# CAPITALISMO DE VIGILÂNCIA E A LEI GERAL DE PROTEÇÃO DE DADOS: PERSPECTIVAS SOBRE CONSENTIMENTO, LEGÍTIMO INTERESSE E ANONIMIZAÇÃO

## SURVEILLANCE CAPITALISM AND THE GENERAL DATA PROTECTION LAW: PERSPECTIVES ON CONSENT, LEGITIMATE INTERESTS AND ANONYMIZATION

Ana Carolina B. Morellato[1]
André Filipe P. Reid dos Santos[2]

**RESUMO:** Este artigo objetiva contextualizar a implantação da recente Lei Geral de Proteção de Dados no Brasil dentro do paradigma de capitalismo de vigilância cujo processo de acumulação é pautado pela exploração mercadológica dos comportamentos humanos. Para tanto, utiliza-se do método de estudo exploratório e da revisão da bibliografia para compreender o consentimento, o legítimo interesse e a anonimização enquanto elementos centrais da regulação, expondo os seus limites e contrariedades. Argumenta-se que a abordagem contratualista do consentimento contribui para a lógica que mercantiliza o dado pessoal, falseando a sensação de segurança em virtude dos desequilíbrios de poder e informação existentes. A abertura dos conceitos que permeiam a hipótese do legítimo interesse e a não exigência de um relatório preliminar, por sua vez, podem resultar num passe livre para arbitrariedades, o que se acirra com a ausência de autonomia da Autoridade Nacional de Proteção de Dados. A anonimização, por seu turno, pode excepcionar a aplicação da lei, o que se mostra inócuo para mitigar práticas predatórias de publicidade abusiva ou marketing político. Ao final, conclui-se que, apesar da LGPD visar garantir a segurança jurídica desse novo mercado de dados, acende luz sobre um debate necessário para a reivindicação de uma tecnologia democrática.

**Palavras-chave**: Lei Geral de Proteção de Dados. Capitalismo de vigilância. Big data.

**ABSTRACT:** This article aims to analyze the new General Data Protection Law in Brazil within the bounds of the surveillance capitalism that commodifies the human behavior. It resorts the exploratory method and the bibliographic research in order to comprehend the limits and obstacles involved in consent, legitimate interests and anonymization, which are the prevailing topics of the current regulation. The contractual approach of consent contributes to the logic that transforms the user's data in commodities, creating a safety perception that is actually false. Meanwhile, the extent of the term "legitimate interests" and the absence of a preliminary report may cause arbitrary practices, and that is reinforced by the lack independency of the National Authority of Data Protection. The anonymization, on the other hand, can except the LGPD application, which is inefficient to reduce the predatory practices like abusive advertising and political marketing. In conclusion, we argue that, although the LGPD intends to warrant legal certainty in the operations of this new data economy, it amplifies a necessary debate to demand the right of a democratic technology.

**Keywords**: General Data Protection Law. Surveillance capitalism. Big data.

[1] Pesquisadora no grupo de pesquisa Direito, Sociedade e Cultura e discente em Direito pela Faculdade de Vitória (FDV).

[2] Professor-pesquisador do Programa de Pós-graduação em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória (FDV), Brasil. Doutor e mestre em Ciências Humanas pelo Programa de Pós-graduação em Sociologia e Antropologia da Universidade Federal do Rio de Janeiro (UFRJ), Brasil.

## 1 INTRODUÇÃO

Em 2016, o vazamento de informações sobre a venda de dados pelo Facebook para a Cambridge Analytica impactou o mundo e acendeu a discussão sobre a necessidade de regulação do tratamento de dados pessoais em vários países. Isso porque a violação da privacidade de milhões de cidadãos não se restringe a esse episódio que, por mais emblemático que seja, faz parte de um contexto global de reestruturação do capitalismo financeiro que se fundamenta na economia de dados.

A produtividade desse sistema e o seu principal ativo passou a residir na extração e utilização constante de dados pessoais dos indivíduos. É formado um complexo constituído por uma rede crescente e estruturada de monitoramento que dão lugar a novas formas de acumulação, o que se chamou de "capitalismo de vigilância" (ZUBOFF, 2015, 2019).

Buscamos nos apropriar da linguagem superficial que exclui a análise dos impactos e causas políticas, econômicas e sociais do debate que se supõe ser exclusivamente "digital" e "neutro", apropriando-se também de sua história imperfeita para interpretar o nosso objeto de análise (a Lei Geral de Proteção de Dados) dentro de um contexto de capitalismo de vigilância.

Para isso, lançamos mão do método de estudo exploratório e da pesquisa bibliográfica, com uma abordagem qualitativa, a fim de expor as determinações essenciais, as contradições e limitações envolvidas na regulação do tratamento de dados no Brasil.

Argumenta-se que a lei, na medida em que se fundamenta no desenvolvimento econômico e na livre iniciativa, inclusive com a proteção do segredo comercial e com uma abordagem meramente contratual e privada do consentimento, apesar da assimetria informacional existente, é um suporte jurídico flexível que viabiliza o fortalecimento do mercado de dados no Brasil, dentro da racionalidade neoliberal.

A despeito do consentimento despontar como a chave principal da LGPD na discussão jurídica atual, existem outras nove hipóteses nas quais os dados do usuário poderão ser coletados, das quais destacamos o legítimo interesse, devido à sua

probabilidade de vir a ser uma das bases legais mais utilizadas para o tratamento de dados, excepcionando o consentimento.

A anonimização também é um elemento importante da regulação, porque excepciona a própria aplicabilidade da LGPD, uma vez que o dado não será considerado pessoal, salvo quando o titular puder ser reidentificado, diante da falibilidade das técnicas mais populares.

Os conceitos jurídicos indeterminados (tais como "legítimo interesse") e as balizas de aplicação ainda precisam ser preenchidos por regulação da Autoridade Nacional de Proteção de Dados. No entanto, a independência do órgão se vê comprometida após a sua vinculação à Presidência da República, que inclusive nomeou militares para cargos de direção.

Ao final, conclui-se que, por um lado, a lei funciona como um instrumento para garantia da segurança jurídica da economia de dados ao tutelar essa extração enquanto uma mercadoria. Por outro, amplifica a importância de um debate necessário para que seja possível demandar uma tecnologia que seja verdadeiramente aberta e democrática.

## 2 A MONETIZAÇÃO DE DADOS SOB A ÉGIDE DO CAPITALISMO AVANÇADO

A pandemia da COVID-19 tem nos fornecido alguns elementos para pensar sobre o aprofundamento das dinâmicas do que a filósofa Shoshana Zuboff (2019, 2015) chamou de "capitalismo de vigilância", na medida em que o uso das tecnologias se intensificou por uma série de razões, dentre elas a necessidade de isolamento social, num primeiro momento.

Essas tecnologias fazem parte de um processo que foi necessário para a reestruturação global do capitalismo em sua nova fase a partir da década de 80, pautado por suas lógicas e interesses de produção e poder. Diferentemente do modo agrário ou industrial de desenvolvimento, a principal fonte de produção não advém substancialmente dos recursos naturais ou da mão de obra, mas da tecnologia da geração de conhecimentos e processamento de informações. Ou seja, o que é específico ao modelo informacional é "a ação de conhecimento sobre os próprios conhecimentos como fonte principal de

produtividade" (CASTELLS, 1999, p. 54), de modo que a própria informação se tornou o produto do processo produtivo.

A ascensão dessa nova mercadoria dos dados é explicitada pelo sociólogo Christian Fuchs (2013, p. 272) da seguinte forma: empresas de tecnologia investem dinheiro na estrutura tecnológica e em trabalhadores que produzirão serviços de social media que serão disponibilizados gratuitamente para os usuários, que por sua vez utilizarão essas plataformas para gerar conteúdo, aprimorando-as. O produto final é o conjunto de dados pessoais que é gerado a partir de uma série de operações sobre o comportamento online, que será vendido como um commodity para o setor de publicidade num preço maior do que o investido inicialmente.

Portanto, o capitalismo de vigilância se alimenta não somente do trabalho, mas de todos os aspectos das experiências humanas (ZUBOFF, 2019, p. 16), uma vez que o big data é constituído de fluxos que emergem de uma universalidade das tecnologias da informação que inclui desde informações bancárias a qualquer comportamento online e offline do indivíduo, formando uma complexa e crescente rede estruturada de monitoramento. Esses dados são adquiridos, codificados, generalizados, agregados, analisados, armazenados, vendidos, analisados e vendidos novamente num processo que os tecnologistas chamaram de "data exhaust", no intuito de que, a partir da redefinição dos dados enquanto um material excedente, a sua extração e monetização não seja contestada (ZUBOFF, 2015, p. 78).

O professor Marcondes Cesar (DE PIERRO, 2018, p. 24), pesquisador do Instituto de Matemática e Estatística da USP, aponta que o poder das grandes corporações depende justamente do big data acumulado e processado pelos seus algoritmos: "o que impede outra empresa de desenvolver um aplicativo da Uber? Isso já foi feito. Mas os dados que a Uber dispõe sobre o trânsito e o comportamento dos usuários acumulado ao longo do tempo pertencem apenas à empresa e são valiosos".

Essa lógica de extração constante é em si uma lógica de vigilância permanente e uma ameaça à democracia porque identifica ilimitadamente o padrão de comportamento das pessoas e os antecipa, tornando-os previsíveis e modificáveis, eliminando o risco nos processos decisórios do setor político e mercadológico. O capitalismo de vigilância tem se

mostrado eficaz não só para os novos ciclos de acumulação que pretende promover, mas para a anulação da autonomia do indivíduo:

> Por exemplo, imaginemos um plano de saúde[3] que, como condição para oferecer preços mais baixos, oferte ao cliente o uso ininterrupto de uma pulseira de monitoramento cardíaco. Antes, a empresa podia apenas recomendar ao cliente que se exercitasse três vezes por semanas por pelo menos 30 minutos ao dia para manter uma vida saudável pelo seu próprio bem. Com a pulseira, a sincronizar dados com os computadores da empresa diariamente, esta tem como estar certa de como o cliente se comportou, se fez exercícios ou não, verificando os batimentos cardíacos. Se o cliente não cumpriu o "recomendado" então os preços, automaticamente, sobem. O risco da empresa cai consideravelmente, pois dá preços mais altos aos sedentários, condição que ela verifica ao vigiar a que velocidade bate o coração do segurado (EVANGELISTA, 2017, p. 247).

Isso nos leva à conclusão que os dispositivos de vigilância dessa nova etapa do capitalismo produzem, naturalmente, efeitos substanciais sobre os mais pobres, sobretudo porque a publicidade predatória identifica os contextos de vulnerabilidade para estabelecer políticas de lucro sobre elas. Por exemplo, se um indivíduo está desesperadamente endividado ou sem dinheiro, surgirão anúncios de ofertas de empréstimos com altíssimas taxas de juros. Na educação, é oferecida uma falsa estrada para a prosperidade ao mesmo tempo em que as empresas do ramo calculam como maximizar sua receita a partir de cada caso, num loop de empréstimos e dívidas sem que o consumidor sequer saiba como determinado anúncio chegou a ele (O'NEILL, 2016, p. 64-65).

Esse paradigma se acirra quando pensamos que as grandes instituições internacionais como o FMI e o Banco Mundial impuseram ao Sul global a sua agenda político-econômica neoliberal, a fim de confinar os países em desenvolvimento, como o Brasil, no subdesenvolvimento. As lógicas empresariais se sobrepõem às da administração pública, de forma que o Estado passa a se compor hibridamente de empresas e a ter seus

[3] Nesse contexto, a Medida Provisória 869 de 28 de dezembro de 2018 já havia alterado a LGPD de modo a autorizar o uso de dados sensíveis para autorizar a troca de informações dos pacientes também entre as prestadoras de plano de saúde. Antes, a lei vedava a comunicação ou uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de vantagem econômica, exceto para os fins de portabilidade com o consentimento pelo titular. Hoje, a lei permite a obtenção de vantagem econômica nos casos da prestação de serviços de saúde, assistência farmacêutica e à saúde, desde que vedado o tratamento de dados para a seleção de riscos na contratação (art. 11, §§4º e 5º).

programas de ação desenhados e estabilizados por softwares e hardwares pensados a partir do modelo de eficiência mercadológico (DARDOT; LAVAL, 2016).

Apesar de não ser o único, o caso da Cambridge Analytica é um dos mais emblemáticos exemplos para se pensar o jogo político das economias digitais. Em 2016, o jornal The Guardian noticiou que características pessoais de aproximadamente 80 milhões de usuários do Facebook tiveram suas informações (traços de personalidade, preferências políticas etc.) ilegalmente extraídas, direta e indiretamente, pela empresa de dados Cambridge Analytica na formação de perfis psicológicos para utilização em marketing político. Com base na personalidade dos receptores, a empresa lhes endereçava propagandas específicas baseadas em cada tipo de perfil comportamental, o que veio a se provar uma poderosa técnica de persuasão na eleição estadunidense (PRIMI, 2018, p. 94).

Evgeny Mozorov (2018, p. 41-42) nos chama atenção para a inocuidade do debate sobre esses fenômenos. Ele é definido como "digital" em detrimento de "político" e "econômico", e desde o princípio é conduzido de forma favorável às empresas do big tech, porque falamos das ferramentas de tecnologia sem discorrer sobre os sistemas sociais, políticos e econômicos que são inviabilizados, ampliados ou atenuados por elas, desviando a discussão do ideal de bem comum, no sentido coletivo. E é a partir desse esforço de reconstrução que buscamos interpretar alguns pilares da Lei Geral de Proteção de Dados no Brasil, afinal, a tecnologia não é neutra, ela não determina de forma exclusiva a sociedade, mas sim os usos políticos que lhes são dados (CASTELLS, 1999).

## 3 A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

A partir das demandas originadas de casos como o da Cambridge Analytica, as pautas sobre a segurança de dados foram se tornando prioritárias no Brasil e no mundo. Em 2018, entrou em vigor o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, que unificou as leis de tratamento de dados que já existiam nos países europeus.

Com a implantação do GDPR, o empresariado brasileiro foi obrigado a se adequar para a realização de operações mercadológicas que envolvessem informações de pessoas físicas da União Europeia (UOL, 2018). Além disso, setores do mercado nacional já

alegavam que os episódios de ataques virtuais (VEJA, 2018), somados à necessidade de segurança jurídica nas operações de tratamento, ensejavam a regulação da matéria de maneira uniforme também no Brasil, a fim de evitar que as empresas ficassem "reféns" de normas setoriais (Instituto de Referência em Internet e Sociedade, 2018, p. 56).

Inspirada na GDPR, em 14 de agosto de 2018 foi sancionada a Lei nº 13.709/18, a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A regulação foi bem recebida por uma parcela de empresas que, inclusive, integraram uma frente empresarial a favor da normativa (INTERNATIONAL CHAMBER OF COMMERCE BRASIL, 2020).

A lei consagra como seus fundamentos, além do respeito à privacidade, autodeterminação informativa e a liberdade de informação (artigo 2º, I, II, III), a promoção da livre concorrência, o desenvolvimento econômico e tecnológico e a inovação (artigo 2º, V e VI).

Isto é, visa fortalecer o mercado de dados no Brasil e forjar uma cultura sobre a segurança de dados pessoais (FORNASIER; KNEBEL, 2020), na medida em que garante enquanto um de seus pontos chave a proteção do segredo comercial e industrial das empresas (artigos 6º, VI; 9º, II; 10, §3º; 18, V, dentre outros), sendo que consta do texto da lei que competirá à Autoridade Nacional de Proteção de Dados (ANPD) "zelar pela observância dos segredos comercial e industrial" (artigo 55-J, II, LGPD).

Basta acessar a rede social de negócios LinkedIn para visualizar que as empresas passaram a se promover sobre a implementação da LGPD nos seus processos internos. E o fazem não só por razões de segurança financeira e jurídica, mas também porque isso aumenta a sua reputação e confiança perante consumidores e investidores, o que chamam de "valuation".

Essa cultura faz parte da racionalidade e ideologia neoliberal "hipermoderna" que engendrou a figura do "sujeito empresarial" (DARDOT; LAVAL, 2016, p. 326) e capturou a ideia de tecnologia e a converteu, no âmbito discursivo, numa variável majoritariamente mercadológica e um instrumento da "expertise" concorrencial. Independentemente do uso exaustivo de termos como "inovação" e "disrupção", essas novas formas de sujeição carregam a marca da "mais inflexível e mais clássica das violências sociais típicas do capitalismo: a tendência a transformar o trabalhador em uma simples mercadoria"

(DARDOT; LAVAL, 2016, p. 329). As grandes descobertas científicas e tecnológicas foram aperfeiçoadas enquanto mecanismos de dominação. Não são direcionadas para o incremento da qualidade de vida, com formas de trabalho mais humanas e menos exaustivas, mas, pelo contrário, contribuem para a redução do valor da força de trabalho (MARX, 2010), sequestrando os postos de trabalho e intensificando os processos de precarização em prol da acumulação capitalista.

E, enquanto um suporte jurídico flexível para viabilizar essa nova economia de dados, são elencadas, no texto da LGPD, dez hipóteses legais nas quais os dados pessoais poderão ser tratados, o que será definido concretamente, a partir das atividades realizadas pelo controlador. Não sendo o caso de exclusão de aplicação da lei, deverá ocorrer o encaixe do tratamento realizado em pelo menos um dos incisos do artigo 7º, de rol taxativo (TEFFÉ; VIOLA, 2020, p. 4), para que a operação seja considerado lícita, tal como ocorre no GDPR.

A definição de dado pessoal recai sobre informações extraídas dos dados coletados que identifiquem diretamente ou tornem identificável uma pessoa natural (física). Inclui-se, aí o nome, RG, CPF e endereço, por exemplo. O conceito abrange também as informações indiretas obtidas de dados de geolocalização de dispositivo móvel, cookies, endereços IP e demais identificadores eletrônicos. A importância de se proteger esses dados indiretos reside no fato de que eles podem ser utilizados para o monitoramento do comportamento, definição de perfis e, por conseguinte, conduzir à identificação das pessoas a quem se referem[4].

[4] A lei objetiva também a proteção dos "dados sensíveis", conceituados como aqueles dados pessoais (art. 5º, II) "sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Por demandarem especial proteção, o tratamento dispensado pela LGPD é no sentido de se exigir o consentimento específico e destacado dos titulares de forma separada das demais cláusulas contratuais (art. 11, I). Essa preocupação se origina a partir dos impactos da publicidade comportamental, que vêm utilizando os dados sensíveis dos usuários para interferir diretamente nos seus direitos individuais e em sua autonomia. No caso dos dados biométricos, uma pessoa que usa um aplicativo de celular para acompanhar e controlar seus batimentos cardíacos e que venha a ser acometida por insuficiência cardíaca no futuro pode estar exposta à monetização dessas informações ou o seu vazamento para seguradoras de saúde que exigirão do usuário um custo abusivo no seu tratamento. Já na hipótese de vazamento de dados sobre a convicção religiosa ou opinião política, o usuário pode estar sujeito à intolerância e discriminação nos mais variados setores como no recrutamento de vagas de emprego, por exemplo. Existem exceções à regra do consentimento do titular para a coleta do dado sensível, como no caso do cumprimento de obrigação legal ou regulatória pela pessoa física ou jurídica responsável pelas decisões sobre o tratamento de dados pessoais, da tutela da saúde por profissionais da área ou por entidades sanitárias, da proteção

Ou seja, a coleta, produção, distribuição, avaliação, transferência e mais outras tantas operações realizadas (artigo 5º da LGPD) sobre os dados pessoais da pessoa natural ficam condicionadas ao esteio em, no mínimo, uma das previsões elencadas no rol do artigo 7º da lei.

Não obstante a particularidade e complexidade de cada uma dessas hipóteses de tratamento, fora do escopo deste trabalho, o consentimento do titular e a alegação de legítimo interesse do controlador sobre o dado pessoal a ser coletado despontam como algumas das principais bases da atual discussão regulatória. A discussão sobre a anonimização do dado também se mostra relevante não só pelo fato de que, em regra, os dados anonimizados não serão tutelados pela LGPD, mas também em razão dos limites que existem na busca pelo anonimato.

### 3.1 Consentimento e assimetria informacional

O consentimento, apesar de ser somente uma das hipóteses de tratamento, figura como protagonista da grande maioria das leis de proteção de dados ao redor do mundo. Isso porque a complexidade em se estabelecer um sistema que regulasse autorizações e proibições sobre o tratamento de dados levou os sistemas de proteção a adotarem uma política que aumentou a carga participativa do indivíduo na autodeterminação de suas informações pessoais (SOLOVE, 2013, p. 1880).

No âmbito da LGPD, o consentimento é a manifestação da vontade livre, informada e inequívoca (art. 5º, XII). Deve existir uma obrigação de informação para a empresa, não bastando o cumprimento formal. O usuário deve ter percepção do conteúdo da informação, uma vez que o fornecedor é quem detém o monopólio da informação sobre a técnica.

Esse dever implica, numa etapa preliminar, na ciência que o titular deve ter sobre a coleta, uso e compartilhamento dos seus dados. Uma vez informado, deve ser capaz de controlar seus dados sem coação física ou moral, a fim de que a autodeterminação informacional seja livre e verdadeira.

---

da vida ou da incolumidade física do titular e da realização de estudos por órgãos de pesquisa, quando assegurarem a anonimização dos dados pessoais, caso possível (art. 11, II).

A lei opera sobre uma aparente contradição: de um lado, reconhece a vulnerabilidade do titular de dados ao estabelecer requisitos mínimos para o consentimento, tendo em vista o desequilíbrio informacional em face das big techs (FORNASIER; KNEBEL, 2020). Do outro, expõe a importância da autonomia privada ao regular essa relação de forma a entender o usuário enquanto um mero contratante, que tem a capacidade de se autorregular e controlar os usos que serão outorgados às suas informações pessoais.

Entende-se, aqui, que as meras disposições da lei seriam insuficientes para mitigar esses desequilíbrios que permeiam a relação do usuário/titular de dados e os controladores de dados num contexto de capitalismo de vigilância.

Para além da discussão sobre os limites cognitivos sobre o consentimento (real capacidade do titular de compreender e avaliar os riscos e prejuízos, sobretudo em face dos termos de uso extensos, complexos e inacessíveis), é preciso pensar nas assimetrias de poder que permeiam as relações que envolvem o tratamento de dados.

Na sociedade capitalista informacional, boa parte das relações jurídicas são relações de consumo[5]. No capitalismo de vigilância essa dinâmica se aprofunda, porque é formado um mercado sem precedentes de digitalização da vida (BELLER, 2013). A partir do registro de dados e monitoramento das ações dos clientes, as empresas têm organizado um planejamento de vendas da forma mais rentável possível, o que conduz o titular a uma posição de vulnerabilidade em detrimento daqueles que detêm suas informações.

As prerrogativas que as corporações passam a deter sobre a coleta de dados e a formação de modelos de negócios no qual a própria experiência humana é um commodity revelam a intensificação da assimetria informacional e do desequilíbrio de poder nessas relações de consumo. O poder do mercado é consubstanciado na opacidade e nas vantagens competitivas baseadas no ocultamento das informações, através de operações

[5] A partir da segunda metade do século XX, a ordem social global tem no consumo não apenas uma variável econômica, mas um processo constitutivo de si mesma, das identidades e subjetividades a serem produzidas. Paralelamente à lógica homogeneizadora fordista, o capitalismo avançado informacional opera na fragmentariedade, com diluição de fronteiras antes rígidas. Para que seja possível a criação de novos modelos de acumulação, a produção necessita ser cada vez mais flexível e capacitada para produzir produtos cada vez mais diversificados em pouco tempo através da substituição do trabalho manual especializado pelo trabalho intelectual, onipresente e volátil (RETONDAR, 2008, p. 140-141).

que são desenhadas para serem indecifráveis para nós. Esse é um dos fatores que explicam o paradoxo que converteu a tecnologia e os seus potenciais de "descentralização, no aumento da informação compartilhada e, portanto, na ampliação das oportunidades de mercado" na sua antítese: a base do poder político, econômico e cultural capitalista (ZANATTA; ABRAMOVAY, 2019, p. 432).

E mesmo quando temos acesso a uma parte ínfima dessas informações, operações secretas paralelas convertem o excedente em operações mercadológicas que vão além dos nossos interesses, e nós não temos o controle porque não somos essenciais para essas ações mercadológicas (ZUBOFF, 2019, p. 100).

No entanto, e, para além do aspecto normativo, a adequação do consentimento a um mero elemento negocial (o que é constitutivo da própria lógica da LGPD, que tem como um dos fundamentos a livre iniciativa e a livre concorrência, em seu artigo 2º, VI) é insuficiente para a proteção das informações pessoais do indivíduo. Companhias ao redor do mundo e a própria administração governamental podem desenvolver novas formas de coleta e usos de dados, o que se agrava diante do fato de que essas tecnologias e mecanismos são desconhecidos para o público em geral.

Condicionar a proteção de dados ao consentimento e entendê-la dentro de uma chave contratual e civilista pressupõe que as pessoas poderiam optar por ceder suas informações de acordo com a sua autonomia privada. Ou seja, fazer uso da privacidade como uma propriedade individual, alienável.

Algumas pessoas poderiam argumentar que não enxergam problemas em entregar alguns de seus dados, tendo em vista possibilitarem, por exemplo, o acesso a sites online ou a obtenção de cupons de desconto. Isso acaba conduzi-los à conclusão de que essa "troca" seria algo trivial e de que esses dados não valeriam muita coisa no fim das contas.

Ceder bits de informação em diferentes contextos pode parecer inócuo, minimizando as consequências finais. No entanto, esse compilado de bits, quando agregado, se torna revelador e produz uma totalidade de informação sobre a pessoa que é de fato uma ameaça à privacidade, uma vez que não se sabe os potenciais e incertos usos que podem ser aplicados a esses dados (SOLOVE, 2013, p. 1881).Esses mecanismos estão inseridos dentro do contexto da nova fase do capitalismo de vigilância, sendo certo que a

LGPD, em última análise, enquanto fruto de uma produção estatal, funciona como garantia da reprodução econômica capitalista (MASCARO, 2013, p. 25).

E, indo de encontro a essa constatação, compreender a privacidade como um direito eminentemente privado significa traduzi-la para um valor monetário, outorgando as empresas o direito de lucro sobre a vida de determinado indivíduo. Não obstante, as informações pessoais do usuário não dizem respeito a ele somente, já que advém da nossa relação em sociedade:

> O problema das databases não é que os coletores falham em pagar o valor adequado das informações pessoais. O problema é a falta de controle, falta de conhecimento sobre como esses dados serão usados no futuro e falta de participação das pessoas no processo. Não é suficiente permitir que as pessoas vendam suas informações, relegar a elas toda a titularidade sobre e permitir que companhias as usem esses dados como lhes for apropriado. Isso proporciona às pessoas uma troca do tipo "tudo ou nada" na qual provavelmente elas se submeterão quando desconhecerem como essa informação poderá ser usada no futuro [...] Privacidade é uma questão que afeta a estrutura da sociedade e envolve nossa relação com a burocracia pública e privada (SOLOVE, 2004, p. 90, tradução nossa).

A abordagem contratualista entre sujeitos de direito é a forma jurídica que proporciona a mediação das trocas de mercadorias sobre o que se pressupõe formalmente ser voluntário, igual, neutro e universal (KASHIURA JR., 2015, p. 58). Os dados pessoais, quando passam a ser regulados por uma lei, são, portanto, uma mercadoria universalizada, disponível a todos no mercado, cuja troca[6] é agora legitimada.

E assim o é também porque a mercadoria passa a ser não somente a força de trabalho, mas a abstração do comportamento humano transformado em dados, a "mais-valia comportamental identificada como processo fundamental da nova economia do capitalismo de vigilância" (FORNASIER; KNEBEL, 2020, p. 19-20), diante das novas necessidades do capital que exigiram uma nova forma de excedente produzido.

Ainda que dentro da forma capitalista, com todas as suas limitações, o simples consentimento é insuficiente para a tutela da proteção da privacidade, porque não abarca os mecanismos de desequilíbrio de poder no tratamento da informação. Liberdade de

[6] O instituto do consentimento é um mecanismo de proteção e condição geral da extração de mais-valia (FORNASIER; KNEBEL, 2020): o sujeito entrega seus dados exercendo o seu consentimento e passa a ter a sua vida codificada pelas empresas, que a monetizam e mercantilizam no mercado de previsão de comportamentos. Em contrapartida, o valor é "retornado" através da plataforma, com os serviços prestados (ZUBOFF, 2019, p. 94-95)

escolha no âmbito do consumo implica informação prévia e precisa sobre a escolha e os efeitos da escolha, com espaço para a tomada de poder e controle sobre os próprios dados pessoais (SOLOVE, 2004, p. 85).

A LGPD exige, ainda, que o consentimento seja vinculado à finalidade específica quando do tratamento, ou seja, o titular deve ter conhecimento do propósito específico conferido aos seus dados. O problema reside na designação de finalidades genéricas, que acabam por esvaziar a autonomia do usuário.

O big data opera substancialmente sobre a reutilização de uma mesma base de dados para diferentes propósitos que não são previamente determinados. Como nos mostra o caso Cambridge Analytica, informações extraídas de dados considerados públicos e até mesmo irrelevantes como idade, nacionalidade, moradia etc. viram insumos para que seja possível desenvolver análises psicográficas de milhões de pessoas (O'NEILL, 2018, p. 153). É quase impossível que o usuário tenha conhecimento prévio de todos os elementos da cadeia do dado, uma vez que esse fluxo perpassa uma variada rede de atores, com uma capacidade de agregação de informação cada vez mais complexa.

Dado a complexidade envolvida na obtenção do consentimento e a onerosidade para o controlador, não se esquecendo também que a lei se fundamenta especialmente no fomento da economia de dados, advogados empresariais já sinalizaram que "um controlador esperto não adota o consentimento como regra e se utiliza também de outras bases mais flexíveis e artesanais apresentadas pela lei brasileira para o tratamento" (BECKER; SCHRAPPE, 2020).

Destaca-se aqui o inciso V, que permite o tratamento "quando necessário para execução do contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados".

Esse dispositivo, se aplicado em sua literalidade, acaba por esvaziar a proteção da LGDP, tornando o consentimento a exceção e não a regra. Isso porque permite que o simples fato de constar do contrato uma cláusula que assegura ao fornecedor o poder de coleta dos dados o isenta da obrigatoriedade de consentimento livre, informado e inequívoco do usuário da plataforma ou outro consumidor em geral.

Outra hipótese de tratamento que também pode excepcionar a regra do consentimento é a do inciso IX do artigo 7º, que será abordada a seguir.

### 3.2 Legítimo interesse

O legítimo interesse do controlador ou de terceiro é uma das hipóteses de tratamento de dados pessoais estritamente necessários, quando existirem finalidades legítimas, consideradas a partir de situações concretas (artigos 7º, IX e artigo 10, §1º, LGPD).

Por não exigir elementos externos autorizadores (como o consentimento ou uma obrigação legal), essa base legal pode ser mais flexível para o controlador, como ocorreu na Europa, onde 70% dos procedimentos de tratamento de dados pessoais se deu com fundamento no legítimo interesse de previsão similar no GDPR (MATTIUZZO; PONCE, 2020, p. 58).

No Brasil, estima-se que o legítimo interesse provavelmente será a hipótese de tratamento mais aplicada. Renato Leite Monteiro, professor do Data Privacy Brasil (site que oferece cursos voltados à proteção de dados), estimou, numa entrevista para o UOL, que 30 a 40% dos processos de adequação que ele tem acompanhado nas empresas estão se fundamentando no legítimo interesse, com destaque também para a base da execução de contratos (inciso V, artigo 7º, LGPD) e proteção ao crédito (inciso X, artigo 7º, LGPD): "O consentimento a gente tem evitado, porque é traiçoeiro, muito fácil de ser revogado" (UOL, 2019).

Os conceitos trazidos pela lei para a implementação do legítimo interesse são genéricos e essa hipótese legal ainda carece de balizas, uma vez que a lei se limitou a definir enquanto finalidades legítimas aquelas que "incluem, mas não se limitam a: I – apoio e promoção de atividades do controlador; e II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem [...]". Essas lacunas deverão ser preenchidas por regulamentação complementar a ser editada pela Autoridade Nacional de Proteção de Dados (ANPD), como consta do artigo 55-J, III e XIII da lei.

A questão é que a ANPD acabou por ser estruturada enquanto um órgão integrante da Presidência da República (artigo 55-A da LGPD), o que já gerava preocupação por conta da ausência de autonomia administrativa do órgão no desempenho de funções como a fiscalização dos dados do próprio governo. E, ato contínuo, em 15 de outubro de 2020, o governo federal nomeou militares do Exército[7] para três dos cinco nomes indicados à diretoria da ANPD. A escolha, evidentemente, é uma ameaça às garantias que deveriam ser protegidas pela ANPD[8], frustrando o caráter técnico e independente indispensáveis à construção de parâmetros a serem definidos para a aplicação eficaz da lei.

De todo modo, a acepção do que se enquadraria como "legítimo interesse" não é unívoca. O Working Party 29, em seu Parecer 06/2014 (2014, p. 56) que baseou o texto da GDPR, propôs o teste da ponderação para balancear os direitos do titular de dados e do controlador. O objetivo é que se verifique, no caso concreto, se as legítimas expectativas e direitos fundamentais dos titulares estão sendo atendidos quando do tratamento baseado no legítimo interesse. Essa análise se dá a partir de quatro fases: avaliação dos interesses legítimos; impacto sobre o titular do dado; equilíbrio entre o interesse do controlador e o impacto sobre o titular; e salvaguarda para proteger o titular (ARTICLE 29, 2014).

No caso brasileiro, Bruno Bioni (2019) aponta a possibilidade de transposição desse teste de proporcionalidade da seguinte forma: i. avaliar se o interesse não é ilegal e se existem benefícios ou vantagens com o uso do dado pelo controlador, bem como se há uma situação que lhe dê suporte (artigo 10, caput e I, LGPD); ii. verificar se os dados são necessários para a finalidade alegada e se o tratamento não poderia se dar por outra base legal (artigo 10, 1º, LGPD); iii. balanceamento do interesse do controlador com a legítima

[7] A militarização da ANPD faz parte de um contexto maior que se intensificou, no Brasil, a partir do golpe de 2016 e da eleição de um representante da extrema-direita ultraliberal e fascista em 2018. As políticas de austeridade social, a demanda por mais vigilância, controle e repressão da juventude e dos movimentos sociais passaram a ter uma aceitação ainda mais ampla no debate público, e, desde então, boa parte das instituições democráticas foram ocupadas por militares. O Exército vem ganhando um protagonismo político inédito desde a redemocratização, o que foi viabilizado pela guinada conservadora que enxerga as Forças Armadas como uma reserva moral da nação. Conforme levantamento realizado pelo Tribunal de Contas da União, até julho de 2020, existiam 6.157 militares exercendo funções civis na Administração Pública federal (SANTOS, 2020).

[8] A Coalização Direitos na Rede, organização que agrega mais de 40 entidades brasileiras da academia e da sociedade civil e de defesa dos direitos digitais e a entidade global de direitos digitais AccessNow enviaram uma carta-denúncia à Comissão Europeia, Conselho da Europa e à Global Privacy Assembly a fim de alertar sobre a militarização da ANPD. A íntegra da carta está disponível no link https://direitosnarede.org.br/2020/11/10/cdr-e-access-now-enviam-carta-denuncia-para-comissao-europeia-conselho-da-europa-e-global-privacy-assembly/.

expectativa do titular (artigo 10, II, LGPD); e iv. verificar as salvaguardas e exigências de transparência e mecanismos de oposição e de mitigação de riscos (artigo 10, §§2º e 3º, LGPD).

Justamente por conta da plasticidade envolvida nesse fundamento legal, o legítimo interesse gera, para o controlador, deveres de transparência (artigo 10, §2º). A principal medida de transparência é o relatório de impacto previsto no §3º, que dispõe que a ANPD "poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos industrial e comercial".

Ou seja, não existe uma obrigação imediata de preparação do relatório (TEFFÉ; VIOLA, 2020, p. 19), ao contrário do que estabelece o GDPR, que exige um relatório de impacto desde o princípio, quando um determinado tratamento possa gerar altos riscos para os direitos fundamentais do titular (artigo 35, GDPR). A legislação europeia exige que esse relatório deve trazer a descrição dos tipos de dados coletados, a metodologia utilizada para coleta e garantia da segurança e os mecanismos de mitigação dos riscos.

A antítese do que se considera um dado pessoal reside no conceito de dado anônimo, isto é, aquele que é incapaz de revelar a identidade do indivíduo (BIONI, 2015, p. 25; 2020, p. 191). A própria lei[9] destaca que o dado anonimizado não se considera dado pessoal (artigo 12), razão pela qual evidenciamos, a seguir, a anonimização enquanto um importante referencial no qual se fundamenta a LGPD.

### 3.3 Anonimização de dados pessoais

Os dados anonimizados (art. 5º, III, LGPD), considerados pelo empresariado como essenciais para o crescimento da inteligência artificial e aprimoramento da tecnologia em

[9] Uma interpretação sistemática da lei e, sobretudo, dos artigos 1º "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" e 12 "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido" conduzem à conclusão de que os dados anonimizados não serão, em regra, objeto de proteção da LGPD, ou seja, não se sujeitam às hipóteses de tratamento elencadas no artigo 7º, inclusive o consentimento. Isso se dá especialmente porque existem situações nas quais o consentimento é considerado oneroso ou até mesmo impossível de ser obtido, como expõe o Information Commisioner's Office do Reino Unido (2016, p. 6 e 28). No mesmo sentido os autores Cunha, Camara e Lerner (2020).

si (SERPRO, 2019), podem advir de uma série uma técnicas de anonimização no intuito de eliminar a possibilidade de identificação e individualização de uma pessoa, sendo hoje uma das principais estratégias na busca da proteção da privacidade.

Inicialmente, são definidos quais conjuntos de dados (atributos) serão anonimizados e quais técnicas serão aplicadas a cada um deles, classificando-os de acordo com a sensibilidade da informação que cada um representa (SILVA, 2019, p. 28). Os atributos são divididos em (BRANCO JR.; MACHADO; MONTEIRO, 2014, p. 53): identificadores (por exemplo, CPF, nome, RG); semi-identificadores (ao serem combinados com outras informações podem identificar o titular, como data de nascimento e CEP); e sensíveis (relacionados a condições específicas da pessoa como salário e exames médicos).

Após a identificação dos atributos, são aplicadas as técnicas de anonimização, das quais se destacam como principais a supressão, ou seja, remoção completa do atributo, comumente utilizada nos dados identificadores; generalização, na qual se mantém somente parte dos dados; e agregação, que consiste na disseminação de dados para liberar estatísticas agregadas (SILVA, 2019, p. 29-31). Destacam-se ainda enquanto técnicas existentes para anonimização a encriptação e a perturbação ou mascaramento (BRANCO JR.; MACHADO; MONTEIRO, 2014, p. 53-54).

A LGPD, apesar de não tratar das técnicas de anonimização de forma específica, dispõe expressamente que a anonimização é um direito do titular (artigo 18, IV). Porém, cada vez mais recorrentemente tem se apontado, na literatura especializada, a falibilidade inerente às principais técnicas utilizadas.

O Article 29 Data Protection Party (antigo órgão responsável pela proteção de dados na Europa) concluiu, através de um estudo sobre as variadas técnicas de anonimização, que cada uma das técnicas analisadas falhou diante dos critérios de anonimização estabelecidos (I. se é possível individualizar a pessoa; II. se é possível conectar pelo menos dois registros ao mesmo tipo de dado e III. se é possível conectar os registros para deduzir novas informações sobre determinada pessoa (ARTICLE 29, DATA PROTECTION WORKING PARTY, 2014, p. 23-24).

Um estudo realizado em 2013 concluiu que pessoas podem ser rastreadas e identificadas a partir de banco de dados que inicialmente foram considerados

anonimizados. Analisando dados móveis de 1,5 milhão de indivíduos durante 15 meses, Montjoye, Hidalgo, Verleysen e Blondel (2013, p. 1) chegaram à conclusão de que com apenas quatro pontos de dados, 95% dos pesquisados puderam ser reidentificados quando a sua informação foi disponibilizada em base horária por antenas de celulares.

Em 2019, outra pesquisa estimou que, com a ajuda de *machine learning* (reconhecimento de padrões que permite aos computadores aprenderem sem a necessidade de que sejam programados), a probabilidade de um indivíduo específico ser reidentificado a partir de databases anônimas, mesmo que incompletas, é de 99,98%. Os pesquisadores concluíram que as técnicas tradicionais de anonimização como *adding noise* (incluir informações imprecisas) e *sampling* (estatística que seleciona subconjuntos de pessoas) seriam ineficientes para ocultar a identidade dos titulares (ROCHER; HENDRICKX; MONTJOYE, 2019, p. 1).

No caso "Netflix prize", a empresa disponibilizou a sua base de dados de avaliações suprimindo o nome dos usuários para que pudesse melhorar o seu algoritmo de sugestão de filmes. Não obstante, os pesquisadores Arvind Narayanan e Vitaly Shmatikov (2005, p. 12) identificaram que seria necessário somente 03 a 19 bits de informação para reverter o processo de anonimização, disponível e acessível na plataforma do Internet Movies Database (IMDB). Com o cruzamento das bases do IMDB e da Netflix, a identidade dos avaliadores da Netflix foi revelada.

Esse contexto se agrava diante do que se chamou de "privacywashing" (marketing de empresas que constroem uma falsa imagem de responsabilidade social com a privacidade do usuário, porem não realizam ações concretas que viabilizem essa proteção): a empresa cita genericamente algum dispositivo da LGPD sem informar ao usuário a técnica de anonimização utilizada e seus possíveis riscos de reidentificação, criando, para o titular, uma falsa percepção de segurança (NEGRI; GIOVANINI, 2020, p. 141).

Para Bruno Bioni (2015, p. 29), esses casos evidenciam a falibilidade consensual do processo de anonimização, o que tem permitido a mitigação de um discurso que antes sustentava a sua irreversibilidade, hoje centrada na política de redução de riscos.

E é nesse sentido que a própria LGPD prevê a aplicação quando a anonimização puder ser revertida mediante "esforços razoáveis" e através de "meios próprios". Ou seja, se empreendidos esforços fora dos razoáveis para a identificação, não haveria que se falar em dados pessoais (BIONI, 2020, p. 192).

No direito brasileiro[10], os limites conceituais de "esforços razoáveis" e "meios próprios" e os padrões e técnicas a serem empregados nos processos de anonimização ainda não foram estabelecidos, sendo que a regulação da matéria também caberá à ANPD (art. 55-J, III, LGPD e artigo 4º, III, "a" do Decreto 10.474/2020).

Apesar de qualquer posterior regulamentação específica, tendo em vista a aceleração da evolução tecnológica, será cada vez mais desafiador garantir uma anonimização efetiva. Ainda que o controlador possa revisar das decisões tomadas no tratamento pelo algoritmo a pedido do titular do dado nas situações mencionadas no artigo 20, a própria lei resguarda o segredo comercial e industrial da empresa no §1º e, dispondo ainda que compete à ANPD zelar por estes interesses comerciais (artigo 55-J, II, LGPD).

Esse tipo de previsão legal é prejudicial para a compreensão e a discussão sobre o que se definiu enquanto a "caixa preta" dos algoritmos, isto é, o desconhecimento sobre os seus desenhos internos e as suas implementações, isto para não falar nas implicações sociais e políticas negativas que já foram apontadas em testes com algoritmos, como a reprodução das relações de poder e opressão[11].

---

[10] No sistema europeu de proteção de dados, a questão foi objeto de um parecer de um órgão técnico consultivo que fixou não se considerar anônimo os dados que permitem a individualização da pessoa, ainda que indiretamente (SOARES, 2019).

[11] Um teste feito pelo site Motherboard/Vice (THOMPSON, 2017) no Cloud Natural Language API (ferramenta do Google que revela o significado de textos) revelou que o algoritmo da ferramenta classificou trechos como "eu sou uma mulher negra gay" e "eu sou judeu" como negativos, enquanto frases como "eu sou cristão" e "eu sou um mano francês heterossexual" foram classificadas enquanto positivas. Nos Estados Unidos, o algoritmo COMPAS (Perfil de Gerenciamento Corretivo de Infratores para Sanções Alternativos) foi elaborado por uma empresa para avaliar a probabilidade de reincidência de pessoas presas. Um estudo elaborado pelo jornal ProPublica (ANGWIN et. al., 2016) constatou que, mesmo eliminando as variáveis de raça do histórico criminal, idade e gênero, o algoritmo ainda classificava as pessoas negras como 77% mais "prováveis" de cometer um novo crime. Leonardo Vieira (2019, p. 4) aponta que para corrigir esses vieses dos algoritmos é importante entender que eles não são imparciais e equitativos, sobretudo se considerarmos quem está desenvolvendo inteligência artificial (por exemplo, somente 22% de desenvolvedoras são mulheres, de acordo com o Global Gender Gap Report de 2018).

E, por isso, é uma previsão também antidemocrática, uma vez que o que se pretende é esconder informação e ocultar os processos de tomada de decisão que impactam a vida e o cotidiano de milhões de pessoas em prol de um discurso neoliberal que glorifica a tecnocracia, a propriedade privada e o consumismo enquanto maximiza as desigualdades, vigilância, o controle e a repressão sobre os mais vulneráveis.

O mais prudente seria que esse processo fosse realizado de forma transparente e por uma entidade independente, o que minimizaria os riscos internos e externos de reindentificação, "na medida em que se reduz o número de atores que teria capacidade de juntar as peças do quebra-cabeça para formar a imagem dos titulares da informação" (BIONI, 2020, p. 198).

Não obstante o necessário preenchimento e balizas aos conceitos gerais trazidos pela lei, a análise sobre a anonimização do dado deve se dar de forma circunstancial. É dentro de cada atividade da cadeia de um dado que se analisa a anonimização, sendo ainda que esse processo "deve representar um conjunto de ações contínuo e logicamente ordenado que abrace toda a extensão do ciclo de vida de um dado – da coleta ao descarte" (BIONI, 2020, p. 197). Daí a necessidade de um gerenciamento focado também em cláusulas contratuais que proíbam as partes de reverterem o processo de anonimização, delimitem o papel de cada agente no tratamento de modo a vedar o repasse e estabeleçam a destruição dos dados após a conclusão da atividade, mediante técnicas atuais e constantemente atualizadas (BIONI, 2020, p. 199).

De todo modo, o funcionamento da internet não demanda por si só a coleta de dados sobre a identidade do usuário para que lhe seja direcionado determinado conteúdo ou até mesmo sujeitá-lo a um processo de decisão automatizada:

> Basta lhe atribuir um identificador eletrônico único que permita separá-lo dos milhões de usuários da rede, como por exemplo, com relação ao computador a qual ele está conectado, o que é feito através do número de conexão a ele atribuído [...] A partir desse identificador eletrônico, reconhece-se o dispositivo conectado, o que permite, dentre outras coisas, a memorização dos logins e/ou senhas para um acesso mais dinâmico às aplicações da web. É dessa maneira que se melhora a experiência do usuário – mantra tão repetido nos diais atuais – que nada mais é que a formação de um perfil comportamental da sua navegação. É possível, portanto, compilar um perfil "browsing" (navegação) [...] ainda que não se tenha certeza a respeito do sujeito que pratica tal ação (BIONI, 2015, p. 37).

Nesse sentido, uma separação rígida entre os conceitos de dados pessoais e anonimizados se torna incoerente, na medida em que a formação de perfis comportamentais que tem por fim último influenciar[12] a vida dos seres humanos prescinde da sua identificação.

Grupos de pessoas são e continuarão sendo afetadas por conta das informações sobre a sua etnicidade, situação socioeconômica e de saúde, origem, etc., sobretudo no que tange à formulação de políticas públicas. Afinal, muitas funções que percebemos enquanto públicas (coletar, categorizar e suprir as necessidades dos cidadãos, por exemplo) são, na realidade, operadas pelo setor privado, o que impacta profundamente a transparência e prestação de contas envolvidas nesse processo, sendo ainda que a "datificação" do governo sempre foi e sempre será executada primariamente pelos corporativistas (TAYLOR, 2017, p. 3).

Isso nos conduz ao entendimento de que uma estratégia regulatória realmente comprometida com a proteção da privacidade deveria não só abarcar a formação dos perfis de comportamento (BIONI, 2015, p. 38-41), como também tutelar as liberdades e os direitos políticos de grupos coletivamente (TAYLOR, 2020, p. 7), uma vez que os impactos da extração de dados dizem respeito ao funcionamento do tecido social como um todo.

## 4 CONCLUSÃO

Algumas pessoas poderiam argumentar que não se importam com o fato de que empresas extraem nossos dados e preveem nossas vontades e comportamentos, dado a conveniência em receber uma indicação de filme na Netflix ou um anúncio direcionado na internet, por exemplo. Especialmente num contexto neoliberal de precarização do trabalho, políticas de austeridade social e avanço da desigualdade, com o aumento do custo de vida familiar e a instauração da insegurança vital, poupar tempo e ter acesso a serviços digitais personalizados de fato é uma conveniência útil.

[12] Bruno Bioni (2015, p. 41) exemplifica a prática da discriminação dos preços: "Da mesma forma que consumidores acabaram por receber ofertas com precificação diferentes por conta do identificador único do seu dispositivo conectado, mediante a inferência de que usuários de Mac/Apple teriam mais condições financeiras do que de Windows, não é difícil imaginar que donos de jaguar terão a reserva online da vaga do estacionamento com precificação maior do que de carros populares, tal como o pedido de compra vindo de uma "Brastemp" em comparação com outras mais marcas de segunda linha".

No entanto, essas necessidades, criadas por esse mesmo sistema produtor de vulnerabilidades, têm sido retroalimentadas e constantemente exploradas pela indústria do big data, sedimentando as companhias mais lucrativas da história do comércio.

O ponto é que esse capital advém de mecanismos de extração contínua da nossa vida cotidiana, que foram criados e projetados de formas que até hoje são desconhecidas, sem ferramentas de controle e participação pública e social. As empresas de tecnologia detém um monopólio informacional que foi desenhado para nos manter ignorantes sobre sua lógica de funcionamento, ao mesmo tempo em que nós desempenhamos um papel essencial no processo produtivo de exploração de dados.

Por isso, tanto o debate sobre as iniciativas regulatórias como a discussão sobre os conflitos envolvendo os usos da tecnologia devem abarcar as implicações sociais, políticas e econômicas que afetam grupos de pessoas a partir de variáveis como local de origem, etnicidade, situação socioeconômica e de saúde etc.

Uma estratégia regulatória eficaz e realmente comprometida com os direitos dos cidadãos deve levar em consideração as assimetrias de poder e de informação imbricadas no jogo das economias digitais, tutelando-os coletivamente e não somente enquanto indivíduos excluídos do tecido social, uma vez que esses impactos nos atingem também de forma coletiva.

Alguns dispositivos da LGPD vão na contramão dessa abordagem. Ainda que dentro de um contexto de capitalismo de vigilância, com todas as limitações existentes, proteger o segredo do negócio diante de um cenário no qual os algoritmos tomam decisões, a todo o tempo, sobre a vida de milhões de pessoas, faz com que a lei funcione muito mais como um suporte jurídico para a viabilização do mercado de dados do que como um instrumento de garantia à privacidade dos indivíduos.

Outro problema emerge a partir da abordagem exclusivamente privada, individual e contratualista do consentimento, o que acaba por reduzir a capacidade emancipatória do usuário, já que os desequilíbrios informacionais imbricados no tratamento de dados impedem que esse consentimento seja pleno. Isto é, o titular acredita ter algum poder de decisão, quando na realidade, sequer lhe são apresentados os riscos que podem advir da coleta.

Abordar a exploração de dados pessoais sobre as mais diversas experiências humanas através do consentimento individual e, portanto, pela lógica de um contrato, legitima e torna lícito a sua transformação em mercadoria, fortalecendo juridicamente a acumulação capitalista baseada nessa extração.

Somos facilmente conduzidos a pensar que privacidade é um assunto particular e privado, ou seja, achamos que se trata de uma escolha, de uma troca. A verdade é que privacidade não é um direito privado, privacidade é um problema e direito coletivo que não se sujeita a um mero cálculo individual, por envolver a estrutura da sociedade como um todo. Tampouco se trata de uma troca justa, porque o produto final, do qual as corporações extraem seu lucro, é o conjunto de informações produzido pelos próprios usuários.

Mesmo com todas as limitações envolvidas nos cálculos do consentimento, é provável que essa base legal, apesar de ser a protagonista nas discussões jurídicas, fique longe de ser a mais utilizada pelas empresas. Isso porque, quando não estiverem amparadas no inciso que trata da obrigação contratual ou da proteção ao crédito, poderão se socorrer à hipótese do legítimo interesse do controlador.

Ainda não foram estabelecidos os limites e especificações sobre o tratamento baseado no legítimo interesse. E, mesmo após a sua definição, a LGPD, ao contrário do GDPR, não exige a confecção de um relatório de impacto dos riscos envolvidos para todo e qualquer tratamento com base nessa hipótese, o que pode resultar num passe livre para arbitrariedades na coleta de dados. Além disso, a regulamentação específica e a fiscalização dessas condutas ficam comprometidas com a ausência de autonomia e independência da ANPD.

Enquanto o legítimo interesse pode excepcionar o consentimento, a anonimização dos dados pessoais pode excepcionar a própria aplicação da LGPD, o que se mostra inócuo para mitigar algumas práticas que sujeitam os indivíduos ao direcionamento de conteúdos específicos ou a um processo de decisão automatizada.

Diante da falibilidade inerente às principais técnicas de anonimização, as iniciativas regulatórias acabaram por direcionar o discurso que antes sustentava a sua irreversibilidade para a redução de riscos. A LGPD cita parâmetros como o da razoabilidade

para tutela do dado pessoal no caso de reidentificação. No entanto, a formação de perfis de comportamento que acabam por influenciar vários segmentos sociais (desde marketing político e formulação de políticas públicas, aos contratos discriminatórios e à publicidade abusiva) prescinde da individualização do usuário, e, portanto, acaba saindo ilesa da regulação.

Por outro lado, a LGPD cumpre o papel de reconhecer, juridicamente, no Brasil, a importância desse debate. Inovação e evolução tecnológica são desejáveis e continuarão ocorrendo. Em vista disso, é preciso que essa pauta englobe e demande uma tecnologia aberta, transparente e transindividual, que não seja responsável por converter as experiências humanas em commodities. A comunicação e o acesso à informação são bens comuns, de todos, e valiosos demais para serem controlados por uma classe em detrimento de toda a população. Por isso, a internet e a tecnologia em geral só serão participativas de verdade quando envolverem poder e propriedade dos cidadãos sobre toda a sua estrutura.

■■■

## REFERÊNCIAS

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 05/2014 on Anonymisation Techniques**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em 12/01/2021. Acesso em: 12 jan. 2021.

ANGWIN, J. *et al*. Machine Bias: there's software used across the country to predict future criminals. And it's based against blacks. **ProPublica**, 23 maio 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 12 jan. 2021.

BECKER, D.; SCHRAPPE, C. Consentimento e o consentimento na LGPD. **Jota**, 03 jan. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/consentimento-e-o-consentimento-na-lgpd-03012021?amp=1. Acesso em: 12 jan. 2021.

BELLER, Jonathan. Digitality and the Media of Dispossession. *In*: Trebor Sholz (org.). **Digital Labor**: The Internet as Playground and Factory. New York: Routledge, 2013. p. 211-234

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

BIONI, Bruno. Compreendendo o conceito de anonimização e o dado anonimizado. **Escola Paulista da Magistratura**, n. 53, 20 mar. 2020. Disponível em: https://epm.tjsp.jus.br/Publicacoes/CadernoJuridico/60662. Acesso em: 12 jan. 2021.

BIONI, Bruno. Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. **Privacidade e vigilância**, Goma Oficina, 02 jul. 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 12 jan. 2021.

BRANCO JR., E. C.; MACHADO, J. C.; MONTEIRO, J. M. Estratégias para Proteção da Privacidade de Dados Armazenados na Nuvem. **Tópicos em Gerenciamento de Dados e Informações**, 1. ed, 2014. Disponível em: http://www.inf.ufpr.br/sbbd-sbsc2014/sbbd/proceedings/artigos/pdfs/14.pdf. Acesso em 12/01/2021. Acesso em: 13 jan. 2021.

BRASIL. **Lei Nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 jan. 2021.

CASTELLS, Manuel. **A sociedade em rede**: volume 1. São Paulo: Paz e Terra, 1999.

COALIZAÇÃO DIREITOS NA REDE. **CDR e Access Now enviam carta-denúncia para Comissão Europeia, Conselho da Europa e Global Privacy Assembly**. 10 nov. 2020. Disponível em: https://direitosnarede.org.br/2020/11/10/cdr-e-access-now-enviam-carta-denuncia-para-comissao-europeia-conselho-da-europa-e-global-privacy-assembly/. Acesso em: 13 jan. 2021.

CUNHA, J. M.; CAMARA; D.; LERNER, V. Anonimização de dados pessoais: entre a proteção e a ilusão do compliance. **Conjur**, 08 ago. 2020. Disponível em: https://www.conjur.com.br/2020-ago-08/cunha-camara-lerner-anonimizacao-dados-pessoais. Acesso em: 12 jan. 2021.

DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo:** ensaio sobre a sociedade neoliberal. São Paulo: Boitempo, 2016.

DE PIERRO, Bruno. O mundo mediado por algoritmos. **Revista de Pesquisa da FAPESP**, ed. 266, abr. 2018. Disponível em: https://revistapesquisa.fapesp.br/o-mundo-mediado-por-algoritmos/. Acesso em: 12 jan. 2021.

EVANGELISTA, Rafael de Almeida. Capitalismo de vigilância no sul global: por uma perspectiva situada. *In:* SIMPOSIO INTERNACIONAL LAVITS VIGILANCIA, DEMOCRACIA Y PRIVACIDAD EM AMÉRICA LATINA: VULNERABILIDADES Y RESISTÊNCIAS, 5., Santiago, Chile, dez. 2017. **Anais** [...]. Santigado, 2017. p. 243-253. Disponível em: http://lavits.org/wp-content/uploads/2018/04/08-Rafael-Evangelista.pdf. Acesso em: 12 jan. 2021.

FORNASIER, Mateus de Oliveira; KNEBEL, Noberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, [s. l.], jun. 2020. Disponível em:

https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/46944/33907. Acesso em: 12 jan. 2021.

FUCHS, Christian. Class and Exploitation on the Internet. *In*: Trebor Sholz (org.). **Digital Labor**: The Internet as Playground and Factory. New York: Routledge, 2013. p. 263-280

EUROPEAN UNION. **General Data Protection Regulation**. Disponível em: https://gdpr-info.eu/. Acesso em: Acesso em: 13 jan. 2021.

INFORMATION COMMISSIONER'S OFFICE. **Anonymisation**: managing data protection risk code of practice. 2016. Disponível em: https://ico.org.uk/media/1061/anonymisation-code.pdf. Acesso em: 13 jan. 2021.

INTERNATIONAL CHAMBER OF COMMERCE BRASIL. **ICC Brasil e mais de 80 entidades pedem segurança jurídica no tratamento de dados pessoais**. Publicado em 11 ago. 2020. Disponível em: https://www.iccbrasil.org/noticias/2020/8/11/frente-empresarial-pede-seguranca-juridica-dados/. Acesso em: 12 jan. 2021.

KASHIURA JR., Celso Naoto. Sujeito de direito e interpelação ideológica: considerações sobre a ideologia jurídica a partir de Pachukanis e Althusser. **Revista Direito e Práxis**, v. 6, n. 1, p. 49-70, mar. 2015. Disponível em: https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/12742/11706. Acesso em: 12 jan. 2021.

MARX, Karl. **O capital**: crítica da economia política. Livro I. Rio de Janeiro: Civilização Brasileira, 2010.

MASCARO, Alysson Leandro. **Estado e forma política**. Boitempo: São Paulo, 2013.

MATTIUZZO, M.; PONCE, P. P. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. **InternetLab**, v. 1, n. 2, dez. 2020. Disponível em: https://revista.internetlab.org.br/o-legitimo-interesse-e-o-teste-da-proporcionalidade-uma-proposta-interpretativa/. Acesso em: 12 jan. 2021.

MONTJOYE, Y. A; HIDALGO, C. A.; VERLEYSEN, M.; BLONDEL, V. D. Unique in the Crowd: the privacy bounds of human mobility. **Scientific Reports**, n. 3, 25 mar. 2013. Disponível em: https://www.nature.com/articles/srep01376.pdf. Acesso em: 12 jan. 2021.

MOZOROV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust De-anonymization of large Datasets** (How to Break Anonymity of the Netflix Prize Dataset). The University of Texas at Austin, 05 fev. 2008. Disponível em: https://arxiv.org/pdf/cs/0610105.pdf. Acesso em: 12 jan. 2021.

NEGRI, S. M. C. A.; GIOVANINI; C. F. R. Dados não pessoais: a retórica da anonimização no enfrentamento à covid-19 e o privacywashing. **Internetlab**, v. 1, n. 2, dez. 2020. Disponível em: https://revista.internetlab.org.br/wp-content/uploads/2020/12/Dados-na%CC%83o-pessoais.pdf. Acesso em: 12 jan. 2021.

O'NEILL, Cathy. **Weapons of math destruction**: how big data increases inequalitity and threatens democracy. New York: Crown Publishers, 2016.

POLIDO; F.; DOS ANJOS, L.; BRANDÃO, L. C. C. **III Seminário Governança das Redes**: política, internet e sociedade. Instituto de Referência em Internet e Sociedade. 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/12/Anais-III-Seminario.pdf. Acesso em: 12 jan. 2021.

PRIMI, Ricardo. Avaliação Psicológica no Século XXI: de onde viemos e para onde vamos. **Psicologia:** ciência e profissão, v. 38, num. esp., p. 87-97, 2018. Disponível em: http://www.scielo.br/pdf/pcp/v38nspe/1982-3703-pcp-38-nspe1-0087.pdf. Acesso em: 12 jan. 2021.

RETONDAR, Anderson Moebus. A (re)construção do indivíduo: a sociedade de consumo como "contexto social" de produção de subjetividades. **Sociedade e Estado**, v. 23, n. 1, p. 137-160, jan./abr. 2008. Disponível em: http://www.scielo.br/pdf/se/v23n1/a06v23n1.pdf. Acesso em: 12 jan. 2021.

ROCHER, L.; HENDRICKX, J. M.; DE MONTJOYE, Y. Estimating the success of re-identifications in incomplete datasets using generative models. **Nature Communications**, 10, 3069, 23 jul. 2019. Disponível em: https://www.nature.com/articles/s41467-019-10933-3.pdf. Acesso em: 12 jan. 2021.

SERPRO. **O que são dados anonimizados, segundo a LGPD**. Serviço Federal de Processamento de Dados, 2019. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd. Acesso em: 12 jan. 2021.

SILVA, Hebert de Oliveira**. Uma abordagem baseada em anonimização para privacidade de dados em plataformas analíticas**. Dissertação (Mestrado em Tecnologia) – Universidade Estadual de Campinas, Limeira, 2019. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/334676/1/Silva_HebertDeOliveira_M.pdf. Acesso em: 12 jan. 2021.

SANTOS, R. **Mais de 6 mil militares já exercem funções civis no governo federal, diz TCU**. Conjur, 17/07/2020. Disponível em: https://www.conjur.com.br/2020-jul-17/mil-militares-exercem-funcoes-civis-governo-federal. Acesso em: 12 jan. 2021.

SOARES, P. S. C. Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD. **Conjur**, 10 mar. 2019. Disponível em: https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protecao-dados. Acesso em: 12 jan. 2021.

SOLOVE, Daniel J. **Digital person**: technology and privacy in the information age. New York: New York University Press, 2004.

SOLOVE, Daniel J. Introduction: Privacy self-management and the consent dilemma. **Harvard Law review**, v. 126, p. 1880-1903, 2013. Disponível em: https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf. Acesso em: 12 jan. 2021.

TEFFÉ, Chiara Spadaccini; Viola, Marco. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, v. 9, n. 1, p. 1-38, 9 maio 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 12 jan. 2021.

THOMPSON, Andrew. Google's Sentiment Analyzer Thinks Being Gay Is Bad. **Vice**, 25 out. 2017. Disponível em: https://www.vice.com/en/article/j5jmj8/google-artificial-intelligence-bias. Acesso em: 12 jan. 2021.

UOL NOTÍCIAS. **Europa fecha cerco aos dados**, 25 maio 2018. Disponível em: https://www.uol/noticias/especiais/gdpr.htm#imagem-6. Acesso em: 12 jan. 2021.

VEJA. **Brasil perde US$ 10 bilhões por ano com cibercrime**, diz McAfee, 21 fev. 2018. Disponível em: https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/. Acesso em: 12 jan. 2021.

VIEIRA, Leonardo Marques. A problemática da inteligência artificial e dos vieses algorítmicos: caso COMPAS. *In:* BRAZILIAN TECHNOLOGY SYMPOSIUM, 2019. Disponível em: https://www.lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf. Acesso em: 12 jan. 2021.

ZANATTA, R. A. F; ABRAMOVAY, R. Dados, vícios e concorrência: repensando o jogo das economias digitais. **Estudos Avançados**, v. 33, n. 96, p. 421-446, 2019. Disponível em: https://www.revistas.usp.br/eav/article/view/161303. Acesso em: 12 jan. 2021.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of na information civilization. **Journal of Information and Technology**, n. 30, p. 75-89, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754. Acesso em: 12 jan. 2021.

ZUBOFF, Shoshana. **The age of Surveillance Capitalism**: The fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.

MORELLATO, Ana Carolina Batista; SANTOS, André Filipe Pereira Reid dos. Capitalismo de vigilância e a Lei Geral de Proteção de Dados: perspectivas sobre consentimento, legítimo interesse e anonimização. **RBSD** – Revista Brasileira de Sociologia do Direito, v. 8, n. 2, p. 184-211, maio/ago. 2021.

**Recebido em:** 04/06/2020
**Aprovado em:** 09/02/2021