VIGILÂNCIA DIGITAL: PODER E CONTROLE SOBRE A PRIVACIDADE E OS DADOS PESSOAIS

Yanka dos Santos Pinto[1]

Rafael Fonseca Ferreira[2]

RESUMO

Este artigo investigou o poder e controle social derivado do capitalismo de vigilância digital. O avanço tecnológico modificou o poder e o controle, instalando uma rede de vigilância centrada em coletar informações privadas. O Brasil ainda está atrasado em relação ao cenário internacional, concentrando-se nas mãos das grandes empresas de tecnologia da informação e comunicação os dados pessoais e a privacidade dos indivíduos. O Estado deve garantir proteção à privacidade e ao tratamento de dados, observando o contexto global, ampliando e complementando legislações existentes por meio de regulações e políticas públicas, buscando meios alternativos como a educação.

Palavras-chave: Poder digital. Controle Social. Privacidade. Dados pessoais. Vigilância digital.

[1] Mestranda em Direito e Justiça Social pela Universidade Federal do Rio Grande (FURG) e advogada.

[2] Doutor e Mestre em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS), professor efetivo da Universidade Federal do Rio Grande (FURG) e advogado.

1 INTRODUÇÃO

A incorporação das novas tecnologias da informação e comunicação no cotidiano da população expandiu a sistematização de dados pessoais e, consequentemente, o monitoramento dos indivíduos, que ganha possibilidade de captar as informações privadas à distância, de forma automatizada e em tempo real, abandonando os meios tradicionais de controle social. Na sociedade digital, há incontáveis maneiras de se alcançar e processar os dados pessoais dos cidadãos visíveis para as grandes empresas de tecnologia.

Esses dados funcionam tanto para o mercado econômico na venda de informações pessoais para o direcionamento de produtos e serviços quanto na previsão de padrões comportamentais para controle sobre os indivíduos com a intenção de modificá-los atendendo aos comandos do poder tecnológico (Zuboff, 2021). As plataformas digitais buscam a extração ao máximo dos dados pessoais nas redes, refinam as informações dos usuários-consumidores e antecipam o que o indivíduo quer e o que ele irá fazer a seguir, e, se for o caso, manipulam as ações humanas para agir de determinada maneira (Zuboff, 2021).

Esse modelo de capitalismo de vigilância usa a tecnologia para analisar uma quantidade massiva de dados e produzir lucro, informação e controle de mercado. Em contraste, os indivíduos ficam submetidos ao sistema tecnológico de vigilância e a sua privacidade e seus dados pessoais são diariamente violados em razão da manutenção e fortalecimento de poder digital e do controle social. Esta pesquisa pretende investigar o poder e controle social derivado das novas tecnologias, bem como explorar o funcionamento do capitalismo de vigilância digital em relação às informações privadas. Ainda, objetiva-se identificar caminhos possíveis no tocante à proteção e tratamento de dados pessoais e do direito à privacidade.

Para o desenvolvimento da pesquisa utilizou-se da revisão de literatura, por meio da técnica de pesquisa de documentação indireta, promovendo uma pesquisa bibliográfica e exploratória, recorrendo a autores como Byung-ChulHan, Bruno Bioni, ShoshanaZuboff, ZigmuntBauman, entre outras obras, periódicos, trabalhos acadêmicos e artigos científicos voltados para o tema capitalismo de vigilância, proteção de dados e direito à privacidade na era digital. O método de abordagem adotado foi hipotético-dedutivo, a partir do estabelecimento de um problema, neste caso o poder e controle sobre a privacidade e dados pessoais pelas grandes empresas de tecnologia da informação e comunicação, e a formulação de uma hipótese

para expressar as consequências derivadas do problema, como a violação do direito à privacidade e aos dados pessoais e a necessidade de proteção deles pelo Estado.

O texto inicia-se pela observação sobre os aspectos do poder digital e o controle social a partir do processamento de dados pessoais, e como o uso dessas informações manipula o comportamento humano, de modo que interfere na privacidade de pessoas e na violação de seus dados, valendo-se do método de procedimento estruturalista. Após, procura uma explicação de fenômenos estruturais da realidade, no qual se discute o monitoramento dos dados pessoais e a vida privada destas, as quais são mediadas pelos recursos tecnológicos, considerando os interesses da rede pela vigilância digital. Por fim, por meio do método de procedimento comparativo ao explicar semelhanças e dessemelhanças entre o caráter nacional e internacional, são analisados determinados aspectos de instrumentos regulatórios, bem como são apontadas algumas medidas de contenção do poder digital.

2 PRIVACIDADE E DADOS PESSOAIS: FONTE DE PODER DIGITAL E CONTROLE SOCIAL

Na modernidade líquida de Bauman (2001), o poder sobre a sociedade navega em todos os lugares, para além da extraterritorialidade proporcionada pelas redes eletrônicas e do controle pelos cidadãos, sua condição ideal de proliferação e dominação é a invisibilidade. Assim, na era da informação, o regime disciplinar se desfaz em redes abertas (Han, 2022) de controle social, no qual o poder permanece invisível, ao passo que é imposta aos súditos uma visibilidade diária (Han, 2022). Desta forma, o regime digital apropria-se das técnicas de disfarce oferecidas pelo poder disciplinar[3]e transforma seu domínio em exploração da liberdade e privacidade das pessoas com a intenção de angariar o maior número de informações possíveis do indivíduo e, por conseguinte, conduzir suas ações, seus comportamentos, seus interesses e suas vontades.

[3] Poder disciplinar é um conceito desenvolvido por Michel Foucault na sua obra "Vigiar e Punir: nascimento da prisão" (1987), consistindo na função de "adestrar" para retirar e se apropriar ainda mais e melhor. Este poder procura separar, analisar e diferenciar os processos de decomposição das forças até as singularidades necessárias e suficientes, funcionando como uma economia calculada e permanente.

Em contraste ao modelo do poder disciplinar, a conexão e a hipercomunicação tornam possível o controle total dos cidadãos (Han, 2018), provocando à sociedade hiperconectada uma constante preocupação em exercer um bom desempenho, substituindo o sujeito da obediência pelo sujeito mais rápido e eficiente (Teixeira; Sparemberger, 2020). Nas palavras de Han (2022, p. 17): "vigiar e punir, as características do regime disciplinar de Foucault, dão lugar a motivar e otimizar". Logo, o poder digital abandona os métodos coercitivos e de proibição disciplinares e adota meios informatizados de incentivo à atuação descomedida dos sujeitos em prol da maximização dos comandos.

Com as tecnologias da informação e comunicação, o medo dá lugar à exibição do ser, onde a liberdade e o controle misturam-se, considerando que a vigilância e a dominação são uma parte inerente da comunicação digital (Han, 2018). O biopoder é alterado para o psicopoder, enquanto a sociedade disciplinar biopolítica é convertida em uma sociedade da transparência psicopolítica, em que a vigilância digital auxilia na decodificação e moderação de pensamentos (Han, 2018).

A psicopolítica domina o comportamento social das massas ao acessar o inconsciente-coletivo da sociedade e, com isso, programa e controla as ações sociais futuras da coletividade, desenvolvendo, portanto, traços totalitários (Han, 2018). A modulação comportamental das técnicas digitais anuncia uma sensação de liberdade ao mesmo tempo em que comina determinadas restrições ou limita as escolhas das pessoas às opções disponibilizadas pelo poder digital (Meireles, 2021). No mesmo sentido afirma Eli Pariser (2012, p. 145) sobre a liberdade fictícia e o controle social:

> A grande promessa da tecnologia é nos dar mais liberdade e mais controle sobre o mundo – lâmpadas que respondam aos nossos caprichos e humores, telas e projeções que nos permitam focar nossa atenção apenas nas pessoas que nos interessam, de modo que não precisemos nos dar ao trabalho de viver. A ironia é que elas nos oferecem essa liberdade e controle retirando-os de nós.

Nota-se que a exposição nas redes de comunicação, enquanto reflexo da liberdade, é paradoxalmente a fonte de monitoramento e controle de organizações no qual o ser humano faz parte de um ciclo infinito de armazenamento e utilização de informações (Szinvelski; Arceno; Francisco, 2019). Desta forma, "na sociedade digital, as pessoas não se sentem realmente vigiadas ou ameaçadas, mas, pelo contrário, sentem-se livres" (Negri; Oliveira; Costa, 2020, p.

88), no entanto, essa sensação de liberdade pautada na ausência de poder-lei e que faz os usuários falarem cada vez mais sobre si é fruto das formas de desenvolvimento do poder na Internet (Pisa, 2014).

O capitalismo das grandes corporações de tecnologia busca o controle econômico e político dos indivíduos a partir da coleta, armazenamento e análise de seus dados, ao mesmo tempo em que os trata como usuários-consumidores das plataformas digitais de tecnologia da informação e comunicação (Fornasier; Knebel, 2021). Os modelos de negócios estabelecidos no processamento de dados possibilitam um poder permanente sobre os cidadãos, com vista de obter informações privadas para formação de perfis detalhados de cada cliente e posteriormente fazer uso na previsão e avaliação dos seus respectivos comportamentos (Masseno, 2019). O regime digital funda-se em uma cultura de controle social por meio da predição e intervenção derivado da simulação e incitação à realização e obtenção de resultados (Bruno, 2008).

As ferramentas eletrônicas têm acesso a todos os dados pessoais existentes on-line e, à medida que os perfis dos sujeitos são aperfeiçoados, aumenta a capacidade de modificar o comportamento humano (Pariser, 2012). O principal objetivo do poder digital é adquirir um conjunto de informações privadas para agir sobre similares, categorizando condutas e visando à simulação de comportamentos futuros (Bruno, 2008).

A mineração de dados é uma técnica que "consiste num mecanismo automatizado de processamento de grandes volumes de dados cuja função central é a extração de padrões que gerem conhecimento" (Bruno, 2008, p. 13). Com efeito, permite a indução de fatos e padrões não espontâneos e orquestrados (Szinvelski; Arceno; Francisco, 2019) com a finalidade de se apoderar dos indivíduos enquanto elabora seus perfis de comportamento (Han, 2022).

O regime de informação envolve tanto categorização dos cidadãos operada pela tecnologia quanto à influência nas ações humanas, de modo a filtrar conteúdos e aconselhar rotas (Meireles, 2021), uma vez que a sociedade é compreendida pelo poder como um sistema social calculável (Han, 2022). Nessa lógica, "o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais" (Zuboff, 2021, p. 22) e, com isso, essas informações possam ser processadas e comercializados no mercado de predição comportamentais de forma a antecipar o ato do indivíduo (Zuboff, 2021). Sendo assim, nota-se o comportamento se converter em uma mercadoria (Pariser, 2012).

Nesse quadro, pode-se afirmar que a Internet é uma rede de controle, e o mundo informatizado provocou um capitalismo em permanente vigilância ante sua enorme capacidade de "monetizar e extrair valor do material cru composto por nossas relações sociais cotidianas, graças à ubiquidade dos smartphones, computadores e barateamento dos custos de coleta e transmissão de informações" (Zanatta; Bioni, 2020). Assim, as companhias de plataformas digitais de extração de dados estão interessadas apenas em obter os dados e comportamentos pessoais da sociedade e convertê-los em predições vendáveis no mercado (Olivieri; Castro, 2021).

O controle social é exercido com intenção de gerar padrões comportamentais lucrativos, que encaminham a sociedade para resultados economicamente satisfativos às grandes organizações. A maneira encontrada para se atingir as condutas das pessoas consiste na intervenção na fonte, aumentando a certeza por meio de certas atividades que incentivam, sintonizam, vigiam, manipulam e modificam o comportamento em direções específicas (Zuboff, 2021), pois "a digitalização, ou seja, o mundo informatizado, não é nada sólido ou tenaz. Ao contrário, é moldável e manipulável à vontade" (Han, 2022, p. 93) do regime digital. Os cientistas de Big Data acreditam que o monitoramento deixou de ser apenas um meio de sintetizar uma grande quantidade de dados de um sistema e passou a ser uma atuação à distância com a habilidade de reintroduzir na sociedade as informações coletadas e usá-las para controlar e forçar as pessoas a adotarem comportamentos específicos (Olivieri; Castro, 2021).

A quantidade de dados processada, analisada, padronizada e armazenada não é somente para benefício do mercado, mas também para controle e modificação de comportamentos em razão do potencial de manipulação das informações pessoais em prol tanto de questões comerciais quanto políticas (Silva; Siqueira, 2019). Por isso, a necessidade dos gigantes da internet em acumular cada vez mais dados sobre os membros da sociedade e usá-los para adaptar suas experiências (Pariser, 2012). Em contrapartida a isto, o cidadão é incapaz de perceber o objetivo oculto na coleta de informações por organizações complexas, escapando a ele o perigo no uso de dados por parte das grandes empresas (Baião; Gonçalves, 2014).

> Com a crescente utilização dos meios tecnológicos, e sem uma regulamentação adequada, há o evidente risco de abusos tais como a utilização não autorizada de dados para disparo de campanhas publicitárias e a comercialização dos dados pessoais para outros fins que não aqueles para os quais foram coletados (Teixeira; Sparemberger, 2020 p. 40).

Até nas situações mais rotineiras da vida, as pessoas são estimuladas a exibir a sua persona nas plataformas digitais de informação e comunicação, bem como a dispor de suas informações privadas para obtenção de um resultado. O acesso a esses dados pessoais funciona como combustível para manutenção do capitalismo digital (Teixeira; Sparemberger, 2020) e o cidadão "queda-se refém de uma estrutura social que lhe deixa ao restrito papel de rendição de seus dados, mascarada de voluntariedade, ou o ostracismo que impossibilita o trabalho ou o lazer" (Fornasier; Knebel, 2021, p. 1012). Agora, detalhes pessoais, outrora eram perdidos no fundo da memória do indivíduo, tornam-se dados perenes e indefinidamente estocáveis (Bruno, 2008) pertencentes as grandes corporações enquanto objeto de armazenamento e desenvolvimento de técnicas personalizadas para controle e aperfeiçoamento comportamental.

Embora haja uma preocupação dos usuários-consumidores com a privacidade dos dados e/ou uma remota desconfia de eventual monitoramento de suas ações por parte das grandes companhias, essa relutância é superada em virtude das estratégias adotadas por essas empresas, seja ao oferecer custos mais baixos ou apresentar o controle como uma função divertida, interativa, competitiva e satisfatória a partir de recompensas e melhorias no sistema, como também incitar uma noção de inevitabilidade e impotência nos sujeitos (Zuboff, 2021). Os dados pessoais tornaram-se moeda de troca para a utilização de serviços prestados gratuitamente nas plataformas digitais (Souza; Machado; Avelino, 2017), e sua recusa em participar do compartilhamento de dados ocasiona a limitação da funcionalidade do produto e da segurança de dados (Zuboff, 2021).

Essa nova forma de exploração da sociedade seduz as pessoas ao apresentar as facilidades e individualidades dos seus produtos e serviços, e a partir desse véu a autonomia comportamental dos indivíduos é confinada e colocada em risco com o objetivo de desenvolver uma propaganda direcionada para um produto específico (Silva; Siqueira, 2019). Ao indivíduo resta consentir ou de deixar de consentir ou eliminar dispositivos da vida cotidiana em razão da incerteza do nível de informações pessoais captadas (Szinvelski; Arceno; Francisco, 2019) pelas grandes corporações em prol do mercado de consumo.

Acompanhada dessa tamanha concentração de conhecimento sobre todos os indivíduos da população, vem uma profunda centralização de poder na tecnologia digital, porque a imensa massa social depende desses meios eletrônicos na sua vida cotidiana (Olivieri; Castro, 2021). As empresas têm a possibilidade de alcançar uma personalização baseada nos

padrões de comportamento dos clientes, nos bens ou serviços que possam complementar as experiências de consumo, na localização dos usuários-consumidores e, ainda, nas negociações conduzidas por programas inteligentes, estabelecendo diálogo entre a máquina e os clientes (Masseno, 2019).

Nota-se que para além do pré-requisito ou comprometimento dos serviços, há a propagação de ser inevitável a concessão de dados pessoais, onde a liberdade humana é atingida enquanto a resistência e a criatividade são apagadas dos membros da sociedade (Zuboff, 2021). Segundo declara Zuboff (2021, p. 273): "a retórica da inevitabilidade é uma fraude astuta projetada para nos tornar indefesos e passivos diante de forças implacáveis que são e sempre devem ser indiferentes ao que é meramente humano". O mundo digital e, portanto, o capitalismo da informação, não está interessado em defender os cidadãos, ao contrário, a tecnologia trabalha para proteger fortemente o seu poder sobre a sociedade e seus dados pessoais.

3 REDE DE VIGILÂNCIA DIGITAL: USO DAPRIVACIDADE E DADOS PESSOAIS

Na era digital da informação, a comunicação transforma-se em vigilância (Han, 2022). Assim sendo, o monitoramento dos indivíduos deixa de acontecer diretamente e passa a ser mediada pela concessão de dados (Lott; Cianconi, 2018). Deste modo, a internet assumiu a função de instrumento indispensável de monitoramento, controle, observação, classificação, registro e checagem (Souza; Machado; Avelino, 2017), facilitando a estocagem e recuperação de informações que em razão do domínio sobre o cotidiano das ações dos indivíduos (Bruno, 2008) fruto da disposição de dados nas plataformas digitais. O mundo real é compilado constantemente por celulares, carros, lares, lojas, cidades e devolvido ao reino digital, onde esses dados são transformados em predições (Zuboff, 2021).

> Dentre as ferramentas utilizadas estão os sistemas de geolocalização, sistemas de controle de trânsito (particulares ou públicos para o controle de pedestres ou veículos), mecanismos de autenticação (senhas, biometrias, reconhecimento de movimento, etc.), cartões magnéticos, sistemas online, mecanismos de busca, webcams pessoais, entre outros (Lott; Cianconi, 2018, p. 122).

Isso significa que a sociedade vive sob o monitoramento diário, protagonizado pelo avanço tecnológico, a partir de dados pessoais cedidos voluntariamente às organizações privadas ou pela vigilância ostensiva não consentida (Negri; Oliveira; Costa, 2020). Por ser considerada útil na rotina das pessoas, a vigilância não é percebida como punitivista, intrusiva ou controladora (Meireles, 2021), porque a noção de vigilância não está mais concentrada no confinamento dos corpos, e sim na dinâmica da comunicação entre os indivíduos e todo o espaço de circulação de mensagens (Souza; Machado; Avelino, 2017). Embora na teoria o conceito de vigilância, no que diz respeito à observação de informações pessoais de modo rotineiro e sistemático com propósito de controlar e influenciar as ações das pessoas, não possa ser alterado; na prática, seus métodos adaptaram-se à sociedade tecnológica, principalmente os mecanismos voltados para observação e cerceamento de indivíduos, identificando e reconhecendo padrões de comportamento de forma automática e massiva (Lott; Cianconi, 2018).

Os sistemas de informação e comunicação tornam-se potenciais meios de tecnologias de vigilância (Bruno, 2008), cuja função é monitorar progressivamente as emoções das pessoas a partir da coleta de dados disponíveis nas redes digitais (Teixeira; Sparemberger, 2020). As mídias sociais exploram a experiência dos usuários, exercendo o paradoxo da liberdade controlada, logo, a capacidade do indivíduo expressar sentimentos e ações de acordo com parâmetros já determinados (Meireles, 2021) pelas próprias regras de monitoramento aplicadas nas plataformas digitais. Portanto, o capitalismo de vigilância apresenta aos cidadãos modelos de conexão social, acesso à informação, economia de tempo e a ilusão de uma rede de apoio. (Zuboff, 2021). Nessa perspectiva, expressa Floridiet al. (apud Negri; Oliveira; Costa, 2020, p. 85) sobre fatores que possibilitam o crescimento da ciência de dados e técnicas digitais:

> [...] esse movimento foi desencadeado pelos seguintes fatores: a criação de métodos estatísticos e probabilísticos cada vez mais sofisticados; a disponibilidade de ampla e crescente quantidade de dados; a acessibilidade a um enorme, e relativamente barato, poder computacional; e a transformação cada vez maior dos ambientes com as novas tecnologias de informação, como a automação residencial e a criação de cidades inteligentes.

No campo da vigilância, os dados pessoais somente ganham sentido quando analisados e classificados de maneira a produzir conhecimentos sobre a realidade ou indivíduos que permitam governar as suas condutas (Bruno, 2008). Para o futuro digital, as pessoas não são essenciais para atividade do mercado, tampouco para a obtenção de controle sobre suas próprias experiências e comportamentos, mas apenas meros recursos naturais humanos (Zuboff, 2021). Todo movimento feito pelo usuário é salvo e rastreável, "nossa vida digital se forma de modo exato na rede. A possibilidade de um protocolamento total da vida substitui a confiança inteiramente pelo controle. No lugar do Big Brother, entra o Big Data" (Han, 2018, p. 38). O monitoramento integral da vida nas redes digitais é a consumação do capitalismo de vigilância.

As noções de intimidade, liberdade, segurança e privacidade tomam novas formas ante a sociedade de vigilância (Teixeira; Sparemberger, 2020). Nesse contexto de armazenamento, tratamento, compartilhamento e monetização de informações; é imperioso definir a concepção de privacidade e proteção de dados pessoais que deverão nortear os avanços tecnológicos (Magrani, 2019). Apesar de consistir em termos inter-relacionados, a privacidade versa sobre o direito ao domínio de suas próprias informações e a construção da sua esfera particular, ao passo que a proteção de dados pessoais constitui uma garantia instrumental derivada da privacidade (Magrani, 2019). A proteção de dados pessoais é uma espécie do qual a privacidade é gênero.

Houve uma evolução na compreensão de privacidade em virtude das técnicas digitais, introduzindo a noção de proteção de dados pessoais e, consequentemente, passando a abranger para além do controle do indivíduo sobre suas informações particulares, também o direito selecionar o que deseja expor à sociedade. Portanto, as novas dimensões contemporâneas que perpassam a esfera privada e as informações pessoais foram acrescentadas à percepção tradicional de privacidade. No entanto, a proteção de dados pessoais não pode ser restringida a uma mera extensão de um direito principal como privacidade, mas enquanto uma garantia fundamental autônoma, que merece ser especificamente regulamentada (Negri; Oliveira; Costa, 2020).

Não obstante, a inovação tecnológica não está disposta a resguardar todos os dados do usuário somente para ele, uma vez que o avanço da tecnologia necessita de matéria-prima humana para divulgar as informações das pessoas (Pisa, 2014) e manter o poder digital das grandes corporações sobre o futuro da sociedade. Assim, relação ao direito à privacidade, este opera-se como uma via de mão única (Pisa, 2014), quando na verdade deveria ser conferido aos indivíduos "um poder de controle direto e contínuo sobre os coletores de informações,

independentemente da existência real de uma violação" (Baião; Gonçalves, 2014, p. 19), deslocando a proteção negativa da privacidade para o funcionamento de regras sobre a circulação de informações pessoais (Baião; Gonçalves, 2014). Nas palavras de Szinvelski, Arceno e Francisco (2019, p. 141) sobre os potenciais danos provocados por uma regularização precária da privacidade e da proteção de dados:

> [...] ausência de transparência que leva ao consentimento não informado ou a coleta não autorizada de dados pessoais; a noção de resguardo à dignidade humana e o livre desempenho da personalidade e da autodeterminação informativa, na construção da identidade própria da pessoa e não identidade que menospreza a singularidade de cada um; e a ideia de democracia e poder, no sentido de coibir o monopólio de informações e a utilização abusiva dos dados pessoais para finalidades deturpadas e não compatíveis com a construção republicada de uma sociedade global e pautada pelo respeito intercultural.

Desta forma, nota-se a necessidade em tutelar os dados das pessoas que poderiam sofrer qualquer perda de dignidade ou autonomia, embora tenha consentido para coleta, tratamento e difusão das suas informações com a intenção exclusiva de obter determinados serviços (Baião; Gonçalves, 2014). A submissão da sociedade aos termos do mundo digital culmina em "uma armadilha perigosa para os próprios indivíduos, que consentem silenciosamente com os dispositivos de vigilância" (Negri; Oliveira; Costa, 2020, 94), sem perceber que essas invasões diárias na esfera privada afastam o controle do sujeito sobre seu espaço de construção da identidade e da proteção à dignidade humana (Negri; Oliveira; Costa, 2020). A percepção de intimidade que conhecemos está comprometida, se não eliminada, (Zuboff, 2021) pelo interesse do capitalismo de vigilância.

Mesmo que informações privadas sejam compartilhadas publicamente nas plataformas digitais e outras mantidas no sigilo, o controle dos dados pessoais deve estar nas mãos dos indivíduos, no seu zelo em mantê-las distantes do público em geral (Negri; Oliveira; Costa, 2020) e principalmente da necessidade de proteger os cidadãos contra discriminações e elaboração de perfis particulares que poderiam resultar em tratamentos desiguais (Baião; Gonçalves, 2014). Assim, "[...] os problemas aos quais se dirigem os apelos por autocontrole não podem ser entendidos como excessos, equívocos, descuidos nem lapsos de julgamento. São

uma necessidade da lógica de acumulação reinante e seus implacáveis imperativos econômicos" (Zuboff, 2021, p. 301).

Em tempo, Baião e Gonçalves (2014) alertam sobre a urgência em superar a concepção tradicional individualista de privacidade e introduz a sua compreensão em uma dimensão coletiva, considerando que as pessoas são parte de determinados grupos sociais, portanto, a privacidade prolonga-se sobre a coletividade. Para Baião e Gonçalves, (2014) a circulação de informações pessoais não pode ser tratada como propriedade exclusiva do interessado, na qual o indivíduo tem liberdade para negociar sua cessão, mas sim como extensão da coletividade atrelada às consequências sociais e às do próprio particular, onde o recolhimento de dados pessoais deve observar valores diversos daqueles puramente do proprietário da informação. No mesmo sentido, posiciona-se Bruno Bioni (2017, p. 57) quanto à ideia de entendimento da vida privada nas redes digitais como bem jurídico coletivo:

> Esse é um passo importante a ser dado para se pensar proteção de dados pessoais, não somente como um direito individual, mas, também, transindividual. Isto é, de um grupo de pessoas, ou toda uma população, que tem a sua vida impactada pela infraestrutura informacional do ambiente no qual estão inseridos.

A noção de proteção de informações privadas enquanto direito transindividual amplia as garantias fundamentais outorgadas aos cidadãos, bem como dá margem para o estabelecimento de novos mecanismos normativos de tutela da sociedade na Internet. No entanto, independentemente da visão individual ou coletiva, "transparência e privacidade são obstáculos para os capitalistas de vigilância" (Zuboff, 2021, p. 301).

4 CAMINHOS DE PROTEÇÃO À PRIVACIDADE E DADOS PESSOAIS NA ERA DIGITAL

Ante a redução do ser humano a dados comerciáveis e, com efeito, a modelos de vida ligados a dinâmica de consumo e o consequente crescimento econômico, podendo-se afirmar como fator desencadeador de processos de desigualdade, faz-se necessário, portanto, a busca

de um poder regulatório de tais atividades digitais. Por isso, destaca-se que este é um dos maiores desafios do século XXI, conforme será delineado a seguir.

O cidadão deve ter controle sobre o modo como o fluxo informacional impacta a sua vida (Bioni, 2017), além da existência de normativas direcionadas à proteção de direitos fundamentais exercidos nas plataformas digitais de tecnologia da informação e comunicação, "de modo que o Direito precisa atuar em defesa dos usuários contra a comercialização dos dados coletados para fins que extrapolam o uso da rede e abusos contra a moderação de conteúdo discricionária" (Poletto; Morais, 2021, p. 601). Assim, considerando a capacidade das empresas em armazenar uma grande quantidade de informações pessoais e, consequentemente, controlar o cotidiano das pessoas, as regras constritivas não são suficientes para proteção da privacidade e dos dados íntimos, portanto, faz-se imperioso o desenvolvimento de garantias constitucionais para os direitos da rede (Szinvelski; Arceno; Francisco, 2019).

De acordo com Baião e Gonçalves (2014), existem alguns princípios que devem ser levados em consideração no tratamento da privacidade e controle de dados pessoais, e não apenas os já consolidados princípios do consentimento e do acesso individual: a) princípio da finalidade, onde o uso e coleta das informações privadas devem obedecer ao fim anteriormente comunicado ao interessado; b) princípio da publicidade, em que é assegurado aos indivíduos o exercício de poder sobre a circulação de suas informações e os meios de utilização; c) princípio da segurança física e lógica da coletânea dos dados, protegendo as pessoas contra os riscos de extravio, destruição, modificação, transmissão ou acesso não autorizado dos seus dados; d) princípio da temporalidade, no qual as informações são conservadas no limite da realização do objetivo do interessado; e) princípio da relevância e da proporcionalidade, referente à coleta de dados pessoais deve ser mínima e com propósito específico.

> Por isso, a transparência (i) de quais dados serão coletados, (ii) dos métodos na coleta de dados orientados de acordo com a finalidade anuída, (iii) dos programas de segurança e de correção de falhas da tecnologia adotados pela organização mostram-se o ideal democrático a ser perseguido em matéria de proteção de dados, por deixarem claro ao titular dos dados pessoais o objeto do consentimento, especialmente no contexto em que a tecnologia avança com intensa rapidez e utiliza os dados pessoais como "matéria prima" (Szinvelski, Arceno e Francisco, 2019, p. 140).

Observa-se a complexidade apresentada ao Estado Democrático de Direito em harmonizar a proteção da privacidade e dos dados íntimos com as tecnologias (Szinvelski; Arceno; Francisco, 2019). No Brasil, o termo "proteção de dados pessoais" foi introduzido no ordenamento jurídico com o Marco Civil da Internet (Lei n. 12.1965/14), enquanto na Europa já se debatia o tema desde a década de 1970, evidenciando uma ausência de tradição regulatória quanto à tutela da vida privada e da liberdade nas redes digitais, o que não deve impedir a adoção de novos instrumentos de proteção de dados e do direito à privacidade (Szinvelski; Arceno; Francisco, 2019), como a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18) e o Projeto de Lei n. 2.630/20 (Lei das *Fake News*), e inspirando-se na legislação internacional.

Em 1977 nos Estados Unidos, um grupo de trabalho, liderado por David Linowes (1917-2007), publicou um relatório (PersonalPrivacy na Information Society) sobre a regulação da proteção de dados pessoais no país, concluindo que há um enorme desequilíbrio entre os registros dos indivíduos e a organização. Em contrapartida, a política de funcionamento das empresas visa apenas fortalecer a participação das pessoas (Zanatta; Bioni, 2020). Em tempo, os pesquisadores fizeram três recomendações políticas a serem colocadas em prática: a) proibição ou restrição de práticas de coleta de dados injustificadamente intrusivas; b) concessão do controle ao indivíduo sobre a divulgação de seus registros; c) outorga de direitos básicos individuais e obrigações de incorporar proteções à privacidade pessoal em suas atividades rotineiras de manutenção de registros (Zanatta; Bioni, 2020).

No cenário europeu, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), que aborda o direito à autodeterminação do titular das informações, bem como o direito de se opor ao tratamento dos dados pessoais (Masseno, 2019). Neste último caso, é garantida ao indivíduo a oposição ao processamento das suas informações íntimas, definição de perfis com base nos dados coletados e/ou a sua comercialização direta (Masseno, 2019). Além disso, o regulamento acrescenta uma previsão de responsabilidade civil objetiva e solidária aos responsáveis pelo tratamento de dados pessoais (Masseno, 2019), como também o desenvolvimento de relatórios de impacto à proteção de dados pessoais em que o controlador tem a obrigação de executá-lo nas situações que representam alto risco à defesa dos dados (ZANATTA; Bioni, 2020).

Da mesma maneira, a Lei Geral de Proteção de Dados Pessoais (LGPD) assemelha-se em vários aspectos à legislação europeia, dentre eles o seu caráter multissetorial e transversal (Teixeira; Sparemberger, 2020), no qual "a lei aplica-se às pessoas naturais e às pessoas de

direito público e privado, respeitadas algumas peculiaridades de cada setor para qualquer operação de tratamento de dados pessoais" (Teixeira; Sparemberger, 2020, p. 41). Constata ainda Rafael Zanatta e Bruno Bioni (2020) que a LGPD prevê uma dimensão principiológica de precaução, estabelecendo comandos normativos abertos de estímulo ao setor privado, propondo os autores a instituição de práticas de incentivo por meio de políticas tarifárias e tributárias.

Diversamente do regulamento europeu, a legislação brasileira não traz minimamente detalhamentos procedimentais, deixando essas questões para posterior regulação pela Autoridade Nacional de Proteção de Dados Pessoais, além de versar sobre a avaliação de impacto como uma possibilidade e não enquanto uma obrigação regulatória(Zanatta; Bioni, 2020).Os mecanismos de construção participativa dos relatórios de impacto também ficaram em aberto, existindo a possibilidade de inclusão deinstrumentos definidos pelas próprias empresas e de uma ferramenta de controle e monitoramento capaz de discutir publicamente como esses relatórios são realizados, desde os métodos até os direitos fundamentais afetados pelo tratamento de dados (Zanatta; Bioni, 2020).

Uma medida alternativa de proteção dos dados pessoais e do direito à privacidade éa alfabetização digital dos indivíduos, conferindo aos usuários das plataformas de mídia mais autonomia para verificar a confiabilidade de determinados comandos e diminuindo sua vulnerabilidade em relação às manipulações (Sampaioet al., 2021). A educação digital pode ser chave fundamental na construção de um senso crítico quanto ao uso das tecnologias de informação e comunicação (Sparemberger; Silva, 2021). A aplicação de políticas públicas voltadas para alfabetização tecnológica deve partir de um processo pedagógico amplo envolvendo as plataformas digitais e a escola (Intervozes, 2021), considerando o papel conscientizador desempenhado pela educação na vida das pessoas.

Assim, os efeitos da esfera pessoal estendem-se na direção de uma sociedade organizada (Szinvelski; Arceno; Francisco, 2019). Nessa lógica, Bruno Bioni (2017, p. 58) sinaliza parâmetros para o desenvolvimento de uma narrativa ecológica de proteção de dados pessoais na sociedade:

> [...] identificar como todo o aporte teórico da ecologia detém desdobramentos bastante práticos em termos do que se idealiza com o uso intensivo de TIC nos centros urbanos [...] para que haja: i) Um controle mais significativo dos

> cidadãos sobre seus dados, a partir da premissa de que a tecnologia é um elemento desencadeador dessa habilidade (ecologia da privacidade); ii) O desenvolvimento de tecnologia de transparência sobre o uso que se faz de tais dados e de toda a infraestrutura informacional da cidade (meta tecnologias e redução da assimetria de informação); iii) O reconhecimento de uma dimensão coletiva da proteção dos dados pessoais, levando-se em consideração que o comportamento de grupos da população, ou dela como um todo, é modulado pela agregação e processamento massivo dos dados dos indivíduos (caráter transindividual da proteção dos dados pessoais) (Bioni, 2017, p. 58).

Sendo assim, o Direito deve estabelecer uma barreira à violação do direito à privacidade e ao tratamento de dados e um escudo contra o arbítrio dos senhores da informação, que se apresentam no despotismo tecnológico, e a favor dos vulneráveis usuários-consumidores (Szinvelski; Arceno; Francisco, 2019). No regime da informação, o maior obstáculo na proteção da vida privada e dos dados pessoais dos indivíduos são aqueles que detêm essas informações nas mãos.

5CONSIDERAÇÕES FINAIS

O capitalismo da informação está interessado apenas em proteger o seu poder digital sobre a sociedade e seus dados. Deste modo, o mundo digital assumiu a função de monitorar, controlar e tratar os dados coletados, facilitando a vigilância ostensiva consentida e/ou não consentida, principalmente pelo fato da tecnologia se mostrar necessária no cotidiano das pessoas, seja no consumo de produtos e serviços ou na dinâmica da comunicação, abordando questões como propaganda personalizada, reconhecimento facial, exposição da intimidade, policiamento preditivo e *fake news*.

Assim, a transparência e privacidade são vistas como barreiras na execução da rede de vigilância promovida pelos mecanismos tecnológicos e, por conseguinte, pelas grandes empresas de tecnologia da informação e comunicação. Nesse sentido, em virtude da aptidão das organizações digitais em armazenar automatizada e massivamente dados pessoais, é imperioso a instituição de regras voltadas para garantias constitucionais em relação ao direito à privacidade nas redes digitais e a proteção de dados pessoais.

No âmbito nacional e internacional, foram estabelecidas legislações dispondo sobre o tratamento de dados, no entanto, devido ao recente debate no Brasil relacionado às questões do mundo digital, comandos normativos brasileiros são preventivos e apresentam algumas lacunas no tocante aos detalhamentos procedimentais e a faculdade no desenvolvimento dos relatórios de impacto. É pressuposto de a ordem jurídica limitar o exercício autoritário das grandes corporações de tecnologia, detalhando princípios e normas constitucionais e protegendo integralmente os direitos do titular dos dados pessoais.

O Poder Público deve priorizar as garantias fundamentais dos cidadãos, compreendendo os riscos impostos pela utilização irrestrita de instrumentos tecnológicos que manipulam e controlam ações humanas por meio da mineração de dados, e pelo uso inadequado de tecnologias de vigilância, ignorando aspectos como transparência, privacidade e dados pessoais. Embora haja legislações sobre o tema, estas estão longe de ser suficientes para reduzir o controle das empresas de tecnologia da informação e comunicação perante os dados pessoais.

A rede de vigilância está despreocupada com a privacidade e os dados pessoais dos indivíduos e com propósitos econômicos e de manipulação comportamental. Sendo dever do Estado Democrático de Direito criar instrumentos de defesa do direito à privacidade e ao tratamento de dados, inspirando-se em normativas já existentes e/ou em meios alternativos de enfrentamento dos senhores da informação, por exemplo, as regulações da União Europeia, políticas públicas direcionada para a alfabetização digital.

REFERÊNCIAS

BAIÃO, Kelly C. Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**, v. 3, n. 2, p. 1-24,2014. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/151/119>. Acesso em: 18 mai. 2023.

BAUMAN, Zigmunt. **Modernidade Líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001.

BIONI, Bruno Ricardo. Ecologia: uma narrativa inteligente para a proteção de dados pessoais nas cidades inteligentes. Pesquisa TIC Governo Eletrônico, 2017. Disponível em: <https://brunobioni.com.br/wp-content/uploads/2019/05/TIC_eGOV_2017_livro_eletronico-55-62.pdf>. Acesso em: 18 mai. 2023.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **Revista FAMECOS**, Porto Alegre (RS), n. 36, p. 16-16, ago. 2008.DOI: https://doi.org/10.15448/1980-3729.2008.36.4410. Disponível em: <https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/4410/3309>. Acesso em: 18 mai. 2023.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto 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 Praxis**, Rio de Janeiro, v. 12, n. 2, 2021.DOI: 10.1590/2179-8966/2020/46944. Disponível em:<https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/46944/33907>. Acesso em: 18 mai. 2023.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

HAN, Byung-Chul. **Infocracia: digitalização e a crise da democracia**. Tradução de Gabriel S. Philipson. Petrópolis, Rio de Janeiro: Vozes, 2022.

HAN, Byung-Chul. **No exame: perspectivas do digital**. Tradução de Lucas Machado. Petrópolis, RJ: Vozes, 2018.

INTERVOZES, Coletivo Brasil de Comunicação Social. **Fake News: como as plataformas enfrentam a desinformação**. Rio de Janeiro: Multifoco, 2021.

LIPOVETSKY, Gilles. **Da leveza: rumo a uma civilização sem peso**. Tradução de Idalina Lopes. São Paulo: Manole, 2016.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da ciência da informação no Brasil. **Perspectivas em Ciência da Informação**, v. 23, n. 4, p. 117–132,out./dez. 2018. Disponível em: <https://periodicos.ufmg.br/index.php/pci/article/view/22594/18178>.Acesso em: 18 mai. 2023.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MASSENO, Manuel David. Como a União Europeia procura proteger os cidadãos-consumidores em tempos de big data. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria (RS), v. 14, n. 3, 2019.DOI: <https://doi.org/10.5902/1981369441708.Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/41708/pdf>.Acesso em: 18 mai. 2023.

MEIRELES, Adriana Veloso. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, Campinas, v. 27, n. 1, jan./abr. 2021.DOI: https://doi.org/10.1590/1807-0191202127128.Disponível em: <https://www.cesop.unicamp.br/vw/1I8PyTqIwNQ_MDA_a8afe_/Algoritmos%20e%20Autonomia%20(1)%20(1).pdf>.Acesso em: 18 mai. 2023.

NEGRI, Sergio Marcos Carvalho de Ávila; OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. **RDP**, Brasília, v. 17, n. 93, maio/jun. 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740/Negri%3B%20Oliveira%3B%20Costa%2C%202020>. Acesso em: 18 mai. 2023.

OLIVIERI, Alejandro Gabriel; CASTRO, Gustavo Javier. A sociedade digital de extração de dados e os desafios para a democracia. **Revista Processus de Políticas Públicas e Desenvolvimento Social**, v. 3, n. 6, p. 19-40, jul./dez. 2021.DOI:

<https://doi.org/10.5281/zenodo.5228500. Disponível em: https://periodicos.processus.com.br/index.php/ppds/article/view/349/433>.Acesso em: 18 mai. 2023.

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você**. São Paulo: Editora Zahar, 2012.

PISA, Lícia Frezza. Discurso e poder: o controle do que dizemos na rede visto pela política de privacidade do Google. **Domínios de lingu@gem**, v. 8, n. 1, jan./jun. 2014.DOI: https://doi.org/10.14393/DL15-v8n1a2014-14.Disponível em: <https://seer.ufu.br/index.php/dominiosdelinguagem/article/view/24624/14640>.Acesso em: 18 mai. 2023.

POLETTO, Álerton; MORAIS, Fausto. (In)sustentabilidade das redes sociais: os impactos da manipulação de dados pelas plataformas de aplicação. **Argumenta Journal Law**, Jacarezinho (PR), n. 35, jul./dez. 2021. Disponível em: <http://seer.uenp.edu.br/index.php/argumenta/article/view/2413/pdf>.Acesso em: 18 mai. 2023.

SAMPAIO, José Adércio Leite; MENDIETA, David; FURBINO, Meire; BOCCHINO, Lavínia Assis. Capitalismo de vigilância e a ameaça aos direitos fundamentais da privacidade e da liberdade de expressão. **Revista Jurídica**, Curitiba, v. 1, n. 63, 2021. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/5135/371373154>.Acesso em: 18 mai. 2023.

SILVA, Lucas Gonçalves; SIQUEIRA, Alessandra Cristina de Mendonça. A (há) liberdade de expressão na sociedade em rede (?): manipulação na era digital. **Revista Relações Internacionais do Mundo Atual**, Curitiba (PR), v. 2, n. 23, 2019.DOI: http://dx.doi.org/10.21902/Revrima.v2i23.4009.Disponível em: <https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/4009/371372329>.Acesso em: 18 mai. 2023.

SOUZA, Joyce; MACHADO, Débora; AVELINO, Rodolfo. Big Data, vigilância e o mercado de dados pessoais na saúde. **Anais V Simposio Internacional LAVITS: Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias**, Santiago (Chile), nov./dez. 2017.Disponível em: <https://lavits.org/wp-content/uploads/2018/04/07-Joyce-Souza-D%C3%A9bora-Machado-e-Rodolfo-Avelino.pdf>.Acesso em: 18 mai. 2023.

SPAREMBERGER, Raquel; SILVA, Ana Carolina EidSoares. O Impacto das fakenews no processoeleitoral brasileiro. **Revista Reflexão e Crítica do Direito**, RibeirãoPreto, v. 9, n. 2, p. 251-277, jul./dez. 2021.Disponível em: <https://revistas.unaerp.br/rcd/article/view/2438/1960>.Acesso em: 18 mai. 2023.

SZINVELSKI, MártinMarks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. **Perspectivas em Ciência da Informação**, v. 24, n. 4, out./dez. 2019. Disponível em: <https://periodicos.ufmg.br/index.php/pci/article/view/22644/18228>.Acesso em: 18 mai. 2023.

TEIXEIRA, João Paulo Allain; SPAREMBERGER, Raquel Fabiana Lopes. Da sociedade do cansaço à sociedade da vigilância: entre utopias e distopias, o direito à privacidade no contexto pós-pandemia. In: MELO,Ezilda; BORGES, Lize; SERAU JUNIOR, Marco Aurélio (org.). **COVID-19 e Direito Brasileiro: mudanças e impactos**. 1. ed. São Paulo: TirantloBlanch, 2020. E-book.

ZANATTA, Rafael; BIONI, Bruno. Direito e economia política dos dados: um guia introdutório. In: DOWBOR, Lacislau (org.). **Sociedade vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instalar uma nova distopia**. São Paulo: Autonomia Literária, 2020.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder**. Tradução de George Schlesinger. Rio de Janeiro: EditoraIntrínseca, 2021.

DIGITAL SURVEILLANCE: POWER AND CONTROL OVER PRIVACY AND PERSONAL DATA

ABSTRACT

This article investigated the power and social control derived from digital surveillance.Technological advancement modified power and social control, establishing a surveillance network focused on gathering private information for economic purposes and behavioral manipulation. Brazil is still lagging behind in relation to the international scenario, concentrating the personal data and privacy of individuals in the hands of large information and communication technology companies.The state should ensure privacy protection and data handling,observing the global context, expanding and complementing existing legislation through regulations and public policies, seeking alternative means such as education.

Keywords: Digital power. Social Control. Privacy. Personal data. Digitalsurveillance.