mais fraca revele suas vulnerabilidades, confiando que não sofrerá qualquer dano. Todos, como se nota, se fazem sentir no contexto do uso de plataformas digitais, como as redes sociais[354].

Cabe-nos, ainda, problematizar o marco teórico, a fim de discutir as potenciais repercussões e dificuldades de sua aplicação prática. Efetivamente, embora o dever de proceder

---

[353] "[...] a referência ao princípio da boa-fé enfatiza a necessária observância dos aspectos concretos de cada situação sob análise pois, a depender do tipo de relação entre o titular dos dados e os agentes de tratamento e as circunstâncias do próprio tratamento, distintos graus de confiança podem surgir." (Frazão; Carvalho; Milanez, 2022, p. 73)

[354] "Quem são os novos fiduciários informacionais na era digital? São organizações e empresas que coletam enormes quantidades de informações sobre seus usuários finais. Os usuários finais são transparentes para essas organizações, mas suas operações não são transparentes para os usuários finais, e é difícil, se não impossível, monitorar suas operações. Como resultado, essas organizações desfrutam de significativas assimetrias de conhecimento e poder sobre seus usuários finais. Essas empresas incentivam seus usuários finais a confiar nelas e a divulgar informações a elas, e os usuários finais devem confiar nelas para se beneficiarem dos serviços que essas organizações fornecem." (Balkin, 2017, p. 14, tradução nossa)

com lealdade no âmbito de uma relação contratual[355] não seja estranho ao ordenamento jurídico brasileiro[356], sua aplicação no âmbito específico do tratamento de dados pessoais pode suscitar perplexidades, à vista do contexto que subjaz às atividades econômicas intermedidas por plataformas digitais.

Nesse sentido, cabe ponderar, em primeiro lugar, que o dever de lealdade pode ser entendido como excessivamente **vago**. Afinal, lealdade é conceito juridicamente aberto e, portanto, carece de significação *ex ante*. Contudo, a abertura semântica do conceito de lealdade tem o mérito de, em primeiro lugar, orientar a elaboração de *standards* de conduta apropriados à realidade de uma miríade de atividades econômicas que se estruturam a partir do tratamento de dados pessoais; em segundo lugar, a amplitude conceitual da lealdade produz, como efeito, uma postura cautelosa das empresas, atentas ao risco de eventual sanção.

Quer-se com isso dizer que a imposição de um dever geral de lealdade no tratamento de dados pessoais promoveria uma postura preventiva por parte dos agentes de tratamento, em que o *excesso de cautela* com relação a eventuais condutas desleais seria preferível aos riscos inerentes à antijuridicidade da conduta. Por fim, como notam Richards e Hartzog (2021, p. 1013), alguma elasticidade é necessária, à vista das constantes modificações das tecnologias de coleta e tratamento de dados pessoais, para permitir uma constante atualização da norma jurídica. Ainda de acordo com os autores (2022, p. 367):

> [A lealdade] pode proteger os consumidores contra riscos digitais novos e emergentes. Os deveres de lealdade podem ir além das preocupações padrão de tratamento dados e danos tradicionais à privacidade. [...]. Os deveres de lealdade devem examinar como essas organizações têm incentivos para usar o poder que as informações humanas lhes dão de maneiras egoístas que entram em conflito com os melhores interesses de uma parte confiante. Os deveres elaborados dessa forma responderiam significativamente às preocupações sobre interfaces de usuário manipuladoras (às vezes chamadas de "padrões obscuros") [...], discriminação algorítmica e proteção contra terceiros e outros usuários durante o uso de um serviço. (Tradução nossa)

Por outro lado, no contexto de atividades econômicas, cogita-se da existência de deveres de lealdade dos agentes de tratamento com relação a indivíduos com **interesses conflitantes**.

---

[355] "No Brasil, o processo de redefinição da autonomia privada está indissoluvelmente ligado aos novos princípios contratuais, a saber, a boa-fé objetiva, função social e equilíbrio, que se somam – e redefinem – aos clássicos princípios da liberdade, relatividade e obrigatoriedade. Tradicionalmente considerados quase que exclusivamente em sua função inovadora e ordenadora, cuja aplicação era sempre subsidiária, condicionada à existência de uma lacuna das regras específicas, aos princípios passou-se a reconhecer força normativa: as normas encerrariam o gênero dentro do qual seriam espécies não apenas as regras, mas também os princípios." (Terra; Konder; Guedes, 2019, p. 3)

[356] Como bem registra Mattietto (2021, p. 137), "[a] proteção da confiança envolve o vínculo contratual, a partir das normas cogentes que visam a promover o equilíbrio das partes da relação jurídica, mediante a adoção de novos paradigmas interpretativos, a proibição da abusividade e a imposição de deveres aos contraentes, na perspectiva de prevenir riscos e reparar prejuízos".

Pense-se, por exemplo, no caso de acionistas das empresas que exploram plataformas digitais, de um lado, e em seus usuários, de outro, mencionado na crítica formulada por Khan e Pozen (2019, p. 504) à formulação teórica de Jack Balkin:

> Um fiduciário com lealdades nitidamente opostas oscila à beira da contradição. Na medida em que os interesses dos acionistas e usuários divergem, os executivos e diretores dessas empresas podem ser colocados na posição insustentável de ter que violar seus deveres fiduciários (para acionistas) [...] para cumprir seus deveres fiduciários (para usuários finais) sob o novo corpo de leis que Balkin propõe [...] que claramente prioriza o último conjunto de deveres. (Tradução nossa)

Todavia, tal como se dá em outras áreas sujeitas à regulação estatal – como a preservação ambiental, por exemplo –, não há que se cogitar da prevalência dos interesses dos acionistas das empresas em detrimento do que determina a lei. Isto é, num cenário em que se verificasse um "conflito" de interesses entre a preservação do meio ambiente e a maximização de lucros dos acionistas, (ao menos em teoria) sequer haveria espaço para indagações a respeito da postura a ser adotada pela empresa, dada a cogência e imperatividade da norma jurídica.

Por último, poder-se-ia objetar que a complexidade dos fluxos informacionais faz com que o problema da lealdade **não se limite** ao agente de tratamento que *colete* os dados pessoais, na medida em que os riscos à privacidade e à autonomia subsistem ao longo de todo o seu ciclo de vida (basta pensar, por exemplo, na figura dos *data brokers*, cuja existência não raro sequer é conhecida pelos titulares de dados pessoais).

Ocorre que, como pontuamos, o paradigma da confiança não é conflitante com a vigência das normas de cariz procedimental previstas pela LGPD (e que se aplicam, de modo amplo, aos agentes de tratamento, não se limitando àqueles que coletem os dados pessoais). Ademais, nada impede a transmissibilidade do dever de lealdade a todos os agentes de tratamento que tenham contato com os dados pessoais (Richards; Hartzog, 2021, p. 1017).

4.2.1 Pensando o contexto brasileiro: a boa-fé objetiva na LGPD e a aplicabilidade de uma nova epistemologia à proteção de dados pessoais

São, de fato, inegáveis as interseções entre o paradigma da confiança e a boa-fé objetiva, erigido à condição de princípio norteador da aplicação de todos os demais previstos no rol do art. 6º da LGPD. À luz do regime jurídico centralizado pela LGPD, a doutrina já vem compreendendo – acertadamente – que o princípio da boa-fé objetiva[357] impõe aos agentes de

[357] "A boa-fé estrutura-se de dois modos: como *standard jurídico*, modelo de comportamento abstraído da conduta social média da população, ou como norma jurídica, sob a forma de princípio, ou de cláusula geral ou norma específica. [...]. Por exemplo, o *standard* mais famoso é o do *bonus paterfamilias*. De acordo com Volansky, a

tratamento o uso dos dados pessoais de modo ético, probo e leal[358], de sorte a não frustrar as expectativas dos titulares de dados pessoais. Interessante, no ponto, transcrever a ponderação de Dobkin (2017, p. 4) sobre o conceito de *expectativas* no contexto de relações informacionais:

> Mesmo que os usuários não consigam articular exatamente como os provedores de serviços devem ou não usar seus dados, eles têm expectativas implícitas. Cada um de nós tem uma reação instintiva que nos diz quando uma empresa cruzou a linha: podemos não ter problemas quando a Uber lembra nosso endereço residencial para que possamos evitar digitá-lo toda vez que usamos o serviço, mas sentiríamos que nossa privacidade foi violada se a Uber fornecesse um banco de dados por meio do qual qualquer um poderia consultar nossos históricos de corridas. [...]. As expectativas e a tolerância dos usuários diferem nas margens, mas certas práticas provavelmente seriam amplamente consideradas como tendo cruzado a linha. E é importante que os provedores de serviços mantenham a confiança dos usuários, que 'pode evaporar em um instante se os clientes sentirem que seus dados estão sendo usados de forma inadequada ou não protegidos de forma eficaz'. (Tradução nossa)

Assim, um questionamento fundamental se impõe: se a LGPD já impõe, textualmente, a boa-fé objetiva (que tem, como um de seus deveres anexos, exatamente, a *lealdade*[359]) como princípio fundamental do regime jurídico de proteção de dados pessoais, que **utilidade** ou **necessidade** haveria em se adotar o paradigma da confiança?

Cumpre observar, em primeiro lugar, que o princípio da boa-fé objetiva, no contexto específico da proteção de dados pessoais, é ainda dependente de maior aprofundamento dogmático. A aplicabilidade da boa-fé objetiva ao tratamento de dados pessoais ressente-se, ainda, de certa vagueza conceitual, o que pode ensejar dois resultados indesejáveis: por um lado, a *sub-aplicação* do princípio, relegando-o a um papel meramente subsidiário ou supletivo, quando violações às normas do regime jurídico de proteção de dados pessoais não puderem ser diretamente solucionadas à luz de princípios dotados de maior densidade conceitual e normativa. Por outro lado, a aplicação *indiscriminada*, como se a boa-fé objetiva fosse um conceito posto e autoevidente, e, bem assim, fosse uma espécie de panaceia para todas as questões que envolvem o tratamento de dados pessoais.

---

boa-fé é um estado de conformidade às regras básicas, isto é, um estado de conformidade social constatado. Para Jaluzot, a boa-fé aproxima-se do conceito de bom pai de família, que, no direito dos contratos se trata do 'contratante de boa-fé'." (Tomasevicius Filho, 2020, p. 91)

[358] "[...] quando a LGPD estabelece que a boa-fé deve ser observada nas atividades de tratamento de dados pessoais, está impondo uma regra de conduta (boa-fé objetiva), ou seja, um padrão de comportamento leal, baseado em uma conduta proba e transparente, que se materializa a partir da observância dos interesses legítimos e das expectativas razoáveis do titular, no contexto de um tratamento que não lhe cause qualquer tipo de abuso, lesão ou desvantagem." (Frazão; Carvalho; Milanez, 2022, p. 740)

[359] Cabe referir à lição de Mattietto (2021, p. 137), para quem "[a] referência à lealdade corresponde a um conjunto de qualidades positivas: não apenas lealdade, mas também, mais amplamente, probidade, veracidade, honestidade, comprometimento, responsabilidade".

Em verdade, a boa-fé objetiva, de larga aplicabilidade na tradição jurídica brasileira, deve ser pensada especificamente à luz do contexto que subjaz ao tratamento de dados pessoais[360]. A adequação procedimental do tratamento – demonstrada, por exemplo, pela apresentação de testes de balanceamento ou relatórios de impacto – pode se traduzir, à luz do paradigma do controle, no cumprimento do princípio da boa-fé objetiva, muito embora evidências de adequação formal sejam meros *indícios* de que o agente de tratamento se portou de acordo com tal norma.

Em segundo lugar, a compreensão da boa-fé objetiva se dá à luz da epistemologia incidente sobre o regime jurídico de proteção de dados pessoais, e não o contrário. Quer-se com isso dizer que a boa-fé objetiva, embora princípio estruturante da "espinha dorsal" da LGPD, em sendo concebida de acordo com o paradigma do controle, poderá ser reduzida – como exemplificamos – a demonstrações de conformidade procedimental do tratamento de dados pessoais.

Assim, o paradigma da confiança desempenha função *mais ampla* na interpretação e integração do regime jurídico de proteção de dados pessoais, na medida em que traz para o cerne das preocupações da norma as relações de poder subjacentes às relações informacionais. Na ilustrativa lição de Richards e Hartzog (2021, p. 1002),

> o direito à privacidade estaria melhor como um todo se perguntássemos menos "os procedimentos para o tratamento de dados pessoais foram seguidos?" e perguntássemos, ao invés disso, "esse tratamento de dados pessoais realmente promove os melhores interesses do usuário humano?" (Tradução nossa)

Conquanto a boa-fé objetiva seja importante para a identificação de excessos cometidos por agentes de tratamento (isto é, usos de dados pessoais que excedam as legítimas expectativas dos titulares, que, como vimos, variam de acordo com o contexto), à luz do paradigma do controle, ela estará adstrita ao exame formal do tratamento, e não às dinâmicas de poder e de dependência a ele subjacentes. A disponibilização de informações a respeito das atividades de tratamento, nesse sentido, poderia afastar alegações de violação à boa-fé objetiva, na medida em que o titular teria tido a oportunidade de informar-se adequadamente sobre as consequências da atividade. Como vimos, o paradigma da confiança ressignifica o dever de transparência para

[360] "A expressão 'boa-fé' apresenta múltiplas significações e é semanticamente vaga e aberta – por isso mesmo, carece de concretização, tarefa essa que é sempre, e necessariamente, contextual. Como alerta Judith Martins-Costa, 'o conteúdo específico da boa-fé, em cada caso, está indissoluvelmente ligado às circunstâncias, aos 'fatores vitais' determinantes do contexto da sua aplicação'. No Direito Brasileiro [...], há farta bibliografia sobre a boa-fé objetiva e suas funções são bem definidas, apesar de sua vagueza semântica." (Terra; Konder; Guedes, 2019, p. 5)

o dever de honestidade, representando uma importante virada epistemológica no regime jurídico da proteção de dados pessoais, nesse particular.

Em terceiro lugar, embora a lealdade seja concebida pela doutrina como um dos deveres anexos da boa-fé objetiva[361], há tendência a que soluções para eventuais condutas antijurídicas à luz da proteção de dados pessoais sejam resolvidas, como pontuamos, a partir de uma aplicação mais próxima e imediata dos princípios da finalidade e da necessidade.

Ainda que tais princípios (previstos, respectivamente, nos incisos I e II do art. 6º da LGPD) sejam decorrências diretas da boa-fé objetiva[362], este princípio é dotado de contornos dogmáticos próprios, que requerem integração regulatória ou mesmo jurisprudencial. Assim, a importância de adotar-se o paradigma da confiança está, exatamente, em atribuir-se ao princípio da boa-fé objetiva um significado próprio à luz das relações informacionais. Como já reconheceu a ANPD, a boa-fé objetiva é um conceito "nebuloso"[363] e, desse modo, o paradigma da confiança pode oferecer densidade normativa ao *caput* do art. 6º da LGPD, que se revela como o ponto de contato natural de nosso regime jurídico com a epistemologia proposta.

Se um dos deveres anexos à boa-fé objetiva é o de lealdade, então é possível cogitar da incidência do paradigma da confiança aqui discutido. A partir da noção fundamental de que lealdade, no contexto das relações informacionais e da necessária proteção à privacidade e à autonomia, está em proscrever comportamentos oportunistas, havidos em ofensa ao melhor interesse dos titulares de dados pessoais, abre-se ao intérprete da norma jurídica importante via de superação do paradigma do controle, aproximando-se a proteção de dados pessoais da proteção substancial das liberdades fundamentais que ele falha em proteger.

Cabe notar, a propósito, que não se propõe – porque desnecessária – a criação de lei nova, ou mesmo a alteração parcial do texto da LGPD. Tampouco se propõe sejam abandonados os mecanismos de controle individual e as exigências de adequação procedimental, na medida

---

[361] Como observam Frazão, Carvalho e Milanez (2022, p. 75), "o princípio [da boa-fé objetiva] tem uma função expansiva, agregando ao tratamento de dados todos os deveres laterais que sejam necessários para a proteção da confiança dos titulares de dados".

[362] A propósito, a ANPD já reconheceu, no Relatório de Instrução n. 01/2024/CGF/ANPD, que "as operações de tratamento de dados pessoais devem ser realizadas pelo controlador **com observância dos deveres de lealdade** e de transparência **com o titular**, isto é, o controlador precisa orientar as suas ações com base nos interesses legítimos e expectativas razoáveis do titular, no contexto de tratamento que não lhe cause qualquer tipo de abuso, lesão ou desvantagem" (grifo nosso).

[363] No Relatório de Análise de Impacto Regulatório a respeito da construção do modelo regulatório previsto na LGPD com relação à aplicação de sanções administrativas e à metodologia de cálculo do valor-base das sanções de multa, assim se manifestou a ANPD: "É fato que o conceito da boa-fé é conceito nebuloso, cuja aplicação e correta interpretação deverão ser objeto de avaliação cuidadosa por aquele que interpretar a norma de forma a conferir previsibilidade e segurança jurídica ao administrado." (ANPD, 2022, p. 29)

em que são relevantes, muito embora insuficientes para conter a lógica de acumulação de poder característica do capitalismo de vigilância.

A proteção das liberdades individuais a partir de uma epistemologia da privacidade enquanto confiança, em verdade, vem ao encontro do arcabouço normativo já existente, de sorte a complementá-lo, e não implica o afastamento das regras existentes (embora se reconheça o seu papel secundário na proteção da autonomia e da privacidade no contexto de relações marcadas por graves assimetrias informacionais e de poder).

4.3 Legítimo interesse do controlador ou melhor interesse do titular?

A ampla inspiração da LGPD no modelo europeu se reflete, dentre outros elementos, na pressuposição elementar de que o tratamento de dados pessoais é, de regra, vedado, salvo se for amparado por alguma das hipóteses que, no caso brasileiro, estão previstas no rol estabelecido pelo art. 7º. Dentre todas as bases legais previstas pela LGPD, apenas o consentimento e o legítimo interesse (incisos I e IX, respectivamente) não estão – prévia ou conceitualmente – vinculadas a uma finalidade específica.

Portanto, caso o tratamento de dados pessoais não se enquadre em qualquer outra das hipóteses legais (como a proteção da vida ou incolumidade física, ou a proteção do crédito), restará aos agentes de tratamento obter o consentimento dos titulares ou, então, ser capazes de demonstrar a necessidade do tratamento para o atendimento de seus interesses legítimos (ou de terceiro). Consideradas as dificuldades inerentes ao consentimento[364], evidenciadas pelo contexto do capitalismo de vigilância e pelas críticas tecidas ao paradigma do controle, poder-se-ia estabelecer uma aproximação entre o paradigma da confiança e uma intensificação do recurso à hipótese legal do legítimo interesse, mesmo porque o uso de tal base legal pressupõe o respeito às *legítimas expectativas* dos titulares de dados pessoais (art. 10, II).

O *interesse* é definido, por nossa própria Autoridade Nacional de Proteção de Dados, como "um conceito amplo que abrange qualquer benefício ou proveito que resulta do tratamento de dados pessoais" (ANPD, 2024, p. 16). Esse mesmo interesse, todavia, deve ser

[364] Como bem pontua Scholz (2020, p. 175): "As limitações do consentimento não são surpreendentes quando consideradas no contexto histórico. O consentimento não é um elemento da formação do contrato. Em vez disso, no direito contratual clássico, o consentimento é uma característica da consideração, que essencialmente se resume à noção de que cada parte em uma troca contratual deve contribuir com valor em troca da promessa da outra. O consentimento ganhou destaque no debate específico que surgiu no final do século XX e início do século XXI porque a consideração caiu em desuso na análise acadêmica do contrato por ser muito indeterminada. Mas [...] o consentimento é potencialmente pelo menos tão indeterminado quanto a consideração, como uma questão de definição, mas sem a amarração que a consideração tem na noção de troca justa." (Tradução nossa)

qualificado como *legítimo*, o que, para tanto, requer a incidência concomitante de três condições: (i) a compatibilidade com o ordenamento jurídico; (ii) o lastro em situações concretas; e (iii) a vinculação a finalidades legítimas, específicas e explícitas (art. 10, *caput*, da LGPD).

Tal hipótese legal de tratamento de dados pessoais ostenta, de fato, destacada importância para o regime jurídico de proteção de dados pessoais, na medida em que tem o mérito de (i) prescindir do consentimento do titular, que deve ser restrito a hipóteses específicas[365], e de (ii) lançar sobre o controlador o ônus de demonstrar que a atividade de tratamento por ele conduzida a partir da base legal do legítimo interesse não ofende as legítimas expectativas dos titulares de dados pessoais, elemento que é especialmente relevante em se considerando o tratamento de dados pessoais a partir do paradigma da confiança. Afinal, o tratamento *leal* pressupõe, como vimos, o dever de não utilizar os dados pessoais de modo oportunista, de sorte a ofender os interesses dos titulares.

Sendo, assim, intuitiva a aproximação do paradigma da confiança com a base legal do legítimo interesse, poder-se-ia indagar se o que se pretende com a criação de *standards* de lealdade não seria mero efeito de uma incidência ampla da base legal do legítimo interesse (que, a propósito, já cumpriria, no regime jurídico brasileiro de proteção de dados pessoais, a função a que se propõe o paradigma da confiança).

Tal como se dá com relação ao princípio da boa-fé objetiva, o potencial protetivo da base legal do legítimo interesse – embora a sua relevância mereça ser ressaltada – também se torna comprometido a partir do paradigma do controle. Em primeiro lugar, porque a verificação da prevalência de direitos e liberdades fundamentais dos titulares de dados pessoais se dá a partir da demonstração retórica, por meio de testes de balanceamento de interesse legítimo, desviando-se o foco – que deveria ser primordial – da criação ou do potencial agravamento das vulnerabilidades caracterizam a posição dos titulares de dados pessoais.

Em segundo lugar, ainda que relevante o dever de balanceamento no uso da hipótese legal do legítimo interesse, trata-se de obrigação que, ao contrário do paradigma da confiança, não irá auxiliar na interpretação de outros deveres decorrentes do regime jurídico de proteção de dados pessoais. Da mesma forma, o emprego da base legal do legítimo interesse, sob a

---

[365] "[...] o consentimento é válido sobretudo quando somos solicitados a escolher raramente, quando os danos potenciais que resultam do consentimento são fáceis de imaginar, e quando temos os incentivos corretos para consentir conscientemente e seriamente. Quanto mais nos afastamos desse padrão de ouro, mais um consentimento em particular é patológico e, portanto, suspeito." (Richards; Hartzog, 2019, p. 1465, tradução nossa)

perspectiva procedimental que caracteriza o paradigma do controle, não será capaz de impor limites substantivos ou limitar o oportunismo de agentes de tratamento, desde que seja constatada a adequação da base legal à situação concreta. Como pontuam Richards e Hartzog (2021, p. 983):

> Infelizmente, mesmo esse conceito [de legítimo interesse], que requer um equilíbrio de interesses substantivos, é poroso o suficiente para acomodar muitos tipos de comportamento desleal. Uma empresa que "equilibra" privadamente seus próprios interesses com os de seus clientes humanos dificilmente colocaria os clientes em primeiro lugar quando suas práticas de dados não estivessem sendo examinadas. Além disso, esse padrão de equilíbrio geralmente não ajudaria na interpretação de outros deveres, não estabeleceria limites substantivos no *design* de tecnologias da informação ou limitaria de outra forma o oportunismo, desde que a base para o processamento de dados pessoais fosse sólida. (Tradução nossa)

Em terceiro lugar, na linha do destacado acima, cumpre notar que o paradigma da confiança ostenta um alcance *mais amplo* do que a base legal do legítimo interesse. O dever de considerar as legítimas expectativas dos titulares de dados pessoais ocorre, na topografia da LGPD, no contexto do emprego da base legal do legítimo interesse (art. 10, II). Muito ao contrário, os melhores interesses dos titulares de dados pessoais devem prevalecer em qualquer outra hipótese legal, inclusive quando seu consentimento tenha sido coletado.

Tem-se, em suma, que a abordagem proposta pelo paradigma da confiança, baseada na consideração do melhor interesse do titular, se mostra mais consentânea com o imperativo de tutela das vulnerabilidades havidas no contexto das relações informacionais do que a aplicação da base legal do legítimo interesse. Aliás, como bem lembram Richards e Hartzog (2022, p. 367),

> Termos tecnocráticos como "minimização de dados" e "interesses legítimos do controlador de dados" fazem pouco pela imaginação ou compreensão do público. Em contraste, a lealdade é clara, é fácil de entender e é potencialmente robusta o suficiente para contrabalançar alegações espúrias da indústria sobre a importância da "inovação" [...]. Ideias no estilo do RGPD, como exigir que as empresas passem por avaliações de impacto de proteção de dados, podem parecer instáveis e fracas, mas cada pessoa [...] provavelmente sabe como é ser traído. (Tradução nossa)

Embora as legítimas expectativas de que trata a LGPD se refiram ao tratamento de dados pessoais, o **conceito** de melhor interesse do titular envolve não apenas, sob uma perspectiva formal, o dado pessoal, mas, também, considera que a relação dos indivíduos com as plataformas digitais produz reflexos que se estendem para além do tratamento de seus dados

pessoais. Afinal, os impactos do uso de ditas tecnologias se refletem sobre seu tempo, sua atenção, suas emoções, sua reputação e suas próprias vulnerabilidades[366].

Assim, os melhores interesses dos titulares de dados pessoais extrapolam o âmbito de incidência da base legal dos interesses legítimos dos agentes de tratamento, bem como o conceito de legítimas expectativas, na forma prevista pelo art. 10, II, da LGPD. Na síntese de Dobkin (2017, p. 7), a que ora recorremos, os agentes de tratamento vulneram os melhores interesses dos titulares ao "(1) usar seus dados para manipulá-los; (2) usar seus dados para discriminá-los; (3) compartilhar seus dados com terceiros sem consentimento; ou (4) violar suas próprias políticas de privacidade" (tradução nossa).

A noção de melhor interesse do titular conduz o intérprete à avaliação do interesse legítimo identificado não apenas na adequação formal e na demonstração textual, mediante testes de balanceamento, de que não haverá prejuízos às legítimas expectativas dos titulares de dados pessoais (porque razoavelmente poderiam esperar este ou aquele tratamento). Muito ao contrário, inclui-se, numa avaliação *substancial* da relação informacional, a consideração ampla das vulnerabilidades envolvidas no tratamento de dados pessoais, e os seus prejuízos aos titulares para além da "surpresa" com relação a um ou outro tratamento realizado sem o seu consentimento prévio.

4.4 A criação de *standards* de conduta para os agentes de tratamento: uma agenda para a Autoridade Nacional de Proteção de Dados

Como observamos, o paradigma da confiança não é conflitante com as regras sobre as quais se estrutura o regime jurídico de proteção de dados pessoais estabelecido pela LGPD. Assim, cumpre notar, em uma perspectiva **propositiva**, que o legislador cometeu à ANPD o dever de editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade (art. 55-J, XVIII, da LGPD), razão pela qual a tutela da privacidade e da autonomia individual à luz da proteção à confiança pode ser implementada pela própria Autoridade no exercício de sua função criadora de normas específicas a respeito do tratamento de dados pessoais.

Mais do que isso, vale recordar que a ANPD é o órgão central de interpretação da LGPD (art. 55-K, parágrafo único) e, por tal razão, pode fixar entendimentos e editar guias orientativos que aproximem o regime jurídico de proteção de dados pessoais de uma perspectiva de tutela

[366] "A internet estimula um consumo compulsivo desenfreado, não apenas fornecendo maior acesso a drogas velhas e novas, mas também sugerindo comportamentos que, de outro modo, poderiam nunca nos ter ocorrido. Os vídeos não se tornam apenas 'virais'. Eles são literalmente contagiosos, daí o surgimento do meme." (Lembke, 2024, p. 33)

substantiva das relações jurídicas informacionais, abrindo-se campo à discussão institucional e pública a respeito dos contornos a serem atribuídos ao dever de lealdade na LGPD.

Como lecionam Richards e Hartzog (2021, p. 996), a **abordagem normativa** acerca do dever de confiança nas relações informacionais estrutura-se, essencialmente – consideradas as dimensões negativa e positiva do dever de lealdade –, sobre a edição de regras *proscritivas* (isto é, que proíbam atividades relacionadas ao tratamento de dados pessoais que ofendam os melhores interesses dos titulares[367]) e *prescritivas*, que estabeleçam a adoção de comportamentos consentâneos com uma postura leal[368].

Como exemplos de normas proscritivas, os autores mencionam (i) a vedação geral ao *design* e ao tratamento de dados pessoais que conflite com os melhores interesses dos titulares, "como base para uma série de regimes regulatórios, esforços de autorregulação e orientação ao público para encorajar e nutrir sua confiança" (Richards; Hartzog, 2021, p. 996, tradução nossa); e (ii) a invalidade de cláusulas de isenção de responsabilidade[369] pela implementação de *design* e pelo tratamento de dados que conflite com os melhores interesses dos titulares de dados pessoais.

Ainda na lição dos mencionados autores, a inserção do paradigma da confiança dar-se-ia por meio de uma *cláusula geral* instituidora do dever amplo de guardar comportamento leal (ou seja, de não tratar dados pessoais ou de não desenvolver interfaces digitais em de sorte a ofender a confiança da parte mais vulnerável). Esse dever primário de lealdade deve ser, naturalmente, densificado a partir de deveres subsidiários e refletir um compromisso substantivo contra comportamentos oportunistas no âmbito das relações informacionais (Richards; Hartzog; Francis, 2023, p. 1338). Por outro lado, normas mais especificas

---

[367] "Negócios digitais como Facebook, Google e Twitter coletam uma enorme quantidade de dados sobre seus usuários. Às vezes, eles fazem coisas com esses dados que ameaçam os melhores interesses dos usuários, desde permitir publicidade predatória e possibilitar discriminação até induzir vício e compartilhar detalhes sensíveis com terceiros. Plataformas online também podem desfavorecer seus usuários e o público em geral de inúmeras outras maneiras, incluindo facilitando a disseminação de desinformação e o assédio de certas categorias de palestrantes." (Khan; Pozen, 2019, p. 498, tradução nossa)

[368] "Na maioria dos casos, o dever de lealdade vai além de sua fundação proscritiva. Normalmente, ele é combinado com o dever fiduciário relacionado de cuidado (conduta prudente), dever de boa-fé (fidelidade e devoção ao beneficiário) e dever de divulgação (compartilhar informações precisas), para criar uma obrigação prescritiva de agir no melhor interesse do beneficiário. Novamente, a justificativa é proteger a parte vulnerável de comportamento oportunista. O conteúdo do dever de lealdade 'deve depender do potencial de oportunismo' ou abuso de poder; os 'deveres se tornam mais intensos à medida que o poder do fiduciário cresce.'" (Whitt, 2019, p. 19, tradução nossa)

[369] "Quando os deveres fiduciários são dispensados, transformando as relações fiduciárias em relações contratuais, a renúncia geralmente deve atender a condições que incluem notificação completa ao beneficiário, uma conclusão de que o beneficiário é capaz de vontade e julgamento independentes, consentimento claro e específico do beneficiário e justiça substantiva. Os tribunais que se deparam com coletores de dados tentando estender seus direitos além do que um titular de dados razoável concordaria podem recorrer a essas linhas de precedentes para se recusar a reconhecer tais 'acordos'." (Filler; Haendler; Fischer, 2021, p. 48, tradução nossa)

atribuiriam regras subsidiárias de lealdade consentâneas com o grau de vulnerabilidade a que se submetam os titulares de dados pessoais[370].

[370] "Essas regras de lealdade subsidiárias podem se aproveitar de e modelar versões de privacidade informacional a partir de deveres fiduciários não relacionados à privacidade, como divulgação, consentimento, responsabilidade pela propriedade (direitos de acesso e portabilidade), confidencialidade e o conjunto completo de princípios de práticas de informações justas. Isso aplicaria algumas das obrigações mais significativas impostas pelo GDPR." (Richards; Hartzog, 2022a, p. 377, tradução nossa)

CONCLUSÃO

A larga disseminação do uso de plataformas digitais viabilizou o surgimento de modos inteiramente novos de ser, estar e participar da vida em sociedade. Da busca individual por aceitação e validação à coletivização da construção do debate público, as plataformas são responsáveis pela intermediação de parcela significativa das experiências individuais, cada vez mais entrelaçadas ao uso de tecnologias da informação e comunicação.

A vida na sociedade algorítmica, complexa e multifacetada, é marcada por uma progressiva dominação da agência individual (e das decisões existenciais ínsitas à experiência humana) por algoritmos que se nutrem da extração massiva de dados pessoais para se aperfeiçoarem *no sentido técnico*. É dizer: o incremento qualitativo do algoritmo se mede, no mais das vezes, não pelos benefícios que pode trazer à humanidade, mas pela eficiência com que é capaz de captar, analisar e classificar dados pessoais e, a partir deles, predizer e interferir no comportamento individual, servindo-se aos interesses de quem quer que o tenha projetado.

Na sociedade algorítmica, *informação é poder*. O acesso à informação sobre os desejos, medos, anseios, segredos e aversões inerentes a todo indivíduo atribui às plataformas digitais a inédita capacidade de direcionar sub-repticiamente o comportamento humano de um modo tão sofisticado que, no mais das vezes, sequer nos damos conta de que nossa conduta e nossas decisões no mundo digital não correspondem exatamente a uma expressão autêntica de nossa vontade mas, sim, do exercício de um poder brando viabilizado por tecnologias especificamente concebidas para que nos tornemos verdadeiras unidades geradoras de uma valiosa *matéria-prima informacional*.

Nesse contexto, *profiling*, *microtargeting*, *data mining*, *surveillance*[371] – dentre outros conceitos – são elementos que se assomaram a uma nova gramática da proteção das liberdades individuais, considerada a simbiótica relação entre a vida humana e as plataformas digitais. Cogita-se, diante de horizontes completamente novos ao exercício do poder, de riscos igualmente inimagináveis poucas décadas atrás. Diante do ubíquo espelho de um lado só, os indivíduos têm acesso a não mais do que um recorte limitado a respeito da forma como suas informações são coletadas e serão utilizadas – mesmo por empresas cuja existência se ignora – de forma nem sempre (ou quase nunca) compatível com seus próprios interesses.

[371] Perfilamento, microdirecionamento, mineração de dados e vigilância, respectivamente (em tradução livre).

Apesar disso, novas tendências, novos dispositivos, novos assistentes virtuais, novas plataformas, novos modos (pretensamente gratuitos) de acesso ao entretenimento e à informação convidam as pessoas a entregar cada vez mais aspectos de suas vidas ao escrutínio de agentes econômicos com relevantes interesses comerciais na extração massiva e na *comodificação* dessas informações. A autonomia, bem como a privacidade, está sob perigo.

Considerado esse contexto, identifica-se, na figura dos padrões obscuros, um exemplo eloquente das novas fronteiras de exercício do poder nos ambientes digitais. Padrões obscuros se voltam, essencialmente, à instrumentalização da agência humana, de forma que os usuários de plataformas digitais já não são mais os *produtos* ou sequer os *produtores* da matéria-prima essencial a esse novo modelo econômico. A partir do hábil manuseio do *design* das plataformas, indivíduos são reduzidos à condição de *ferramentas* necessárias ao atingimento de finalidades políticas ou econômicas. Não por outra razão, na economia movida a dados, têm vantagem competitiva os agentes econômicos mais capazes de manipular o comportamento humano, e não propriamente aqueles que ofereçam os melhores preços, serviços ou produtos ao mercado.

A objetificação dos usuários, no ambiente digital, equivale à própria negação da autonomia (e, bem assim, à antítese da promoção da dignidade da pessoa humana). A partir de noções precisas do comportamento humano, padrões obscuros servem como formas de induzir escolhas, criar estados de ansiedade, incentivar o vício (necessário à manutenção da coleta de dados pessoais), condicionar as escolhas individuais, dar aos usuários a falsa impressão de que, de fato, estão fazendo escolhas significativas e autônomas sobre a sua privacidade, ou mesmo desincentivar a busca pela tomada de decisões a respeito das atividades de tratamento a que serão submetidos os seus dados pessoais.

Os efeitos do emprego de tais técnicas de *design* de plataformas digitais – a serviço da extração massiva de dados pessoais – vêm se apresentando em âmbitos que extrapolam o ambiente formal das regras de proteção de dados. O uso compulsivo de redes sociais criou uma *geração ansiosa* (Haidt, 2024) e uma *nação* engajada em uma busca incessante por *dopamina* (Lembke, 2022). A propósito, em dezembro de 2024, *brain rot* (“apodrecimento do cérebro”, em tradução livre) foi eleita a *Oxford Word of the Year*. O termo designa, essencialmente, a degradação de faculdades mentais essenciais à cognição – como a atenção, a memória e o autocontrole – causada pelo vício na visualização rápida (e virtualmente infinita) de conteúdos apelativos, trágicos, engraçados, revoltantes, propagados nas redes sociais. Os dados pessoais já não são mais o único preço a se pagar. Usuários – especialmente os mais jovens – pagam com a atenção, com a saúde mental, com o tempo de vida desperdiçado.

Diante desse cenário, cabe ao Direito a árdua missão de reconduzir o indivíduo ao centro da ordem jurídica, assegurando-se e reafirmando-se o seu valor intrínseco, inerente à própria condição humana. Com efeito, desde o surgimento dos bancos de dados eletrônicos, a norma jurídica tem se ocupado de conter o fenômeno da concentração desproporcional de informações (e, consequentemente, de poder) nas mãos de alguns poucos agentes econômicos ou estatais.

Diferentemente, contudo, do processo de produção da norma jurídica, decisões corporativas sobre o funcionamento das plataformas digitais – aí incluídas escolhas sobre moderação de conteúdo, sobre (des)incentivos à propagação de discurso de ódio, sobre a implementação de padrões obscuros – são tomadas com notável celeridade, assim como rápidas são as modificações inerentes ao contexto das tecnologias de comunicação e informação.

Incontornável, a propósito, a referência à recente mudança de posicionamento da Meta a respeito de sua política de moderação de conteúdo em suas plataformas de mídia social[372]. Motivadas pelo alinhamento com uma retórica apoiada na promoção da liberdade de expressão, as alterações a serem implementadas pela empresa – que envolvem a descontinuação do emprego dos verificadores de fatos (*fact-checkers*) – poderão causar graves repercussões sobre a disseminação da desinformação e do discurso de ódio. Tem-se, com esse episódio, uma demonstração eloquente do poder exercido pelas grandes plataformas digitais: as decisões das *big techs* (como a Meta), não sujeitas ao escrutínio público, infensas à deliberação democrática, projetam seus efeitos ao redor de todo o mundo, mostrando-se capazes de produzir profundos impactos sobre a higidez do debate público, a radicalização de conflitos sociais e, no limite, a estabilidade de governos democráticos.

Diante desse cenário, sempre tão surpreendente quanto cambiante, é necessário refletir sobre a efetividade dos instrumentos jurídicos postos a serviço da proteção da pessoa humana. Essa tarefa não prescinde da reflexão atenta sobre a própria forma de se pensar (e compreender) a proteção da privacidade e da autonomia. É dizer: no capitalismo de vigilância, o que significa proteger a privacidade e autonomia?

Leis de proteção de dados pessoais, herdeiras da tradição das *Fair Information Practices* (FIPs), concebem a privacidade em sua expressão dinâmica, reconhecendo-se que o conceito já

---

[372] Confira-se trecho da nota pública divulgada pela Meta em 7 de janeiro de 2025: "Agora estamos mudando essa abordagem. Encerraremos o atual programa de verificação de fatos de terceiros nos Estados Unidos e, em vez disso, começaremos a migrar para um programa de Notas da Comunidade. Vimos essa abordagem funcionar no X – onde eles capacitam sua comunidade a decidir quando as postagens são potencialmente enganosas e precisam de mais contexto, e pessoas em uma gama diversificada de perspectivas decidem que tipo de contexto é útil para outros usuários verem." Disponível em: https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/. Acesso em: 15 jan. 2025.

não pode mais ser compreendido unicamente como a simples delimitação de um âmbito indevassável da vida individual. Proteger a privacidade é, na perspectiva gestada no contexto europeu, conceber o fluxo de informações pessoais (e a sua virtude intrínseca, na perspectiva da inovação e da eficiência econômica) como um fato inescapável da realidade, mas, ao mesmo tempo, atribuir *controles* aos indivíduos para que façam escolhas (idealmente autônomas) sobre as formas como seus dados serão utilizados; é, também, estabelecer padrões a serem observados no tratamento de dados pessoais, de sorte que o *procedimento* também se revela como outro importante vetor de proteção da vida privada.

A atribuição de controles individuais se mostrava como mecanismo viável de tutela da privacidade nos primórdios da Internet; ademais, do ponto de vista epistemológico, compreende-se a tendência a relacionar a proteção da privacidade à atribuição de controles, na medida em que a autonomia, valor fundante das democracias liberais, é fortemente associada ao exercício de escolhas individuais. Se aumentam as ameaças à privacidade, dever-se-ia aumentar, consequentemente, o controle dos indivíduos (e, assim, o reforço à autonomia), de sorte a que sejam capazes de impor limites e restrições ao livre uso de seus dados pessoais.

Ocorre que o avanço implacável das tecnologias de informação e comunicação causou, mesmo em sociedades habituadas ao tema da proteção de dados – fruto de décadas de sedimentação de uma cultura de efetivo cuidado com o fluxo das informações pessoais –, uma superação das aptidões do controle individual como paradigma para a tutela das liberdades individuais, considerado o contexto do capitalismo de vigilância. Não por outra razão, tem-se percebido, nos últimos anos, uma inclinação legislativa em favor da proteção da confiança: no contexto europeu, o art. 1(1) do recente Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (AI Act) torna evidente o objetivo de definir "regras harmonizadas para um ambiente online seguro, previsível **e de confiança** que facilite a inovação e no qual os direitos [...] **sejam efetivamente protegidos**" (tradução e grifo nossos).

Se, na União Europeia, o paradigma do controle dá sinais de desgaste, com maior razão há de se cogitar de sua insuficiência diante do contexto brasileiro, marcado, como vimos na presente investigação, por preocupantes níveis de analfabetismo, desigualdades sociais, ausência de habilidades digitais básicas e pouco (ou nenhum) conhecimento a respeito da própria *existência* da Lei Geral de Proteção de Dados Pessoais. A análise do contexto de elaboração da Lei n. 13.709/2018 revela preocupação preponderante do legislador com o alinhamento a padrões internacionais, que tinham no RGPD o seu "padrão de ouro" (*gold standard*). Editar uma legislação inspirada largamente no modelo europeu, naturalmente, criaria

um ambiente de adequação formal no qual o fluxo de informações entre o Brasil e países integrantes da União Europeia pudesse ocorrer.

Todavia, o olhar atento do legislador para o cenário europeu – além das negociações e pressões políticas comuns ao processo legislativo – causou um comprometimento do modelo proposto para a grave e delicada temática da proteção de dados pessoais no Brasil. O paradigma do controle, gestado na tradição europeia, se erige sobre a figura idealizada de um *titular médio*, que é capaz de ler e compreender razoavelmente os riscos envolvidos no tratamento de dados pessoais; que está minimamente apto a manejar interfaces digitais para realizar escolhas significativas a respeito de sua privacidade; que não se constrange, em ambientes físicos (como supermercados ou drogarias), em apresentar objeções à coleta de seus dados pessoais, ao menor sinal de desconforto. Afinal, no contexto europeu, "o RGPD é um estado de espírito" (Richards; Hartzog, 2022a, p. 369). A imagem desse *titular médio*, como se vê, discrepa em larga medida da realidade do *brasileiro médio*.

Assim como o exercício do controle individual, a regulação do tratamento de dados pessoais – por meio de requisitos procedimentais como a prévia condução de análises de impacto ou de testes de balanceamento de interesses – se revela incapaz de efetivamente reduzir as gigantescas assimetrias de poder entre os usuários e as empresas que operam plataformas digitais. Quando a proteção da autonomia e da privacidade é *indireta*, opera-se uma indesejável separação entre *relação informacional* e *relação substancial*, sendo aquela limitada aos aspectos formais do tratamento, de que se ocupa a LGPD mais diretamente, e esta, a seu turno, marcada pelas dinâmicas de poder que envolvem a extração massiva de dados pessoais, o manejo de técnicas de *design* malicioso (como os padrões obscuros) e os prejuízos efetivos à autonomia e à própria vida humana, em sua acepção mais ampla.

Dados pessoais não são metafísica. Não transitam no vácuo ou em um ambiente imaginário, etéreo, descolado da realidade. A todo fluxo de informação humana subjaz uma relação igualmente *humana*, destinada a satisfazer uma ou mais necessidades inerentes à vida afetiva, à vida em sociedade, à dinamização das relações civis e comerciais, dentre outros vários objetivos havidos em relações nas quais a informação exerce um papel fundamental. Nesse cenário, a proteção da *pessoa humana*, sobretudo em se considerando a sua progressiva *objetificação* no contexto do capitalismo de vigilância (além da inimaginável concentração de poder nas mãos de agentes econômicos sobre os quais pouco efetivamente é sabido), não prescinde da consideração das *dinâmicas de poder* envolvidas nos fluxos informacionais.

Informação atribui poder a quem a detenha. Esse poder pode ser utilizado, dentre outras finalidades, para manipular, para constranger, para humilhar, para coagir, para viciar, para negar oportunidades de emprego, para aumentar ou diminuir preços de produtos ou serviços. Se os riscos e as consequências da concentração de imensos repositórios de informações pessoais nas mãos de algumas empresas são tão graves para a tomada de decisões existenciais autônomas, para a vida em sociedade, e para a própria democracia, combater esse novo Leviatã com a atribuição de direitos de acesso e oposição (dentre outros) aos indivíduos é fazer tábula rasa do fenômeno real e implacável do capitalismo de vigilância, da ubiquidade das plataformas (que tornam impossível um controle efetivo), da dependência, da unilateralidade do *design* das plataformas, que condicionam a agência humana, a ponto de causar – tanto nos titulares quanto no regulador – a impressão da conformidade.

Se informação é poder, a proteção dos dados pessoais deve ser enxergada sob as lentes da *confiança*, e não do controle. A comunicação de aspectos inerentes à vida humana pressupõe, de acordo com o contexto em que ocorra, maior ou menor grau de confiança do emissor com relação ao destinatário. Confiança é um aspecto fundamental ao florescimento das relações humanas e comerciais. Especialmente com relação àquelas, ambientes de confiança abrem campo fértil ao livre desenvolvimento da personalidade, à autodescoberta, à expressão das individualidades e à materialização de escolhas existenciais fundamentais. Em suma, à autonomia.

Foi com atenção a esse contexto que a presente investigação buscou responder a uma indagação fundamental: *em que medida uma epistemologia da proteção de dados pessoais baseada no paradigma da confiança poderia reforçar a proteção da autonomia individual no uso de plataformas digitais?*

Proteger a autonomia individual dos riscos inerentes ao uso das plataformas digitais, com especial enfoque à manipulação consubstanciada no emprego de interfaces maliciosas (padrões obscuros), não prescinde de uma epistemologia da proteção de dados pessoais pautada por um paradigma centrado na confiança.

Afinal, o paradigma da confiança traz para a regulação das relações informacionais a consideração da *hipervulnerabilidade*, da dependência e das assimetrias informacionais entre usuário e plataformas, circunstâncias que caracterizam a relação *substancial* em que se dão a coleta e o trânsito dos dados pessoais. Ao compreender a confiança como a propensão do titular de dados pessoais a se tornar vulnerável à ação daquele que passe a deter informações a seu respeito, o paradigma em comento lança luzes sobre os *deveres* do receptor (isto é, do agente

de tratamento), que decorrem da assunção de uma postura leal e, portanto, consentânea com a confiança que nele fora depositada (confiança essa que, aliás, ele mesmo induziu).

Essencialmente, o dever de lealdade impõe a adoção de um padrão de conduta compatível com a proteção dos melhores interesses do titular de dados pessoais. Ao passo que modelos de proteção de dados pessoais baseados em controles e, bem assim, em adequações procedimentais, olham diretamente para o cumprimento de requisitos formais relacionados ao tratamento (consentimento válido, princípio da necessidade, testes de balanceamento, etc.), a proteção de dados à luz da confiança busca proteger aquele que confiou seus dados pessoais contra usos oportunistas e auto-interessados do agente de tratamento. Ao assim fazer, efetiva-se, da mesma forma, a tutela material das liberdades fundamentais que a LGPD buscou resguardar.

Ao refletir sobre a potencial aderência do paradigma da confiança ao ordenamento jurídico brasileiro, a presente pesquisa constatou que a confiança é elemento consagrado na tradição jurídica nacional, sendo componente fundamental do conteúdo dogmático da boa-fé objetiva, de sorte a orientar a estruturação de institutos caros ao Direito Civil brasileiro, como o fideicomisso, a alienação fiduciária e a cláusula geral de vedação ao comportamento contraditório. Sem prescindir das contribuições oferecidas pelo paradigma do controle, a centralidade da confiança em uma nova epistemologia da proteção de dados pessoais se revela apropriada e oportuna ao enfrentamento dos desafios impostos pelo capitalismo de vigilância, dos quais não se pode furtar a norma jurídica.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Boletim de diagnóstico: habilidades digitais no Brasil e no mundo**. jun./2024. Disponível em: <https://agenciagov.ebc.com.br/noticias/202406/estudo-mostra-que-apenas-30-da-populacao-tem-habilidades-digitais-basicas>. Acesso em: 10 dez. 2024.

AKERLOFF, George; SHILLER, Robert. **Pescando tolos: a economia da manipulação e fraude**. Rio de Janeiro: Alta Books, 2016.

ALBERS, Marion. Realizing the complexity of data protection. In GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (eds.). **Reloading data protection: multidisciplinary insights and contemporary challenges**. Heidelberg: Springer, 2014, p. 213-236.

ALBUQUERQUE, Nathalia; VALENÇA, George; FALCÃO, Taciana Pontual. **Investigating manipulative design on social media platforms – the case of kidinfluencers**. Journal on Interactive Systems, 2024, vol. 15, issue 1, 2024, p. 1-15.

ALVES, Rainer Grigolo de Oliveira; FERNANDES, Marcia Santana; GOLDIM, José Roberto. **Autonomia, autodeterminação e incapacidade civil: uma análise sob a perspectiva da bioética e dos direitos humanos**. Revista de Direitos e Garantias Fundamentais, Vitória, b. 18, n. 3, p. 239-266, set./dez. 2017.

ANDRÉA, Gianfranco Faggin Mastro; ARQUITE, Higor Roberto Leite; CAMARGO, Juliana Moreira. **Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a lei geral de proteção de dados no Brasil**. Revista de Direito Constitucional e Internacional, vol. 121, p. 115-139, set./out. 2020.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo: cookies e proteção de dados pessoais**, versão 1.0. Brasília, out./2022.

_____. **Guia orientativo: hipóteses legais de tratamento: legítimo interesse**, versão 1.0. Brasília, fev./2024.

BALKIN, Jack. **Fixing social media's grand bargain**. Hoover Working Group on National Security, Techonolgy and Law, Aegis Series Paper no. 1814, 2018, p. 1-20.

_____. **Free speech in the algorithmic society: big data, private governance, and new school speech regulation**. University of California Davis Law Review, Forthcoming, 2017, p. 1-68.

_____. **How to regulate (and not regulate) social media**. Knight Institute Occasional Paper Series, vol. 71, issue 1, 2021, p. 71-96.

_____. **Information fiduciaries and the first amendment**. University of California, Davis, vol. 49, 2016, p. 1183-1234.

_____. **The fiduciary model of privacy**. Harvard Law Review Forum, vol. 134, issue 1, 2020, p. 11-33.

BANDURA, Romina; LEAL, Elena I. Méndez. **The digital literacy imperative**. Center for Strategic & International Studies Briefs, 2022, p. 1-6.

BARRETT, Lindsey. **Confiding in con men: U.S. privacy law, the GDPR and information fiduciaries**. Seattle University Law Review, vol. 42, 2019, p. 1057-1113.

BENTES, Anna. **Quase um tique: economia da atenção, vigilância e espetáculo em uma rede social**. Rio de Janeiro: Editora UFRJ, 2021.

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

BOTES, Marietjie. **Autonomy and the social dilemma of online manipulative behavior**. AI and Ethics, vol. 3, issue 1, 2023, p. 315-323.

BRENNAN-MARQUEZ, Kiel. **Fourth amendment fiduciaries**. Fordham Law Review, vol. 84, 2015, p. 611-659.

BRENNCKE, Martin. **Regulating dark patterns**. Notre Dame Journal of International & Comparative Law, vol. 14, issue 1, 2024, p. 1-41.

BRITZ, Gabriele. **Livre desenvolvimento da personalidade (art. 2 | 1 da Lei Fundamental da Alemanha) – promessa constitucional entre ingenuidade e temeridade?** Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 23-43, jul./dez. 2021.

BÜYÜKEREN, Berkeren; MAKARIN, Alexey; XIONG, Heyu. **The impact of dating apps on young adults: evidence from Tinder**. MIT Sloan Research Paper no. 6833, 2022, p. 1-72.

CALO, Ryan. **Digital market manipulation**. The George Washington Law Review, vol. 82, 2014, p. 995-1051.

CALONGA, Luiz Octavio Lanssoni; SOARES, Carla D. M.; MELO, Thiago Coelho de; MACHADO, Luciano Marchi. **Pensa que me engana, eu finjo que acredito: padrões obscuros sob a perspectiva do usuário**. XLVI Encontro da ANPAD – EnANPAD 2022, set./2022, p. 1-24.

CAMARGO, Gustavo Xavier de. **Dados pessoais, vigilância e controle; como proteger direitos fundamentais em um mundo dominado por plataformas digitais?** Rio de Janeiro: Lumen Juris, 2021.

CATE, Fred H. The failure of the fair information practice principles. *In* WINN, Jane K. **Consumer protection in the age of the "information economy"**. Londres; Nova Iorque: Routledge, 2006.

COHEN, Julie. **Examined lives: informational privacy and the subject as object**. Stanford Law Review, vol. 52, 2000, p. 1373-1437.

_____. **What privacy is for**. Harvard Law Review, vol. 126, 2013.

_____. **Law for the platform economy**. 51 U.C. Davis Law Review (forthcoming), 2017.

COFONE, Ignacio. **The privacy fallacy: harm and power in the information economy**. Nova Iorque: Cambridge University Press, 2024.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Shaping choices in the digital world: from dark patterns to data protection: the influence of ux/ui design on user empowerment**. IP Reports – Innovation and Foresight, n. 6, 2019.

CORRALES, Eluane de Lima; BERTONCINI, Carla. **O princípio da dignidade da pessoa humana como fundamento da justiça restaurativa a partir do pensamento de Immanuel Kant**. Revista Direitos Humanos e Democracia, ano 7, n. 14, jul./dez. 2019, p. 249-262.

CUSTÓDIO, Júlia de Moraes; GODOY, Henri Alves de. **Dark patterns: seria mesmo distração, ou o design foi pensado para ludibriar?** Revista Tecnológica da Fatec Americana, vol. 11, n. 1, 2023, p. 23-35.

DE MARCO, Cristhian Magnus; CASTRO, Matheus Felipe. **As dimensões e perspectivas do direito fundamental ao livre desenvolvimento da personalidade**. Prisma Jur., São Paulo, v. 12, n. 1, p. 13-49, jan./jun. 2013.

DOBKIN, Ariel. **Information fiduciaries in practice: data privacy and user expectations**. Berkeley Technology Law Journal, vol. 33, 2018, p. 1-50.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them**. Version 2.0, 2023.

FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital: por uma crítica hacker-fanoniana**. 1. ed. São Paulo: Boitempo, 2023.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. **Privacidade e proteção de dados pessoais: perspectiva histórica**. InCID: Revista de Ciência da Informação e Documentação, Ribeirão Preto, v. 12, n. 2, p. 151-172, set. 2021/fev. 2022.

FILLER, Daniel M; HAENDLER, David; FISCHER, Jordan. **Negligence at the breach: information fiduciaries and the duty to care for data**. Connecticut Law Review, Forthcoming, 2021, p. 1-55.

FORBRUKERRÅDET. **You can log out but you can never leave: how Amazon manipulates consumers to keep them subscribed to Amazon Prime**. 2021. Disponível em: <https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/>. Acesso em: 6 dez. 2024.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019a, p. 23-52.

_____. Objetivos e alcance da Lei Geral de Proteção de Dados. *In* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019c, p. 23-52.

_____. ***Data-driven economy* e seus impactos sobre os direitos da personalidade: indo além da privacidade e do controle aos dados pessoais**. Jota, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicaoempresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade>. Acesso em: 9 nov. 2024.

_____. **Direito ao livre pensamento na era digital: a necessária proteção das pessoas contra as múltiplas e variadas estratégias de manipulação**. *In* MENEZES, Joyceane Bezerra de; BARBOSA, Fernanda Nunes (coords.). A prioridade da pessoa humana no Direito Civil-Constitucional: estudos em homenagem a Maria Celina Bodin de Moraes. Indaiatuba: Foco, 2024, p. 3-23.

_____. **O mito da soberania do consumidor: é legítimo esperar que as soluções de mercado protejam o consumidor?**. Jota, 2021. Disponível em: <https://www.jota.info/opiniao-e-

analise/colunas/constituicao-empresa-e-mercado/o-mito-da-soberania-do-consumidor>. Acesso em: 13 dez. 2024.

_____. Plataformas digitais, *big data* e riscos para os direitos da personalidade. *In* TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de. **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019b, p. 333-349.

_____. Plataformas digitais e os desafios para a regulação jurídica. *In* PARENTONI, Leonardo (coord.); GONTIJO, Bruno Miranda; LIMA, Henrique Cunha Souza (orgs.). **Direito, tecnologia e inovação. Vol. 1**. Belo Horizonte: D'Plácido, 2018, p. 635-669.

_____. Proteção de dados e democracia: a ameaça da manipulação informacional digital. In FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio (coords.). **A Lei Geral de Proteção de Dados Pessoais: aspectos práticos e teóricos relevantes no setor público e privado**. São Paulo: Thomson Reuters, 2021, p. 739-762.

_____; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de proteção de dados pessoais: fundamentos da LGPD**. 1. ed. Rio de Janeiro: Forense, 2022.

_____; GOETTENAUER, Carlos. *Black box* e o direito face à opacidade algorítmica. *In* BARBOSA; Mafalda Miranda; BRAGA NETTO, Felipe; SILVA, Michael César; FALEIROS JÚNIOR, José Luiz de Moura (coords.). **Direito digital e inteligência artificial: diálogos entre Brasil e Europa**. Indaiatuba: Foco, 2021, p. 27-42. Revista de Direito Brasileira, Florianópolis, v. 24, n. 9, p. 168-182, set./dez. 2019.

FREITAS, Riva Sobrado de; MEZZAROBA, Orides; ZILIO, Daniela. **A autonomia decisória e o direito à autodeterminação corporal em decisões pessoais: uma necessária discussão**. Revista de Direito Brasileira, Florianópolis, v. 24, n. 9, set./dez. 2019, p. 168–182.

FRUGOLI, Alice Gomes; PRADO, Raquel de Souza; SILVA, Tercia Moreira Ribeiro da; MATOZINHOS, Fernanda Penido; TRAPÉ, Carla Andrea; LACHTIM, Sheila Aparecida Ferreira. ***Fake News* sobre vacinas: uma análise sob o modelo dos 3Cs da Organização Mundial da Saúde**. Revista da Escola de Enfermagem da USP, vol. 55, 2021, p. 1-8.

GONÇALVES, Maria Rita; DINIZ, Larissa. **O que a exclusão digital tem a ver com a desinformação no Brasil?** Instituto de Referência em Internet e Sociedade (IRIS), 2024. Disponível em: <https://irisbh.com.br/o-que-a-exclusao-digital-tem-a-ver-com-a-desinformacao-no-brasil/>. Acesso em: 10 dez. 2024.

GRISSE, Karina. Recommender systems, manipulation and private autonomy: how european civil law regulates and should regulate recommender systems for the benefit of private

autonomy. *In* GENOVESI, Sergio; KAESLING, Katharina; ROBBINS, Scott (eds.). **Recommender systems: legal and ethical issues**. Cham: Springer, 2023, p. 101-128

HAIDT, Jonathan. **A geração ansiosa: como a infância hiperconectada está causando uma epidemia de transtornos mentais**. 1. ed. São Paulo: Companhia das Letras, 2024.

HAN, Byung-Chul. **Infocracia: digitalização e a crise da democracia**. 1. ed. Petrópolis: Vozes, 2022.

HARARI, Yuval Noah. **Sapiens: uma breve história da humanidade**. 1. ed. São Paulo: Companhia das Letras, 2020.

HARTMANN, Gabriel Henrique; PATZ, Stéfani Reimann; PIAIA, Thami Covatti. **O impacto da autodeterminação informativa na proteção de dados pessoais e no direito ao esquecimento**. Revista Direito UFMS, Campo Grande, vol. 7, n. 1, p. 154-167, jan./jun. 2021.

HARTZOG, Woodrow. **The case against idealising control**. European Data Protection Law Review, vol. 4, 2018, p. 423-432.

_____. **The inadequate, invaluable fair information practices**. Maryland Law Review, vol. 76, 2017, p. 952-982.

_____; SELINGER, Evan; GUNAWAN, Johanna. **Privacy nicks: how the law normalizes surveillance**. Washington University Law Review, vol. 101, 2024, p. 717-789.

HAUPT, Claudia E. **Platforms as trustees: information fiduciaries and the value of analogy**. Harvard Law Review Forum, vol. 134, 2020, p. 34-41.

HAWLEY, Josh. **A tirania das big tech**. Campinas: Vide Editorial, 2022.

HEIMER, Carol Anne. Solving the problem of trust. *In* COOK, Karen S. **Trust in society**. Nova Iorque: Russell Sage Foundation, 2001.

HELBERGER, N,; SAX, M.; STRYCHARTZ, J.; MICKLITZ, H.-W. **Choice architectures in the digital economy: towards a new understanding of digital vulnerability**. Journal of Consumer Policy, vol. 45, 2022, p. 175-200.

HIRSCH, Dennis. **From individual control to social protection: new paradigms for privacy law in the age of predictive analysis**. Maryland Law Review, Forthcoming, 2019, p. 1-66.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathaniel; WAMBACH, Dietrich; AYENSON, Mika. **Behavioral advertising: the offer you cannot refuse**. Harvard Law & Policy Review, vol. 6, 2012, p. 273-296.

_____; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. **The European Union general data protection regulation: what it is and what it means**. Information & Communications Technology Law, vol. 28, issue 1, 2019, p. 65-98.

JANDREY, Claudio Luiz. **O uso de dark patterns na oferta de produtos e serviços em meios digitais: análise sob a perspectiva das normas de proteção de dados e do consumidor brasileiras**. 2023. Dissertação (Mestrado em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2023.

JAROVSKY, Luiza, **Dark patterns in personal data collection: definition, taxonomy and lawfulness**. 2022, p. 1-51.

JONES, Kyle M. L.; RUBEL, Alan; LECLERE, Ellen. **A matter of trust: higher education institutions as information fiduciaries in an age of educational data mining and learning analytics**. Journal of the Association for Information Science and Technology, Forthcoming, 2019, p. 1-24.

KAHNEMAN, Daniel. **Rápido e devagar: duas formas de pensar**. 1. ed. Rio de Janeiro: Objetiva, 2012.

KHAN, Lina M.; POZEN, David E. **A skeptical view of information fiduciaries**. Harvard Law Review, vol. 133, 2019, p. 497-541.

KIETZMANN, Jan; ANGELL, Ian. **Panopticon revisited**. Communications of the ACM, vol. 53, issue 6, 2010, p. 135-138.

KLENK, Michael; HANCOCK, Jeff. **Autonomy and online manipulation**. Internet Policy Review, 2019. Disponível em: < https://policyreview.info/articles/news/autonomy-and-online-manipulation/1431>. Acesso em: 16 nov. 2024.

KOOPS, Bert-Jaap. **The trouble with European data protection law**. Tilburg Law School Legal Studies Research Paper Series no. 04/2015, 2014.

KRAMER, Adam; GUILLORY, Jamie; HANCOCK, Jeff. **Experimental evidence of massive-scale emotional contagion through social networks**. Proceedings of the National Academy of Sciences of the United States of America, vol. 111, n. 24, 2014, p. 8788-8790.

LAGE, Fernanda de Carvalho. **Manual de inteligência artificial no Direito brasileiro**. 1. ed. Salvador: JusPodivm, 2021.

LASTOWKA, Greg. **Google's law**. Brooklyn Law Review, vol. 73, issue 4, 2008, p. 1327-1410.

LEE, Sun Kyong; SUN, Juhyung; JANG, Seulki; CONNELLY, Shane. **Misinformation of COVID-19 vaccines and vaccine hesitancy**. Scientific Reports, vol. 12, issue 13681, 2022, p. -1-11.

LEMBKE, Anna. **Nação dopamina: por que o excesso de prazer está nos deixando infelizes e o que podemos fazer para mudar**. 1. ed. São Paulo: Vestígio, 2022.

LU, Wencheng. **Inevitable challenges of autonomy: ethical concerns in personalized algorithmic decision-making**. Humanities and Social Sciences Communications, vol. 11, 2024, p. 1-9.

LUGURI, Jamie; STRAHILEVITZ, Lior. **Shining a light on dark patterns**. Journal of Legal Analysis, vol. 13, 2021, p. 43-109.

MACHADO, Débora. A modulação de comportamento nas plataformas de mídias sociais. *In* SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da; AVELINO, Rodolfo. **A sociedade de controle: manipulação e modulação nas redes digitais**. 2. ed. São Paulo: Hedra, 2021.

MATHUR, Arunesh; ACAR, Gunes; FRIEDMAN, Michael; LUCHERINI, Elena; MAYER, Jonathan; CHETTY, Marshini; NARAYANAN, Arvind. **Dark patterns at scale: findings from a crawl of 11k shopping websites**. Proceedings of the ACM on Human-Computer Interaction, vol. 3, issue CSCW, 2019, p. 1-32.

MARQUES, Claudia Lima; MUCELIN, Guilherme. **Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor**. Civilistica.com. Rio de Janeiro, a. 11, n. 3, 2022.

_____; MENDES, Laura Schertel; BERGSTEIN, Laís. **Dark patterns e padrões comerciais escusos**. Revista de Direito do Consumidor, vol. 145, ano 3, p. 295-316. São Paulo: Revista dos Tribunais, jan./fev. 2023.

MARTINS-COSTA, Judith. A boa-fé no direito privado: critérios para a sua aplicação. 3. ed. São Paulo: SaraivaJur, 2024.

MATTIETTO, Leonardo. **Sobre o princípio da boa-fé no Código Civil brasileiro de 2002: interpretação, correção e integração dos contratos**. Cadernos de Dereito Actual, n. 16, 2021, p. 133-145.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. **The cost of reading privacy policies**. I/S: A Journal of Law and Policy, vol. 4, n. 3, 2008, p. 540-565.

MENDES, Laura Schertel Ferreira. ***Habeas data* e a autodeterminação informativa: os dos lados da mesma moeda**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

_____. **Autodeterminação informativa: a história de um conceito**. Pensar, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

_____; BIONI, Bruno Ricardo. **O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência**. Revista de Direito do Consumidor, vol. 24, ano 28, p. 157-180, São Paulo: Revista dos Tribunais, jul./ago. 2019.

_____; FONSECA, Gabriel C. Soares da. **Proteção de dados para além do consentimento: tendências contemporâneas de materialização**. Revista de Estudos Institucionais, vol. 6, n. 2, p. 507-533, mai./ago. 2020.

MILLS, Stuart; COSTA, Samuel; SUNSTEIN, Cass. **AI, behavioural science, and consumer welfare**. Journal of Consumer Policy, vol. 46, 2023, p. 387-400.

NADLER, Anthony; MCGUIGAN, Lee. **An impulse to exploit: the behavioral turn in data-driven marketing**. Critical Studies in Media Communication, vol. 35, issue 2, 2018, p. 151-165.

NISSENBAUM, Helen. **Privacy in context: technology, policy, and the integrity of social life**. Stanford: Stanford Law Books, 2010.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2023**. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2024.

_____. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2020**. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2021.

_____. **Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil**. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2024.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy**. Reino Unido: Penguin Books, 2017.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Consumer vulnerability in the digital age**. OECD Digital Economy Papers, no. 355, 2023.

_____. **Dark commercial patterns**. OECD Digital Economy Papers, no. 336, 2022.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

OYADOMARI, Winston; COSTA, Ramon Silva; RIBEIRO, Manuella Maia. **Perspectivas da sociedade brasileira em relação à privacidade e à proteção de dados pessoais**. Panorama Setorial da Internet, ano 15, n. 2, jun./2023, p. 1-10.

PACTO NACIONAL DE COMBATE ÀS DESIGUALDADES. **Relatório do Observatório Brasileiro das Desigualdades**. Disponível em: < https://www.dmtemdebate.com.br/2024-relatorio-do-observatorio-brasileiro-das-desigualdades/>. Acesso em: 10 dez. 2024.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2016.

RICHARDS, Neil. **The GDPR as privacy pretext and the problem of co-opting privacy**. Hastings Law Journal, vol. 73, issue 5, 2022, p. 1511-1538.

_____. **The puzzle of Brandeis, privacy, and speech**. Vanderbilt Law Review, vol. 63, issue 5, 2010, p. 1295-1352.

_____. **Why privacy matters**. Nova Iorque: Oxford University Press, 2022.

RICHARDS, Neil; HARTZOG, Woodrow. **A duty of loyalty for privacy law**. Washington University Law Review, vol. 99, 2021, p. 961-1021.

_____. **A relational turn for data protection?** European Data Protection Law Review, vol. 4, issue 1, 2020a, p. 1-6.

_____. **Against engagement**. Boston University Law Review, vol. 104, 2024, p. 1151-1179.

_____. **Legislating data loyalty**. Notre Dame Review Reflection, vol. 97, issue 5, 2022a, p. 356-384.

_____. **Privacy's constitutional moment and the limits of data protection**. Boston College Law Review, vol. 61, issue 5, 2020b, p. 1687-1761.

_____. **Privacy's trust gap: a review**. The Yale Law Journal, vol. 126, 2017, p. 1180-1224.

_____. **Taking trust seriously in privacy law**. Stanford Technology Law Review, vol. 19, 2016, p. 431-472.

_____. **The pathologies of digital consent**. Washington University Law Review, vol. 96, 2019, p. 1461-1503.

_____. **The surprising virtues of data loyalty**. Emory Law Journal, vol. 71, issue 5, 2022b, p. 985-1033.

_____; FRANCIS, Jordan. **A concrete proposal for data loyalty**. Harvard Journal of Law and Technology, vol. 37, no. 3, 2023, p. 1335-1386.

RIEGER, Poliene Fernanda Souza Nascimento. **Privacidade mental e liberdade cognitiva: perspectivas e desdobramentos para novos direitos fundamentais no contexto de desenvolvimento e aplicação de neurotecnologia**. 2022. Dissertação (Mestrado em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODRÍGUEZ, Daniel Piñeiro. **O direito fundamental à proteção de dados: vigilância, privacidade e regulação**. Rio de Janeiro: Lumen Juris, 2021.

ROSTIÓN, Ignacio. **Sobre la ley de protección de la vida privada: la importancia de una "fuente legal" y su aplicación em las personas jurídicas**. Revista Jus et Praxis, ano 21, n. 2, 2015, p. 499-502.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 9. ed. rev. e atual. Porto Alegre: Livraria do Advogado, 2006.

_____. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020.

SCHEDELOSKI, Mariana Almirão Sousa. **Comércio de dados pessoais**. Rio de Janeiro: Lumen Juris, 2024.

SCHOLZ, Lauren Henry. **Fiduciary boilerplate: locating fiduciary relationships in information age consumer transactions**. The Journal of Corporation Law, vol. 46, 2020, p. 143-198.

SCHWARTZ, Paul. **Privacy and democracy in the cyberspace**. Vanderbilt Law Review, vol. 52, 1999, p. 1609-1701.

SILVEIRA, Sergio Amadeu da. A noção de exclusão digital diante das exigências de uma cibercidadania. *In* HETKOWSKI, Tânia Maria (org.). **Políticas públicas & inclusão digital**. Salvador: EDUFBA, 2008, p. 43-66.

SOLÍS, Edgar Esquivel. **A batalha dos gigantes – plataformas digitais: entre a manipulação e propaganda**. Contemporânea – Revista de Ética e Filosofia Política, v. 2, n. 5, set./out. 2022, p. 1051-1071.

SOLOVE, Daniel. **Introduction: privacy self-management and the consent dilemma**. Harvard Law Review, vol. 126, 2013, p. 1880-1903.

_____. **Privacy and power: computer databases and metaphors for information privacy**. Stanford Law Review, vol. 53, 2001, p. 1393-1462.

_____. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004.

_____. **The limitations of privacy rights**. Notre Dame Law Review, vol. 98, issue 3, 2023, p. 975-1036.

_____. **The myth of the privacy paradox**. The George Washington Law Review, vol. 89, issue 1, 2021, p. 1-51.

_____; HARTZOG, Woodrow. **Kafka in the age of AI and the futility of privacy as control**. Boston University Law Review, vol. 104, issue 1021, 2024, p. 1021-1042.

SPENCER, Shaun. **The problem of online manipulation**. University of Illinois Law Review, vol. 2020, issue 3, 2020, p. 959-1006.

SRNICEK, Nick. **The challenges of platform capitalism: understanding the logic of a new business model**. Juncture, vol. 23, issue 4, 2017, p. 254-257.

SUNSTEIN, Cass. **Fifty shades of manipulation**. Journal of Marketing Behavior, vol. 213, n. 1, 2016, p. 1-32.

_____; THALER, Richard. **Nudge: como tomar melhores decisões**. Rio de Janeiro: Objetiva, 2023.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. **Technology, autonomy, and manipulation**. Internet policy review: journal on internet regulation, vol. 8, issue 2, 2019a, p. 1-22.

_____. **Online manipulation: hidden influences in a digital world. Georgetown Law Technology Review**, vol. 4, issue 1, 2019b, p. 1-45.

TATEOKI, Victor Augusto. **O uso dos dados pessoais como mecanismo de persuasão no processo de tomada de decisão dos usuários de internet**. Rio de Janeiro: Lumen Juris, 2021.

TEPEDINO; Gustavo; TEFFÉ, Chiara Spadaccini de. **O consentimento na circulação de dados pessoais**. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

TERRA; Aline de Miranda Valverde; KONDER, Carlos Nelson; GUEDES, Gisela Sampaio da Cruz Costa. Boa-fé, função social e equilíbrio contratual: reflexões a partir de alguns dados

empíricos. *In* TERRA; Aline de Miranda Valverde; KONDER, Carlos Nelson; GUEDES, Gisela Sampaio da Cruz Costa (coords.). **Princípios contratuais aplicados: boa-fé, função social e equilíbrio contratual à luz da jurisprudência**. Indaiatuba: Foco, 2019.

_____; BALZ, John. **Choice architecture**. 2010, p. 1-20.

TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no Direito Civil**. São Paulo: Almedina, 2020.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT). **Manual for measuring ICT access and use by households and individuals**. ITU Publications, 2020.

_____. **Digital skills toolkit**. ITU Publications, 2018.

VÉLIZ, Carissa. **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**. 1. ed. São Paulo: Contracorrente, 2021.

VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camille. **Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológica do assédio de consumo**. Revista de Direito do Consumidor, vol. 119, ano 27, p. 349-384. São Paulo: Revista dos Tribunais, set./out. 2018.

_____; HOMCI, Janaina Vieira. **A responsabilidade civil por padrões obscuros estruturados por modelos algorítmicos**. Revista de Direito do Consumidor, vol. 156, nov./dez. 2024.

WALDMAN, Ari Ezra. **Industry unbound: the inside story of privacy, data, and corporate power**. Nova Iorque: Cambridge University Press, 2021.

_____. **Privacy as trust: information privacy for an information age**. Nova Iorque: Cambridge University Press, 2018.

_____. **Privacy, sharing and trust: the Facebook study**. Case Western Reserve Law Review, vol. 67, issue 1, 2016, p. 193-233.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, vol. 4, issue 5, 1890, p. 193-220.

WHITT, Richard S. **Old school goes online: exploring fiduciary obligations of loyalty and care in the digital platforms era**. Santa Clara High Tech Law Journal, vol. 36, 2019, p. 1-60.

WU, Tim. **Blind spot: the attention economy and the law**. Antitrust law journal, vol. 82, 2019, p. 771-806.

_____. **The attention merchants: the epic struggle to get inside our heads**. Londres: Atlantic Books, 2017.

YEUNG, Karen. **‘Hypernudge’: Big Data as a mode of regulation by design**. Information, Communication & Society, vol. 20, issue 1, 2017, p. 118-136.

ZAC, Amit; HUANG, Yu-Chun; VON MOLTKE, Amédée; DECKER; Christopher; EZRACHI, Ariel. **Dark patterns and consumer vulnerability**. Behavioural Public Policy, Forthcoming, 2023, p. 1-56.

ZARSKY, Tal. **Privacy and manipulation in the digital age**. Technical Inquiries in Law, vol. 20, issue 1, 2019, p. 157-188.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. 1. ed. Rio de Janeiro: Intrínseca, 2020.

_____. **Big other: surveillance capitalism and the prospects of an information civilization**. Journal of Information Technology, vol. 35, 2015, p. 75-89.