

**UNIVERSIDADE DE PASSO FUNDO – UPF
VICE-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGDireito
MESTRADO EM DIREITO**

Roberta de Oliveira Sutel

**PROTEÇÃO DE DADOS E DIMENSÕES DO PODER: O DIREITO NA
ERA DO CAPITALISMO DE VIGILÂNCIA**

**Passo Fundo, RS
2024**

Roberta de Oliveira Sutel

**PROTEÇÃO DE DADOS E DIMENSÕES DO PODER: O DIREITO NA ERA DO
CAPITALISMO DE VIGILÂNCIA**

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade de Passo Fundo (UPF), sob Área de Concentração “Novos Paradigmas do Direito”, com ênfase na Linha de Pesquisa “Relações Sociais e Dimensões do Poder”, como requisito parcial para obtenção do título de **Mestra em Direito**.

Orientador:
Prof. Dr. Gabriel Divan

Passo Fundo, RS
2024

CIP – Catalogação na Publicação

S965p Sutel, Roberta de Oliveira
Proteção de dados e dimensões do poder [recurso eletrônico] :
o direito na era do capitalismo de vigilância / Roberta de Oliveira
Sutel. – 2024.
1.034 KB ; PDF.

Orientador: Prof. Dr. Gabriel Divan.
Dissertação (Mestrado em Direito) – Universidade de Passo
Fundo, 2024.

1. Capitalismo de vigilância. 2. Era da informação. 3. Proteção
de dados. 4. Brasil. [Lei geral de proteção de dados pessoais
(2018)]. I. Divan, Gabriel, orientador. II. Título.

CDU: 34

Catalogação: Bibliotecária Jucelei Rodrigues Domingues - CRB 10/1569

A Comissão Examinadora, abaixo assinada, aprova a Dissertação.

“PROTEÇÃO DE DADOS E DIMENSÕES DO PODER: O DIREITO NA ERA DO CAPITALISMO DE VIGILÂNCIA”

Elaborada por

ROBERTA DE OLIVEIRA SUTEL

Como requisito parcial para a obtenção do grau de “Mestre em Direito”
Área de Concentração – Novos Paradigmas do Direito

APROVADA

Pela Comissão Examinadora em: 26/03/2024



Dr. Gabriel Antinolfi Divan
Presidente da Comissão Examinadora
Orientador



Dr. Liton Lanes Pilau Sobrinho
Coordenador PPGDireito



Dra. Josiane Petry Faria
Membro interno



Dr. Felipe da Veiga Dias
Membro externo



TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade de Passo Fundo, a Coordenação do Curso de Mestrado em Direito, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Roberta de Oliveira Sutel

Mestranda

Passo Fundo, RS
2024

Aos meus pais: Inêz de Oliveira e Roberto Sutel (em memória).

AGRADECIMENTOS

O estudo foi fundamental na minha vida; foi através dele que consegui "reconstruir" a minha vida após tantas perdas. Estudar em uma universidade particular com bolsa integral do PROUNI possibilitou tudo isso. Sou eternamente grata aos programas sociais, pois é por meio deles que diversas pessoas, como eu, filhas de dona de casa e de um padeiro, conseguem ter acesso a uma universidade de qualidade.

Após a formação em bacharelado em Direito, conquistei uma vaga no mestrado, novamente com bolsa integral, o que me permitiu ampliar os conhecimentos e me apaixonar ainda mais pela docência.

Nessa jornada do mestrado, conheci pessoas maravilhosas que acreditaram no meu potencial e me incentivaram. Em especial, ao meu orientador Gabriel Divan, que se tornou um amigo nessa árdua caminhada, e às minhas amigas/colegas Vitória, Victória, Beatriz, Gabriely e Flávia.

Em 2016 perdi meu pai e minha tia em um lapso temporal de 2 meses, este é um agradecimento especial a eles. Tenho certeza de que estão orgulhosos do caminho escolhido. E que mesmo distantes seguraram minha mão para que a desistência não fosse uma opção.

Agradeço à minha família, que nunca mediu esforços para me garantir educação. À minha mãe, Inêz de Oliveira, e à minha irmã, Graziela Iop, que foram meu alicerce, meu abrigo durante todos esses anos. Não tínhamos condições financeiras, mas tínhamos muito amor e união.

Agradeço ao Tio João e à Tia Neli (em memória) por ajudar na minha criação e estar presente em todos os momentos da minha vida. Também aos irmãos de coração Simone, Fabricio, Giorgione, Bianca e Maria Clara pelo suporte e carinho que tiveram comigo nessa trajetória. E, aos afilhados/sobrinhos que não consegui acompanhar no crescimento, mas que os pequenos encontros eram motivo de continuar: Bernardo, Maria Eduarda, Miguel e Tomás.

Aos amigos especiais que me incentivaram de alguma forma nessa caminhada, alguns secaram as lágrimas e outros foram responsáveis pelas gargalhadas: Andressa, Bianca, Fabiani, Gessica, Kati, Paola, Paulina, Regina, Luiz Henrique e Mauricio.

E, por último, agradecer ao meu companheiro de vida, Mauricio Bolzan, que acompanhou de perto toda a graduação e o mestrado. Limpou por diversas vezes as minhas lágrimas, segurou a minha mão e não deixou que eu desistisse. Também, agradecer à família Bolzan pelo amparo e carinho nesses 7 anos.

Gostaria de agradecer, nome por nome, às pessoas que passaram por esta trajetória e iluminaram o percurso, mas corro o risco de não conseguir mencionar todos. De uma forma geral, o sentimento é de gratidão aos amigos e aos familiares. Sem todo esse pessoal, não seria possível!

*Então vá em frente! Saia do sistema.
Shoshana Zuboff*

RESUMO

PROTEÇÃO DE DADOS E DIMENSÕES DO PODER: O DIREITO NA ERA DO CAPITALISMO DE VIGILÂNCIA

A presente dissertação está inserida na área de concentração Relações Sociais e Dimensões do Poder do Programa de Pós-graduação da Universidade de Passo Fundo-RS. O trabalho tem como objetivo analisar o comportamento do direito diante do capitalismo de vigilância e questionar como a nova forma de poder surgida neste capitalismo atual se relaciona com a proteção jurídica. Para responder à problemática, utiliza o método de abordagem dedutivo e o método de procedimento monográfico. A hipótese principal é que o capitalismo é um sistema em constante mudança, o que implica que as práticas de coleta e uso de dados pessoais também estão em constante evolução. Na primeira parte, o trabalho versa sobre o contexto histórico da proteção de dados no Brasil, até culminar na promulgação da Lei Geral de Proteção de Dados, incluindo exemplos de incidentes envolvendo entes particulares e administração pública. Na segunda seção, o trabalho aborda as questões de poder, onde o capitalismo de vigilância está inserido em outras dimensões de poder, ocupando o topo de uma pirâmide. No terceiro e último capítulo, o trabalho oferece um contraponto à proteção jurídica para então concluir que a relação entre o capitalismo de vigilância e a proteção jurídica não se limita apenas à implementação de regulamentações, mas também abrange abordagens complementares como a promoção da educação digital e a conscientização sobre questões de privacidade e segurança online. Essas abordagens complementam as legislações, principalmente a Lei Geral de Proteção de Dados, sendo fundamentais para lidar com os dilemas que surgem em decorrência do capitalismo de vigilância.

Palavras-chave: capitalismo de vigilância; dimensões do poder; era da informação; Lei Geral de Proteção de Dados.

ABSTRACT

DATA PROTECTION AND DIMENSIONS OF POWER: LAW IN THE AGE OF SURVEILLANCE CAPITALISM

This dissertation is part of the concentration area Social Relations and Dimensions of Power of the Postgraduate Program at the University of Passo Fundo-RS. The work aims to analyze the behavior of law in the face of surveillance capitalism and question how the new form of power that has emerged in this current capitalism relates to legal protection. To answer the problem, the deductive approach method and the monographic procedure method are used. The main hypothesis is that capitalism is a constantly changing system, which implies that practices for collecting and using personal data are also constantly evolving. In the first part, the work deals with the historical context of data protection in Brazil, until culminating in the promulgation of the General Data Protection Law, including examples of incidents involving private entities and public administration. In the second section, the work addresses issues of power, where surveillance capitalism is inserted into other dimensions of power, occupying the top of a pyramid. In the third and final chapter, the work offers a counterpoint to legal protection and then concludes that the relationship between surveillance capitalism and legal protection is not limited only to the implementation of regulations, but also encompasses complementary approaches such as the promotion of digital education and raising awareness about online privacy and security issues. These approaches complement legislation, mainly the General Data Protection Law, and are fundamental to dealing with the dilemmas that arise as a result of surveillance capitalism.

Keywords: surveillance capitalism; dimensions of power; information age; General Data Protection Law.

LISTA DE SIGLAS E ABREVIATURAS

Art.	Artigo
TIC	Tecnologias da Informação e Comunicação
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
CF/88	Constituição Federal Brasileira de 1988
STJ	Supremo Tribunal de Justiça

SUMÁRIO

INTRODUÇÃO	11
1 A PROTEÇÃO DE DADOS NO BRASIL (DESAFIOS E ADAPTAÇÕES NECESSÁRIAS PARA A LGPD LIDAR COM A REALIDADE DO FLUXO DE DADOS PESSOAIS)	14
1.1 A REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL: ELEMENTOS PARA PENSAR NA HISTORICIDADE	15
1.2 ANÁLISE DA PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA E NAS INSTITUIÇÕES PRIVADAS	23
2 A RELAÇÃO ENTRE DIMENSÕES DE PODER E A PROTEÇÃO DE DADOS ...	30
2.1 A EVOLUÇÃO DOS PODERES NA ERA DA TECNOLOGIA	31
2.2 DIMENSÕES DE PODER E SUA INFLUÊNCIA NA GOVERNANÇA DE DADOS: UMA ANÁLISE CRÍTICA	37
3 A ERA DO CAPITALISMO DE VIGILÂNCIA NA PERPECTIVA DA PROTEÇÃO DE DADOS	47
3.1 CAPITALISMO DE VIGILÂNCIA: A FUSÃO ENTRE LUCRO E CONTROLE DE DADOS	48
3.2 OS NOVOS SENHORES DO CAPITAL: PODER, INFORMAÇÃO E PROTEÇÃO DE DADOS	58
3.3 A NECESSIDADE DE ABORDAGENS COMPLEMENTARES À REGULAMENTAÇÃO NA PROTEÇÃO DE DADOS NO CAPITALISMO	68
CONSIDERAÇÕES FINAIS	82
REFERÊNCIAS.....	87

INTRODUÇÃO

A presente dissertação busca analisar, as relações de poder e as influências do Capitalismo de Vigilância após a recente Lei Geral de Proteção de Dados no Brasil, a fim de evitar práticas de inviolabilidade de dados. A dissertação enquadra-se na área de concentração Relações Sociais e Dimensões do Poder do Programa de Pós-graduação da Universidade de Passo Fundo-RS.

Com o dinamismo da tecnologia, a cada dia surgem novas formas de conectividade e comunicação entre os diversos elementos de um ambiente cooperativo e de trabalho. No entanto, o surgimento de uma tecnologia também representa novas possibilidades de ataques contra os dados pessoais dos usuários.

Durante o século XXI a sociedade moderna está passando por uma revolução denominada revolução informacional. Essa revolução decorre da crescente utilização das Tecnologias da Informação e Comunicação (TIC), a qual permite que questões de tempo e distância, tenham sua amplitude reduzida, facilitando o acesso ao conhecimento e a informação em qualquer ponto no planeta, desde que haja um acesso à *internet*.

Entretanto, a velocidade decorrente da *internet* e do grande fluxo de informação das redes sociais, deixam o ser humano em posição de vulnerabilidade, colocando à prova a Constituição da República e o arcabouço legislativo nacional, no que toca ao direito à privacidade e a proteção de dados pessoais.

O capitalismo da vigilância é uma nova dimensão de poder, talvez o maior poder atuante nessa geração, e esse poder ameaça a sociedade por ser capaz de manipulá-la em todas os seus aspectos. Diante deste contexto, a questão central do trabalho reside em questionar como a nova forma de poder emergente neste atual modelo de capitalismo se relaciona com a proteção jurídica.

Para responder a esse questionamento, adota-se o método dedutivo que parte de uma análise ampla da Proteção de Dados e da privacidade na sociedade informacional para uma abordagem mais específica do capitalismo de vigilância como dimensões de poder. Quanto ao método de procedimento, é utilizado o monográfico, devido à análise e estudo da Lei Geral de Proteção de Dados.

A hipótese principal do presente trabalho é de que o capitalismo é um sistema em constante mudança, o que significa que as práticas de coleta e uso de dados pessoais também estão em constante evolução.

Assim, uma abordagem estática e rigorosa para a proteção jurídica poderia não ser eficaz em lidar com as novas formas de coleta e uso de dados pessoais que surgem constantemente. Por outro lado, abordagens complementares poderiam ser mais capazes de responder às mudanças no mercado de tecnologia e informação, demonstrando-se mais eficazes em garantir a proteção dos dados pessoais dos cidadãos.

O objetivo geral é analisar como a Lei Geral de Proteção de Dados (LGPD) pode estabelecer um escopo e foco adequado para lidar com a realidade atual do capitalismo, onde o setor financeiro depende do trabalho com o fluxo de dados pessoais, muitas vezes fornecidos voluntariamente, bem como analisar como a nova forma de poder surgida neste capitalismo atual se relaciona e difere da necessidade de uma proteção jurídica mais estática e rigorosa.

Por outro lado, os objetivos específicos é observar como a doutrina aborda o tratamento de dados pela administração pública ou pelos entes particulares frente aos riscos de manipulação de dados pessoais, verificar as novas formas de capitalismo e os impactos na era tecnológica. E por fim, examinar as abordagens complementares a Lei Geral de Proteção de Dados.

No primeiro capítulo, a pesquisa traz aspectos históricos da Lei Geral de Proteção de Dados no Brasil, desde a carta magna, sob a perspectiva da intimidade e vida privada, até a promulgação da Lei de nº 13.709, em 14 de agosto de 2018. Inclusive dos incidentes a essa proteção envolvendo a Administração Pública e os entes particulares.

Na sequência do trabalho, o capítulo 2 abordará assuntos que tratam da relação entre dimensões de poder e a proteção de dados. Neste capítulo, será realizada uma análise sobre como diferentes estruturas de poder e como o capitalismo de vigilância influencia o tratamento e a salvaguarda das informações pessoais dos indivíduos.

O capítulo três oferece reflexões acerca da era do capitalismo de vigilância na perspectiva da proteção de dados examinando a interseção entre a crescente economia de dados e as práticas de vigilância que têm se desenvolvido no contexto do capitalismo contemporâneo. Além disso, demonstra que as abordagens

complementares às normativas, como a educação digital, capacitação e outras iniciativas afins, são essenciais para enfrentar os desafios atuais.

Essas medidas não apenas ajudam a conscientizar os cidadãos sobre a importância da proteção de dados pessoais, mas também capacitam indivíduos e organizações a implementarem práticas seguras de maneira proativa.

Nesse sentido, é necessário entender o caminho que percorre a proteção de dados no Brasil, especialmente em relação às dimensões de poder e à era do capitalismo de vigilância. Esses aspectos são fundamentais para contextualizar a discussão e compreender como as dinâmicas de poder influenciam as práticas de proteção de dados em um contexto de vigilância intensificada.

1 A PROTEÇÃO DE DADOS NO BRASIL: DESAFIOS E ADAPTAÇÕES NECESSÁRIAS PARA A LGPD LIDAR COM A REALIDADE DO FLUXO DE DADOS PESSOAIS

No cenário contemporâneo, marcado pela crescente digitalização e interconexão global, a proteção de dados emergiu como um tema de importância inegável. No Brasil, esse tópico ganhou destaque com a promulgação da Lei Geral de Proteção de Dados (LGPD), um marco regulatório que busca equilibrar a livre circulação de informações com a salvaguarda da privacidade e da segurança das informações pessoais.

No entanto, a jornada rumo à implementação eficaz da LGPD é permeada por desafios complexos e nuances que exigem adaptações consideráveis para alinhar a lei com a realidade do fluxo de dados pessoais.

No capítulo inicial, a abordagem histórica e evolutiva da proteção de dados, delineada neste estudo, examina as principais normativas que tratam desse assunto.

Dentre essas normativas, incluem-se a Constituição Federal, o Código de Direito Penal, o Código de Direito Civil e o Código do Consumidor. A análise também se estende a duas leis preexistentes à LGPD, a saber, a Lei de Acesso à Informação (LAI) e o Marco Civil da *Internet*.

O objeto de estudo em questão não se trata de uma genealogia exaustiva no âmbito da proteção de dados em sentido amplo, mas sim da análise dos fatores determinantes que moldam a configuração da proteção de dados na atualidade.

Em vez de analisar todos os aspectos históricos e jurídicos relacionados à proteção de dados, o enfoque será direcionado para compreender os elementos cruciais que influenciam a forma como os dados são protegidos no contexto contemporâneo. Essa abordagem permitirá uma compreensão mais precisa das questões e desafios atuais associados à privacidade e à segurança dos dados.

Serão explorados os principais aspectos positivos e negativos da legislação vigente, com destaque especial para a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor recentemente.

Além disso, será abordado os principais princípios e diretrizes presentes na LGPD, bem como suas aplicações práticas no contexto brasileiro, tanto na administração pública quanto nas entidades privadas.

Em seguida, uma análise também sobre os órgãos responsáveis pela fiscalização e aplicação da lei, bem como as sanções previstas para o não cumprimento das normas de proteção de dados. A constante evolução do cenário tecnológico requer uma abordagem proativa na adaptação e atualização das políticas de proteção de dados.

Em última análise, a efetiva implementação da LGPD não apenas resguarda a privacidade individual, mas contribui para a construção de um ecossistema digital mais ético e transparente.

Ao aliar a conformidade legal a uma cultura organizacional de respeito à privacidade, as instituições podem não apenas cumprir com suas obrigações legais, mas também se destacar como agentes responsáveis e confiáveis na era da informação.

1.1 A REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL: ELEMENTOS PARA PENSAR NA HISTORICIDADE

O direito à privacidade teve sua origem no século XVIII com as revoluções liberais, capitaneadas pela burguesia ascendente, a qual objetivava um estado minimamente interventor, mas que ao mesmo tempo, alcançasse a segurança jurídica¹. Nesse sentido, “os efeitos da violação da privacidade ganham outras dimensões que acabam por aumentar a necessidade de se criar um fio condutor em torno do qual se possa estruturar essa proteção”².

Adentrando-se as questões atinentes à privacidade, há tempos a mesma possui importância e reconhecimento no cenário internacional, citando-se como exemplo, a Declaração Universal dos Direitos Humanos e o Pacto Internacional sobre Direitos Civis e Políticos³.

¹ DONEDA, Danilo. Privacidade e transparência no acesso à informação pública. *In.*: MEZZARROBA, Orides; GALINDO, Fernando. **Democracia eletrônica**. Zaragoza: Prensas Universitarias de Zaragoza, 2010. p. 179-216.

² NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. **Revista de Informação Legislativa**, Brasília, v. 54, n. 213, p. 13, jan./mar. 2017.

³UNICEF. **Declaração Universal Dos Direitos Humanos**. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 11 out. 2024.

Esses regramentos já dispunham acerca da proteção à honra, à reputação, a vida privada, a inviolabilidade de correspondência, assegurando a legislação internacional à proteção da lei contra intervenções ou atentados nas esferas citadas.

No Brasil, a Constituição da República de 1988 assegura o direito à privacidade, sob o prisma da intimidade e da vida privada, sendo estas prerrogativas fundamentais e invioláveis. O fato é que tanto a expressão “vida privada” quanto o termo “intimidade” pretendem o mesmo objetivo, qual seja: tutelar a pessoa humana de forma mais ampla possível, considerando a complexidade das situações subjetivas existentes⁴.

O art. 5º, inciso X da Constituição Federal foi concebido em um contexto no qual a *internet* e a disseminação de dados ainda não faziam parte da realidade, e, portanto, a troca e aquisição de informações não detinham a mesma relevância que assumem atualmente.

Interpretar o inciso X nos dias de hoje requer uma análise mais aprofundada das novas formas de adquirir informações. O contexto original estabelecido pela Constituição refletia uma noção social muito diferente da sociedade contemporânea, destacando a necessidade de uma interpretação flexível que leve em conta as transformações tecnológicas e sociais que moldam a realidade atual.

Antigamente, a invasão de privacidade muitas vezes ocorria por meio de invasões físicas nas casas das pessoas. Isso poderia incluir arrombamentos, busca e apreensão sem mandado judicial, ou ações intrusivas por parte das autoridades ou de terceiros.

As leis e regulamentos naquela época frequentemente tinham como objetivo proteger as pessoas contra essas invasões físicas de privacidade. O Código Penal⁵ remete até hoje a invasão de privacidade e a violação da correspondência:

Art. 150 do CP - Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências [...].

Art. 151 do CP - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem [...].

⁴ MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil**. Porto Alegre, RS: Editora Fi, 2018.

⁵ BRASIL. **Código Penal. Lei nº 2.848, de 7 de dezembro de 1940**. Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 dez. 2023.

Hoje, com o avanço da tecnologia e a proliferação de dispositivos eletrônicos, a invasão de privacidade assume novas formas. As ameaças à privacidade agora incluem vigilância digital, *hacking*, coleta de dados pessoais não autorizada e espionagem cibernética. Em resposta a essas novas realidades, muitas jurisdições modernizaram seus códigos penais para incluir disposições que abordam essas questões. Exemplo disso a redação dada pela Lei nº 14.155, de 2021 no Código Penal⁶:

Art. 154-A do CP - Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021).

Outro exemplo é a Lei nº 9.296/1996, que foi modificada pela Lei nº 13.964/2019, também conhecida como “Pacote Anticrime”. Essa legislação trata da interceptação telefônica, da gravação ambiental e da escuta ambiental.

Como base do ordenamento jurídico, o art. 1º, inciso III, da Constituição Federal reconhece o princípio da dignidade da pessoa humana, o qual dá sustentáculos à proteção de todos os direitos da personalidade, além de positivizar garantias como: direito à liberdade de expressão, direito à informação, direito a inviolabilidade da vida privada e da intimidade, Habeas Data, a proibição da invasão de domicílio e, por fim, proibição a violação de correspondências.⁷

O *Habeas Data* é oriundo das primeiras demonstrações de mecanismos de proteção de dados no Brasil, e se encontra previsto no art. 5º, inc. LXXII da Constituição Federal. Esse instrumento tem por finalidade garantir acesso a informações relativas à pessoa do impetrante constantes de registros ou de bancos de dados de entidades governamentais ou de caráter público.⁸

⁶ BRASIL. **Código Penal. Lei nº 2.848, de 7 de dezembro de 1940**. Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/lei/del2848compilado.htm. Acesso em: 05.out.2023.

⁷ DONEDA, Danilo. Privacidade e transparência no acesso à informação pública. *In.*: MEZZARROBA, Orides; GALINDO, Fernando. **Democracia eletrônica**. Zaragoza: Prensas Universitarias de Zaragoza, 2010. p. 179-216.

⁸ BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

Esse dispositivo também permite a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. Além disso, frisam Gonçalves e Varella⁹,

[...] há críticas ao habeas data no Brasil pelo fato de: a) seu objeto também poder ser arguido por meio de Mandado de Segurança; b) constar exceção para o fornecimento dos dados quando eles forem de “uso privativo do órgão ou entidade produtora ou depositária das informações” (art. 1º, p. ún)¹⁸⁰; c) os tribunais rejeitarem liminarmente os pedidos impetrados por terceiros por entenderem que se trata de direito personalíssimo¹⁸¹. Diante desses motivos, é nítida a percepção de que houve um esvaziamento do conteúdo desse instituto. E, com isso, ele não conseguiu, de fato, atingir a proteção de dados pessoais.

No contexto atual, enquanto tradicionalmente o debate se centrava na administração pública e no exercício do poder, torna-se evidente que as preocupações evoluíram substancialmente. Embora a administração pública ainda desempenhe um papel crucial, é necessário reconhecer que o verdadeiro cerne da questão está na esfera dos dados.

Os dados pessoais não são mais apenas informações abstratas, mas sim bens fundamentais que sustentam a vida cotidiana, os sistemas sociais, econômicos e a esfera privada dos indivíduos. Além disso, a crescente ameaça de ataques à privacidade dos dados coloca em evidência a necessidade premente de repensar não apenas o escopo da administração pública, mas também como proteger esses ativos vitais para indivíduos e sociedades como um todo.

Em um momento em que a privacidade e a segurança das informações são fundamentais na sociedade digital, é essencial reavaliar e fortalecer o habeas data, aprimorando sua aplicação e garantindo que esse importante instrumento legal possa cumprir seu propósito original de salvaguardar os direitos individuais e a privacidade dos cidadãos.

A adoção de medidas que superem essas lacunas é vital para assegurar uma proteção adequada dos dados pessoais, contribuindo, assim, para uma sociedade mais justa e confiável em relação ao tratamento e uso dessas informações sensíveis.

Em relação a leis infraconstitucionais, o Código de Defesa do Consumidor, Lei nº 8.078/90, foi a primeira normativa a regulamentar relações de consumo. Em seu

⁹ GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Rev. direito GV**, São Paulo, v. 14, n. 2, p. 96, ago. 2018.

artigo 43, estabelece uma série de garantias para o consumidor no que se refere às informações pessoais presentes em bancos de dados e cadastros. O Código Civil de 2002, também possui um capítulo específico sobre direitos da personalidade, salientando que “a vida privada da pessoa é inviolável”.¹⁰

Diante do exposto, é notável que a Carta Magna e as leis infraconstitucionais, como o Código Civil e o Código do Consumidor, foram fundamentais para as primeiras regulamentações a respeito da proteção e privacidade.¹¹

Inexistindo normativa que tratasse especificamente do tema de proteção de dados no Brasil, no ano de 2010, o Ministério da Justiça deu início a um dos maiores debates a respeito da proteção de dados no Brasil, com o intuito de regulamentar a temática.

Paralelamente em 2011, foi sancionada a Lei de Acesso à Informação (LAI) que dispõe sobre os dados de acesso público, e com interesse coletivo, visando promover a transparência e o acesso à informação por parte dos cidadãos.¹²

A LAI foi um marco significativo no Brasil, pois trouxe uma nova perspectiva para a relação entre o Estado e a sociedade, estabelecendo regras claras para a disponibilização de informações governamentais. A partir dessa lei, os órgãos públicos foram obrigados a tornar públicos diversos tipos de dados, documentos e informações, exceto aqueles que são sigilosos por natureza.

Na sequência, houve a propositura do Projeto de Lei nº 2.126, sobre o Marco Civil da *Internet*, que envolveria direitos e deveres dos usuários e provedores. A Lei de nº 12.965/14, que ficou conhecida como o Marco Civil da *Internet*, tem por seu escopo tratar sobre direitos e deveres de usuários perante a *internet*, porém deixou lacunas no que tange a proteção de dados pessoais dos indivíduos, conforme explica Machado¹³,

Discute-se se o Marco Civil da Internet já não teria tratado satisfatoriamente da questão relativa à proteção de dados pessoais. A resposta é negativa, isto

¹⁰ BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.

¹¹ GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Rev. direito GV**, São Paulo, v. 14, n. 2, p. 23, ago. 2018.

¹² BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio.

¹³ MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil**. Porto Alegre, RS: Editora Fi, 2018. p.126.

porque a citada lei tem como objetivo principal o uso da internet, fixando-se direitos e deveres dos usuários, no entanto, na parte que trata de proteção de dados pessoais, o faz de forma bem tímida, até porque não é este o seu foco principal, deixando ainda uma lacuna muito grande [...]

No Brasil, até o ano de 2018 não havia legislação específica sobre a proteção de dados pessoais, somente leis gerais que abordavam o tema sobre alguns aspectos já citados.

Consoante a isso, foi proposto ao Senado Federal o Projeto de Lei nº 330/2013 sobre a proteção, o tratamento e o uso de dados pessoais, sendo aprovado na comissão de ciência e tecnologia do Senado em 2015, resultando na promulgação da Lei de nº 13.709, em 14 de agosto de 2018, após a unificação dos textos da Câmara de Deputados e do Senado.¹⁴

A legislação brasileira foi inspirada na regulamentação europeia, denominada Regulamento Geral de Proteção de Dados, também conhecida como RGPD, em vigor desde maio de 2018.

A legislação Europeia causou um “efeito dominó”, uma vez que passou exigir que os países e empresas que se relacionem comercialmente com a União Europeia, tenham uma legislação de mesmo nível que a RGPD, sob pena de sofrer com barreiras econômicas e dificuldades na realização de negócios.¹⁵

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, estabelece as diretrizes de coleta, armazenamento, compartilhamento e gestão de dados pessoais por empresas e organizações com sede em território nacional, bem como visa dar aos titulares, pessoas naturais, um maior controle sobre seus dados pessoais, proibindo a coleta e compartilhamento dessas informações por empresas ou entes públicos sem o seu consentimento.¹⁶

A proteção de dados inerente aos titulares é uma garantia de direitos fundamentais de liberdade, de intimidade e de privacidade. O ordenamento jurídico a fim de prevenir ataques de dados pessoais rege-se pelos seguintes princípios:

¹⁴ BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709**, de 14 de agosto de 2018.

¹⁵ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018.p.18.

¹⁶ BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709**, de 14 de agosto de 2018.

finalidade; adequação; necessidade; livre acesso; qualidade; transparência; segurança; prevenção; e não discriminação.¹⁷

Os princípios em questão trabalham para prevenir futuros danos em decorrência dos riscos que a realização da coleta de dados compreende, no sentido de evitar os danos possíveis, de preveni-los com o uso da segurança. Esse balizamento principiológico reflete em essência as bases de uma consciência e educação preventivas.¹⁸

Esses princípios trabalham em conjunto para assegurar que a LGPD promova uma cultura de proteção de dados sólida e responsável no Brasil, proporcionando maior segurança e confiança na relação entre titulares e controladores de dados.

No que diz respeito aos dados, a lei define no artigo 5º, inciso I, dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”, e define dados pessoais sensíveis, no inciso II, como o “dado pessoal sobre 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”.¹⁹

Sobre os dados de caráter sensíveis, quando divulgados, possuem potencial para causar discriminações, como revela Machado²⁰

Insta destacar uma categoria específica de dados, chamados sensíveis, que significam determinados tipos de informação, que caso sejam conhecidos ou divulgados, poderiam se prestar a uma potencial utilização discriminatória, como aqueles que dizem respeito a orientações políticas, religiosas, filosóficas, sexuais raciais e outros.

Depreende-se do exposto que dados sensíveis são aqueles que, quando divulgados, podem ser potencialmente lesivos aos aspectos particulares da personalidade do titular desses dados, causando discriminações, perseguições, entre outros.

¹⁷ DONEDA, Danilo. **Privacidade e Proteção de Dados Pessoais**. Brasília, Ministério da Transparência, Fiscalização e Controladoria Geral da União, 2017. p. 39.

¹⁸ MARQUET, Helena Maria; DE GREGORI, Isabel Christine Silva. A EDUCAÇÃO DIGITAL COMO INSTRUMENTO EFICAZ DA PROTEÇÃO DE DADOS PESSOAIS. **Universidade Regional Integrada do Alto Uruguai e das Missões (URI)**, 2021, p. 179.

¹⁹ BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709**, de 14 de agosto de 2018.

²⁰ MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil**. Porto Alegre, RS: Editora Fi, 2018. p. 53.

Nesse cenário, a LGPD objetiva tutelar os dados pessoais, que são aqueles necessários a identificação ou a possibilidade de identificação do titular, conforme o exposto no art. 1º e no inciso I do art. 5º, da LGPD.

A Medida Provisória de nº 869, de 27 de dezembro de 2018, convertida na Lei de nº 13.853, de 8 de julho de 2019, trouxe alterações à Lei Geral de Proteção de Dados e criou a Autoridade Nacional de Proteção de Dados (ANPD). O artigo 5º, XIX da Lei Geral de Proteção de Dados conceitua a ANPD como “órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional”.²¹ O seu intuito é de garantir segurança aos dados pessoais. Lima²² explica que

Atualmente, a ANPD é um órgão da administração pública direta, integrante da Presidência da República, a quem caberá nomear os Diretores e Conselheiros, após aprovação do Senado Federal (§ 1º do art. 55-D da LGPD). A opção brasileira é justamente a correção, ou seja, a ANPD desempenhará suas funções fiscalizadora, reguladora e sancionatórias, sem excluir a possibilidade de os agentes de tratamento de dados pessoais estabelecerem “Boas Práticas” (art. 50 da LGPD).

Assim, com o objetivo de proteger e fiscalizar a segurança dos indivíduos, garantindo a efetividade do sistema “essa entidade deve ter absoluta independência funcional e autonomia financeira para que possa tomar decisões imparciais”.²³ Além disso, o artigo 55-B da LGPD assegura autonomia técnica e decisória à ANPD.

A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel de extrema importância na garantia da proteção de dados em um cenário cada vez mais digitalizado. Ao ser estabelecida como órgão regulador, a ANPD tem o objetivo de supervisionar e orientar a aplicação da Lei Geral de Proteção de Dados (LGPD) no Brasil, bem como promover a conscientização sobre a importância da privacidade e segurança das informações pessoais.

Embora as punições por violações de dados sejam essenciais para desencorajar práticas inadequadas, a mera aplicação de penalidades não será suficiente para assegurar a conformidade generalizada.

²¹ BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018.

²² LIMA, Cintia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. p. 377.

²³ LIMA, Cintia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. p. 378.

A ANPD deve atuar também na capacitação de empresas e indivíduos, fornecendo diretrizes claras, auxiliando na implementação de medidas preventivas e educando sobre as boas práticas de tratamento de dados. Dessa forma, ao combinar a fiscalização rigorosa com a conscientização e o apoio na adequação às normas, a ANPD poderá efetivamente promover uma cultura de proteção de dados sólida e responsável em todo o país.

A Lei Geral de Proteção de Dados Pessoais é um novo marco legal brasileiro, com grande impacto tanto nas instituições privadas quanto nas públicas, uma vez que trata da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva tratamento de informação classificada como dado pessoal, em qualquer meio, por pessoas naturais ou jurídicas.²⁴

Assim sendo, a partir 18 de setembro de 2020, data de início de vigência da LGPD, as entidades da administração pública e instituições privadas estão tendo que se adaptar a novas normativas, de modo a cumprir as exigências impostas pela LGPD e preservar as informações fornecidas pelos usuários, conforme se verá a seguir.

1.2 ANÁLISE DA PROTEÇÃO DE DADOS: DIFERENÇAS NA ADMINISTRAÇÃO PÚBLICA E NAS INSTITUIÇÕES PRIVADAS

A proteção de dados tornou-se uma questão crucial tanto na Administração Pública quanto nas instituições privadas.

Com o avanço da tecnologia e a crescente coleta, processamento e compartilhamento de informações pessoais, surge a necessidade de avaliar como essas entidades lidam com a segurança e privacidade dos dados que lhes são confiados.

Tanto o setor público quanto o privado têm o dever de proteger os direitos individuais e garantir a conformidade com a legislação vigente, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Os princípios da Lei Geral de Proteção de Dados citados no tópico anterior estão intrinsecamente interligados na aplicação da lei, tanto para a Administração Pública quanto para as entidades particulares. Esses princípios formam a base

²⁴ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. p. 15.

fundamental para o tratamento ético, seguro e responsável dos dados pessoais em ambos os setores, assegurando a privacidade e a proteção dos direitos individuais.

O principal desafio na era da sociedade em rede está relacionado com a privacidade e a falta de gestão de dados pessoais. Principalmente no atual contexto contemporâneo em que os dados são transferidos de maneira instantânea, impossibilitando que o cidadão, titular de seus dados, tenha controle de todas as informações que lhe diz respeito, até mesmo as informações mais pessoais e íntimas.

Na Administração Pública, a proteção de dados envolve a segurança e a privacidade das informações coletadas dos cidadãos, empresas e outras entidades. Os governos geralmente lidam com uma ampla gama de informações, incluindo dados de identificação pessoal, registros médicos, informações fiscais e até mesmo dados biométricos. Garantir a confidencialidade, integridade e disponibilidade desses dados é garantir a confiança e a transparência nas operações governamentais.

O Guia de Boas Práticas da Lei Geral de Proteção de Dados foi criado em março de 2020 pelo Comitê Central de Governança de Dados com a finalidade de instruir os órgãos públicos acerca da respectiva lei.

O guia dispõe que a Administração Pública só poderá realizar o tratamento de dados no setor público se houver relação com “a execução de políticas públicas, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador”.²⁵ Ainda, esclarece sobre as medidas de políticas públicas

No caso do setor público, a finalidade relaciona-se com a execução de políticas públicas, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador. E, mesmo sendo eventualmente dispensado o consentimento do titular para o tratamento dos dados pelo poder público, nas hipóteses legalmente definidas, tal dispensa não exime a administração pública de atender às demais obrigações da LGPD, em especial aos princípios gerais e à garantia dos direitos dos titulares.²⁶

As políticas públicas desempenham um papel fundamental na proteção de dados na administração pública, indo além das meras normativas legais. Além de cumprir as obrigações legais, essas políticas proporcionam uma abordagem proativa,

²⁵ BRASIL. Serviço Federal de Processamento de Dados. **Guia de Boas Práticas da Lei Geral de Proteção de Dados**. Brasília, DF, 2020. p. 8.

²⁶ BRASIL. Serviço Federal de Processamento de Dados. **Guia de Boas Práticas da Lei Geral de Proteção de Dados**. Brasília, DF, 2020. p. 8.

adaptável e eficiente para enfrentar os desafios contínuos relacionados à proteção de dados.

Ao promover a conscientização entre os funcionários públicos e incentivar a cultura de segurança, essas políticas reforçam a importância de tratar os dados com responsabilidade e transparência, fortalecendo a legitimidade do governo e a parceria com a sociedade.

A administração pública no Brasil é responsável por uma grande quantidade de informações sensíveis e pessoais de cidadãos, tornando a proteção de dados uma questão crítica. Nos últimos anos, houve várias violações de proteção de dados que chamaram a atenção para a necessidade de melhorar a segurança e a privacidade das informações do governo.

Em novembro de 2020, o Ministério da Saúde do Brasil enfrentou um sério incidente de violação de dados quando informações pessoais de pacientes com COVID-19, incluindo nomes, números de CPF e endereços, foram indevidamente expostas online. Isso levantou preocupações sobre a segurança dos dados de saúde e a capacidade do governo de proteger informações confidenciais.

Diante dos incidentes de vazamentos de dados, o Conselho Nacional de Saúde (CNS), por meio de nota pública, pediu esclarecimentos ao Ministério da Saúde, de maneira urgente, “sobre os reais acontecimentos que motivaram a inegável falha de procedimentos de segurança de dados e informações em saúde da população brasileira”. A resposta ao CNS foi feita por meio de órgãos de controle interno.²⁷

A divulgação inadequada ou o vazamento de dados sensíveis de saúde podem comprometer a dignidade, a intimidade e até mesmo a segurança das pessoas. Por isso a necessidade de medidas de segurança de dados em sistemas de saúde, a fim de proteger a privacidade e a confidencialidade das informações dos cidadãos.

O Superior Tribunal de Justiça (STJ) em 2020 também sofreu um ataque cibernético que resultou no vazamento de informações confidenciais de processos judiciais. Este incidente demonstrou a vulnerabilidade dos órgãos governamentais à ação de cibercriminosos.

Os dados da entidade foram criptografados, bloqueando o acesso a eles, comportamento típico de ransomwares, software malicioso (vírus) que “sequestra” os dados e costuma pedir pagamento para que sejam liberados.

²⁷ LEMES, Delwin. Lei Geral de Proteção De Dados Pessoais (LGPD): O setor público e vazamentos de dados pessoais. **Revista eixo**, v. 12, n. 2, p. 115, 2023.

O STJ comunicou que os sistemas de backup do órgão foram preservados e, em ação conjunta da Secretaria de Tecnologia da Informação e Comunicação (STI), do Comando de Defesa Cibernética do Exército brasileiro, da Polícia Federal, do SERPRO, bem como diversos servidores do quadro permanente do STJ, empresas privadas e fabricantes de tecnologia, trabalharam para reverter os dados, reverter os dados. Assim, no dia 18 de novembro, os sistemas de informática da Corte foram plenamente restabelecidos.²⁸

A soma dos esforços de diversos órgãos públicos e privados permitiu que os dados fossem recuperados e os sistemas de informática restabelecidos. Nas instituições privadas o tema é de extrema importância também.

À medida que as organizações acumulam e utilizam cada vez mais informações pessoais de clientes, funcionários e parceiros de negócios, a necessidade de garantir a segurança e a privacidade desses dados se tornou uma prioridade.

Um dos princípios da proteção de dados é a minimização de dados, que implica coletar apenas as informações necessárias para a finalidade específica para a qual foram obtidas. Além disso, as instituições privadas são responsáveis por implementar medidas robustas de segurança de dados para proteger as informações contra acesso não autorizado, vazamentos ou violações de segurança.

No cenário global, o incidente de violação de dados da Cambridge Analytica em 2018 é um exemplo marcante. A empresa, com sede no Reino Unido, coletou indevidamente informações pessoais de milhões de usuários do Facebook sem seu consentimento.

Esse episódio lançou luz sobre as práticas duvidosas de coleta de dados por parte de empresas de análise de dados e levantou questões sobre a privacidade e a ética no mundo digital.

Um dos maiores exemplos dos possíveis ensinamentos que o escândalo da CA nos apresenta é que infelizmente se está fadado a apenas um único e fatídico episódio de (i) usurpação de dados pessoais, (ii) de coleta de informações em grande quantidade e de forma continuada e (iii) que podem tecer toda uma narrativa comportamental de quem é cada indivíduo. Mesmo que essas narrativas sejam verossímeis, indivíduos serão sempre mais do que apenas métricas; conjuntos de indicadores transformados em estatística e logo permitindo que algumas conclusões sejam inferidas.²⁹

²⁸ LEMES, Delwin. Lei Geral de Proteção De Dados Pessoais (LGPD): O setor público e vazamentos de dados pessoais. **Revista eixo**, v. 12, n. 2, p. 114, 2023.

²⁹ DE OLIVEIRA FORNASIER, Mateus; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, v. 29, n. 53, p. 189, 2020.

Os indivíduos são muito mais do que meras métricas e conjuntos de indicadores. Eles são seres cujas experiências, valores, motivações e, acima de tudo, vidas não podem ser totalmente capturados por números.

As empresas detêm um grande poder econômico quando se trata de dados, e isso pode afetar a proteção de dados de várias maneiras. Empresas que coletam grandes volumes de dados muitas vezes têm recursos para investir em segurança cibernética e conformidade regulatória.

No entanto, também podem estar inclinadas a priorizar o lucro sobre a privacidade dos indivíduos, o que pode levar a práticas questionáveis de coleta e uso de dados.

A magnitude da violação de dados da Cambridge Analytica teve implicações significativas nas eleições presidenciais de Donald Trump, particularmente em relação à disseminação de fake news.

A partir das informações obtidas pela Cambridge Analytica, a empresa criou perfis altamente segmentados de eleitores, permitindo que campanhas políticas direcionassem mensagens específicas para públicos selecionados.

Basta recordar que, antes de Donald Trump contratar a CA, a empresa prestava consultoria nos EUA para Ted Cruz, seu adversário dentro do Partido Republicano. A operação continuada de Fake News, somada à práticas de microtargetting e coleta de dados via data mining & scraping, demonstrou a terrível essência do setor privado em querer minerar e gerar lucro de processos democráticos. Dito isso, é necessário perceber que seria temerário afirmar que todos os problemas relacionados com as práticas da CA foram-se quando a empresa faliu. Hoje existem novas empresas, como a Data Propria, que operam de maneira similar para não dizer de forma mais sofisticada que antes.³⁰

A Cambridge Analytica conseguiu coletar informações pessoais e privadas de milhões de cidadãos através das redes sociais, trocando esses dados pela influência na eleição de candidatos que mais investiram financeiramente na empresa. Além disso, suas práticas incluíram a disseminação de fake news, que desempenharam um papel significativo na manipulação da percepção pública e na polarização política durante esses processos eleitorais.³¹

³⁰ DE OLIVEIRA FORNASIER, Mateus; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, v. 29, n. 53, p. 193, 2020.

³¹ DE OLIVEIRA FORNASIER, Mateus; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, v. 29, n. 53, p. 193, 2020.

O Congresso dos Estados Unidos convocou Mark Zuckerberg, CEO do Facebook, para prestar depoimento sobre o incidente, resultando em debates sobre a regulamentação de gigantes da tecnologia e suas práticas de privacidade. Além disso, autoridades de proteção de dados em vários países, incluindo o Reino Unido e a União Europeia, investigaram a Cambridge Analytica e suas operações.

Essa violação também desencadeou uma mudança significativa na maneira como as redes sociais e as empresas de tecnologia abordam a privacidade e a segurança dos dados. O Facebook implementou alterações em suas políticas de privacidade e restringiu o acesso de aplicativos a dados de usuários, em um esforço para reconquistar a confiança do público.

“Apesar deste apresentar de forma ampla e genérica a forma como os dados são captados e quais as suas finalidades, tal conduta não é suficiente para garantir aos usuários o livre acesso aos seus dados pessoais”.³² A segurança dos dados não é apenas uma questão técnica; ela também envolve a conscientização e a responsabilidade das partes envolvidas.

Considerando o déficit de informação, a situação de muitos brasileiros com pouca familiaridade com o uso de tecnologias e até mesmo a baixa instrução, por um lado, e a exclusão digital ainda reinante entre as classes mais pobres, por outro, essa informação pode não estar chegando de maneira adequada ou não ser corretamente compreendida pelo titular dos dados pessoais.

O capítulo IV da LGPD, especialmente nos artigos 26 e 27, trata do compartilhamento de dados pelo Poder Público, inclusive a transferência de dados para entidades privadas. A Lei de nº 13.853 de 2019 incluiu o inciso IV ao artigo 26, § 1.º da LGPD, possibilitando a transferência de dados da administração pública a entidades privadas quando a transferência for respaldada em contratos, convênios ou instrumentos congêneres, mesmo sem o consentimento do titular (art. 27, III).

Portanto, é crucial que as organizações treinem seus funcionários para compreenderem as implicações das leis de proteção de dados e adotem melhores práticas para garantir a conformidade.

³² SANTOS, Dhiulia de Oliveira. A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018). Trabalho de Conclusão de Curso (Graduação em Direito). Centro Universitário de Brasília, Brasília, 2019. p. 20. Disponível em: < <https://repositorio.uniceub.br/jspui/handle/prefix/13802> > Acesso em: 04 out 2023.

A partir do exposto e dos incidentes mencionados, não se pretendeu esgotar os acontecimentos relacionados aos vazamentos de dados, mas sim descrevê-los no contexto da discussão.

Dessa forma, a implementação de políticas públicas sólidas e abrangentes na proteção de dados é essencial para uma administração pública moderna e instituições privadas, capaz de se adaptar às rápidas mudanças tecnológicas e às crescentes expectativas de privacidade dos cidadãos. “É importante ter em mente que não basta ter a lei de proteção de dados pessoais, é preciso educar, capacitar”.³³

É necessário estabelecer protocolos claros de resposta a incidentes de segurança, que incluam planos de ação específicos para lidar com possíveis vazamentos ou violações de dados, minimizando os danos e garantindo a confiança dos cidadãos e clientes.

³³ PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018. p. 23.

2 A RELAÇÃO ENTRE DIMENSÕES DE PODER E A PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados entra no meio de uma tensão: quando "dados" são parte crucial do que é o novo capital. Não podendo falar em proteção de dados apenas como fator gerador de indenização ou como se o problema fosse apenas a troca, venda e distribuição de dados, mas de algoritmização dá vida, em si.

A ascensão das tecnologias de informação e comunicação (TICs) marcou o início de uma revolução que transcendeu fronteiras geográficas e setores econômicos. As TICs possibilitaram a criação, coleta e análise massiva de dados, redefinindo o poder em várias esferas. A digitalização e a conectividade mundial permitiram que entidades governamentais e corporações exercessem influência em escalas sem precedentes.

O poder se expande, têm a capacidade de moldar políticas e práticas relacionadas à coleta, uso e compartilhamento de informações pessoais. A análise crítica dessa dinâmica é essencial para compreender como as dimensões de poder afetam a privacidade, a segurança e a equidade na era digital.

O foco do capítulo é abordar essas interações sociais e interpessoais que vão além de um poder ideal, que muitas vezes é codificado em leis e regulamentos, e exercido por agentes do Estado. Embora o poder estatal seja um componente essencial da estrutura de poder de uma sociedade, ele não é a única fonte de influência e autoridade.

Analisar a interconexão entre o colonialismo de dados, big data e a cooperação dos indivíduos, pois, muitas questões sociais, políticas e econômicas são moldadas por relações de poder que não são exclusivamente governamentais.

Discutir de como os chamados *hackerspaces* podem ser valiosos locais de discussão e ação em relação a marcos regulatórios, como a LGPD. Eles podem fornecer conhecimento técnico, desenvolver soluções práticas e educar a comunidade sobre questões de privacidade e proteção de dados, desempenhando um papel significativo na conformidade regulatória e na promoção de práticas éticas no tratamento de informações pessoais.

Diante de todo esse cenário, mostra-se fundamental a análise crítica relacionando o contexto da *internet* com o direito à privacidade e a proteção de dados pessoais. Principalmente sobre as perspectivas do novo marco regulatório decorrente

da aprovação da Lei Geral de Proteção de Dados Pessoais, que aprofunda a normatização acerca do tratamento de dados pessoais.

2.1 A EVOLUÇÃO DOS PODERES NA ERA DA TECNOLOGIA

O desenvolvimento humano pressupõe a gestão da informação e a facilidade de sua transferência e armazenamento. No final do século XX, e no início do atual século XXI, a sociedade globalizada está passando por uma revolução informacional decorrente das novas Tecnologias da Informação e Comunicação – TIC, formando a chamada sociedade em rede.

A sociedade informacional é uma sociedade em rede, que constituiu uma nova morfologia social, possibilitando por meio dessa organização, a primazia econômica, política, social e cultural.³⁴

Fala-se em poder, e é inerente o pensamento de que este está ligado ao poder ideal advindo de leis e do poder estatal. No entanto, não se pode iniciar um capítulo sem antes adentrar no mérito do que realmente é poder.

O conceito de poder³⁵ transcende as simples noções de autoridade governamental. Ele pode se manifestar de diversas formas, tanto de maneira formal, como nas estruturas legais e institucionais, quanto de maneira informal, em interações sociais e relações interpessoais.

A ideia de poder vem muito além da vinculação ao Estado, pode ser considerado um símbolo que representa as relações humanas. “O poder não é, ele atua, faz parte da prática humana, está inserido nas relações e se articula como um modo de ser da ação”.³⁶

O simbolismo que envolve essa dimensão humana é a chave para entender que o poder não é estático, mas fluido e sujeito a constante transformação. Esse simbolismo reflete a complexidade do poder, que pode se manifestar de maneiras diversas e até contraditórias ao longo do tempo e em contextos variados.

³⁴ CASTELLS, Manuel. Fim de milênio: a era da informação: economia, sociedade e cultura.

Trad. Klauss Brandini Gerhardt e Roneide Venancio Majer. v. 3. São Paulo: Paz e Terra, 1999. p. 46.

³⁵ RUIZ, Castor M. M. Bartolomé. 2004. Os labirintos do poder: o poder do simbólico e os modos de subjetivação. Porto Alegre, Escritos Editora, 281, p. 11.

³⁶ RUIZ, Castor M. M. Bartolomé. 2004. **Os labirintos do poder**: o poder do simbólico e os modos de subjetivação. Porto Alegre, Escritos Editora, 281, p. 11.

O poder criador desdobra-se de modo singular em modos diferentes de ser e de agir assim como em relações e práticas sempre diversas, conferindo à prática humana a potencialidade de instituir formas de poder dominador, mas também é esse mesmo poder criador que outorga à prática a possibilidade de criar formas de poder emancipador. Estamos falando do mesmo poder, do simbolismo que conota uma dimensão humana sempre criativa e, portanto, indefinível.³⁷

A afirmação de que o poder criador se manifesta de maneira singular em diferentes modos de ser e de agir, bem como em diversas relações e práticas, aponta para a complexidade do poder na experiência humana. Essa capacidade de moldar o poder é o que confere à prática humana a potencialidade de instituir formas de poder dominador, mas também de criar formas de poder emancipador.

A concepção de que o poder não está inerentemente vinculado ao Estado, mas sim às condições sociais, desafia a visão tradicional do monopólio estatal sobre o poder. “A razão é que o aparelho de Estado é um Instrumento específico de um sistema de poderes que não se encontra unicamente nele localizado, mas o ultrapassa e complementa”.³⁸

O aparelho de Estado, composto por seus órgãos executivos, legislativos e judiciários, é um dos pilares do poder, mas está longe de ser o único. Ele opera em coordenação e muitas vezes em colaboração com outros atores, como organizações não governamentais, empresas, mídia e indivíduos. Isso ocorre porque o exercício do poder e a tomada de decisões não estão confinados apenas ao governo central, mas são distribuídos de maneira mais ampla, incorporando diversos interesses e influências que permeiam a sociedade.

“A ideia básica de Foucault é de mostrar que as relações de poder não se passam fundamentalmente nem a nível do direito nem da violência: nem são basicamente contratuais nem unicamente repressivas”.³⁹

O poder é influenciado por diversos fatores, com destaque para o capitalismo. O capital não se limita apenas ao dinheiro, como apontou Michel Foucault, mas envolve uma complexa dinâmica de estratégias, muitas vezes operando de forma implícita e sem um estrategista.

³⁷ RUIZ, Castor M. M. Bartolomé. 2004. **Os labirintos do poder: o poder do simbólico e os modos de subjetivação**. Porto Alegre, Escritos Editora, 281, p. 11.

³⁸ FOUCAULT, Michel. Soberania e Disciplina. In: *Microfísica do Poder*. Rio de Janeiro: Graal, 1979, p. XIII.

³⁹ FOUCAULT, Michel. Soberania e Disciplina. In: *Microfísica do Poder*. Rio de Janeiro: Graal, 1979, p. XV.

Além disso, a ideia de Foucault sobre a estratégia sem estrategista ressalta que o poder muitas vezes opera de forma sutil e invisível, moldando as interações sociais e a política, mesmo na ausência de atores claramente identificáveis como detentores do poder.

Como já exposto, o conceito de poder vai além da mera coerção legal e estatal. Ele está ligado ao saber e ao conhecimento. A máxima “conhecimento é poder” não é meramente retórico, mas sim um alicerce na interação entre poder e tecnologia. O conhecimento não é apenas uma moeda de troca intelectual, é também a matéria-prima que alimenta a infraestrutura de uma sociedade.

O acesso ao poder transcendente é restrito àqueles que têm um conhecimento e um contato especiais com as verdades nele reservadas e que são inacessíveis à imensa gama de indivíduos. Esse poder os dota, de modo legítimo, de autoridade representativa das idéias verdadeiras que transcendem as contingências do mundo. A transcendência como significação simbólica não foi desconstituída pelo processo racionalista da modernidade, já que a própria racionalidade funciona como um simbolismo transcendente.⁴⁰

Uma ideia central a ser considerada é que é muito mais fácil exercer controle sobre alguém que não tem consciência de que está sendo controlado. Isso se deve, em grande parte, à falsa ilusão de liberdade que pode ser instilada nas pessoas, levando-as a agir de acordo com sua própria iniciativa, mesmo quando, na realidade, estão sendo manipuladas.

A expansão do capitalismo gera um controle que envolve a cooperação do indivíduo, criando uma ilusória sensação de autonomia.

O foco desta tecnologia de poder dirige-se para a condução da subjetividade dos indivíduos. Não busca a submissão forçada de sua vontade, mas requer sua colaboração ativa; para tanto, o impacto de sua eficiência reside na capacidade de estimular as motivações individuais para aderir às verdades estabelecidas como se fossem o principal ou o único modo de desenvolvimento pessoal. Seu poder manifesta-se como capacidade de induzir e produzir os modos da subjetividade.⁴¹

⁴⁰ BRAGATO, Fernanda Frizzo. Resenha. **Os labirintos do poder**: o poder do simbólico e os modos de subjetivação, de Castor M. M. Bartolomé Ruiz. p. 253.

⁴¹ RUIZ, Castor M. M. Bartolomé. 2004. **Os labirintos do poder**: o poder do simbólico e os modos de subjetivação. Porto Alegre: Escritos Editora, 281, p. 25.

Sob o capitalismo, os indivíduos podem acreditar que estão fazendo escolhas livres, mas essas escolhas são frequentemente moldadas e limitadas pelas estruturas econômicas e sociais do sistema.

O chamado colonialismo de dados ou digital é uma extensão do capitalismo que penetra de forma econômica, social e cultural na sociedade. “O colonialismo digital não é mera metáfora ou discurso de poder, mas um dos traços objetivos do atual estágio de desenvolvimento do modo de produção capitalista”.⁴²

O sistema jurídico enfrenta um desafio na regulamentação, enquanto as garantias fundamentais são frequentemente percebidas como barreiras. O direito não representa o auge da estrutura, revelando sua fragilidade diante da era do capitalismo de vigilância.

Os poderes estão interligados à era tecnológica, o regime disciplinar, por exemplo, é uma forma de capitalismo industrial. Han⁴³ conceitua a máquina disciplinar do poder de fenômeno de produção, que não porta dados e informações, mas que possui energia.

Esse fenômeno explica-se pelo fato que “no regime disciplinar, os seres humanos são adestrados em um animal do trabalho”.⁴⁴ O autor considera que a vigilância no regime da informação ocorre através de dados e que no regime biopolítico acontece por meio dos corpos em um maquinário de produção e vigilância que se potencializa no poder disciplinar.

O regime da informação, porém, cujo surgimento Foucault evidentemente não percebeu, não segue uma biopolítica. Seu interesse não está no corpo. Apodera-se da psique pela psicopolítica. O corpo é, hoje, em primeira linha um objeto da estética e do fitness. Ele está, ao menos no capitalismo ocidental da informação, em sua maior parte livre do poder disciplinar que o adentra em máquina do trabalho.⁴⁵

Não são os meios de produção que são determinantes para o ganho de poder “mas o acesso a dados utilizados para vigilância, controle e prognóstico de

⁴² FAUSTINO, Deivison; LIPPOLD, Walter. Colonialismo digital: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023.

⁴³ HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022. p. 8.

⁴⁴ HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022. p. 8.

⁴⁵ HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022. p. 9.

comportamento psicopolíticos”.⁴⁶

O capitalismo contemporâneo é marcado por uma economia globalizada, avanços tecnológicos, e uma ênfase no consumo. Críticos do capitalismo frequentemente apontam para desigualdades socioeconômicas, exploração de recursos naturais e preocupações ambientais como questões problemáticas associadas a esse sistema.

O regime de informação está atrelado ao capitalismo da informação “que se desenvolve em capitalismo da vigilância e que degrada os seres humanos em gado, em animais de consumo e dados”.⁴⁷

Atualmente o poder se passa por “liberdade”, deixando cada vez mais os indivíduos dependentes na era digital. Não trabalhando apenas com punições e proibições, mas gerando satisfação, desejos e preferências⁴⁸. Isso quer dizer que “sujeitos com direitos são obrigados a ser livres, isto é, fazer opções dentro de um estado limitado onde o bem estar é reduzido ou modificado a cada viravolta do mercado ou de arranjos semelhantes a mercado”.⁴⁹

A década de 1970 foi a responsável pelo crescimento lucrativo do mercado e gerou efeitos principalmente para as tecnologias da informação e da comunicação.

De acordo com Oro Boff, Fortes e Freitas⁵⁰ a preocupação com o tratamento de dados pessoais como desdobramento da privacidade é um efeito colateral do fenômeno informacionalização da sociedade, iniciada na década de 1970, sendo que seus reflexos impactam diretamente na atividade econômico-empresarial como na atuação do próprio Estado, que, além de criar e consumir informação, controla o fluxo de informações.

Conforme Faustino e Lippold⁵¹, as novas tecnologias de comunicação, que ganharam destaque a partir da década de 1970, desempenharam um papel fundamental na reestruturação produtiva global. Essas inovações revolucionaram a

⁴⁶ HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022. p. 8.

⁴⁷ HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Vozes, 2022. p. 8.

⁴⁸ HAN, Byung-Chul. **O que é poder?**. Tradução Lucas Machado. Petrópolis: Vozes, 2018. p. 26.

⁴⁹ PETERS, Michael. **Financeirização, o ácido que corrói a democracia**. IHU On- Line, v. 472, n. 15, p. 28, set. 2015.

⁵⁰ BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018. p. 13.

⁵¹ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023.

maneira como empresas operam, interagem e competem. Uma das mudanças mais marcantes foi a intensificação da disputa pelo controle e pelo fluxo de informações

As novas tecnologias de comunicação ocuparam papel fundamental na reestruturação produtiva que emergiu a partir da década de 1970. Com elas, a disputa pelo controle e pelo fluxo de informações adquiriram patamares jamais vistos, viabilizando, de um lado, a aceleração dos tempos de produção de mercadorias e a circulação de capitais e, do outro lado, a intensificação da maximização dos lucros ao possibilitar a usurpação e análise de grande quantidade de dados privados e coletivos de comportamento.⁵²

Com a disseminação da *internet*, dos computadores pessoais, dos smartphones e das redes de comunicação digital, as organizações se viram em uma corrida para adquirir, processar e utilizar dados. Essa busca pelo acesso a informações tornou-se um fator determinante na competitividade empresarial. A disponibilidade de dados em tempo real possibilitou uma aceleração notável nos tempos de produção de mercadorias e na circulação de capitais.

Lévy⁵³ sugere que o virtual tem o potencial de ampliar ou potencializar o poder. Ele observa que as tecnologias da informação e a cibercultura permitem a disseminação rápida de informações e a conectividade global, o que pode ser usado tanto para fins positivos quanto negativos.

O poder pode se manifestar no controle e na manipulação dessas redes virtuais. Por outro lado, Lévy também argumenta que o virtual pode descentralizar o poder. Ele vê a *internet* e as redes digitais como meios pelos quais as pessoas comuns podem participar ativamente na criação e distribuição de informações, possibilitando formas alternativas de poder e resistência.

A disseminação de desinformação e a manipulação algorítmica são exemplos de ferramentas que podem promover a conformidade, mesmo entre aqueles que possuem um alto índice de formação e informação. Esses meios virtuais, paradoxalmente, têm o potencial tanto de ampliar o acesso ao conhecimento quanto de serem veículos eficazes para a disseminação de narrativas dominantes.

Numa dita sociedade do conhecimento e do saber, com um alto índice de formação e informação dos indivíduos, como é possível a aceitação generalizada dessas novas formas de dominação? Como se produz e consolida a sujeição das pessoas e dos grupos sociais às novas formas de

⁵² FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023.

⁵³ LÉVY, Pierre. **O que é o virtual?**. Editora 34, 2011.

poder? Quais são os mecanismos que viabilizam a conjugação atual de elementos tão contraditórios como a expansão globalizada de formas de dominação, sua aceitação social, inclusive por parte dos dominados, e, por sua vez, o aumento do conhecimento, da informação e da subjetividade - entendida como consciência da própria individualidade?⁵⁴

A subjetividade, entendida como a consciência da própria individualidade, pode manifestar-se de várias maneiras nos meios virtuais, desde a construção de identidades digitais até a participação em movimentos de resistência.

O poder transcende as esferas de estado à soberania e permeia todos os aspectos da sociedade. O poder é uma força onipresente que tece sua influência através de todos os aspectos da vida cotidiana, moldando dinâmicas sociais, econômicas e culturais.

As sociedades pós-industriais que se autolegitimam como amplamente democráticas consolidam-se com o mínimo de força e o máximo de persuasão. Contraditoriamente, constata-se que esse modelo pós-industrial criou novas formas sutis de maior controle e de sujeição mais eficiente das pessoas. Ele massificou as identidades, padronizou comportamentos, mercantilizou a vida, disseminou novas formas de pobreza, globalizou os tipos de dominação, expandiu os modos de exclusão e universalizou os mecanismos de exploração econômica aperfeiçoando a concentração de riqueza em minorias privilegiadas.⁵⁵

À medida que a sociedade avança no século XXI, pode-se observar que o poder, em sua essência, não sofreu grandes transformações. No entanto, sua expressão e manifestação na sociedade evoluíram consideravelmente. Essas mudanças podem ser comparadas às “novas roupagens” que o poder adotou.

As diferentes dimensões em que o poder se manifesta, desde as instituições políticas tradicionais até os novos atores emergentes revela uma paisagem complexa e dinâmica que caracteriza o século XXI.

2.2 DIMENSÕES DE PODER E SUA INFLUÊNCIA NA GOVERNANÇA DE DADOS: UMA ANÁLISE CRÍTICA

O poder estatal é destinado aos indivíduos, que têm seus direitos garantidos na CF. O poder abordado no capítulo anterior age diretamente sobre o indivíduo,

⁵⁴ RUIZ, Castor M. M. Bartolomé. **Os labirintos do poder**: O poder (do) simbólico e os modos de subjetivação. Porto Alegre: Ed. Escritos, 2004. p. 42.

⁵⁵ RUIZ, Castor M. M. Bartolomé. **Os labirintos do poder**: O poder (do) simbólico e os modos de subjetivação. Porto Alegre: Ed. Escritos, 2004. p. 51.

conhecendo as preferências de cada pessoa. Ele se relaciona não de maneira ideal, buscando moldar a subjetividade de qualquer indivíduo.

O desafio de proteger a autonomia individual exige não apenas o sistema legal, mas também a cultura, a ética e a consciência coletiva da sociedade.

Conforme destacado no subcapítulo 2.1, o colonialismo digital envolve questões relacionadas à privacidade, direitos individuais, regulação e ética, à medida que os dados se tornam um recurso valioso e estratégico na sociedade digital contemporânea. Essa prática é frequentemente vista como uma extensão do capitalismo:

O grande problema do colonialismo de dados, no entanto, não é a informações com serção voluntária de informações em um aplicativo, e sim o fato de que de são programados algoritmicamente para coletar e cruzar ou sem o consentimento do usuário, a fim de mapear padrões e perfis de comportamento e, em seguida, vendê-los a quem possa pagar ou utilizar essas informações para induzir determinadas práticas de consumo - determinado comportamento político.⁵⁶

A falta de consentimento e a comercialização das informações pessoais suscitam preocupações éticas e de privacidade, enquanto a possibilidade de influência no comportamento político levanta questões mais amplas sobre a integridade da democracia e a liberdade individual.

Estamos diante de um verdadeiro saque milionário de informações transformadas em ativos económicos, perpetrado por corporações imperialistas que extraem, armazenam e processam dados, expertise e padrões sociais, quantificando parte fundamental de nossa vida para melhor mercantilizá-la.⁵⁷

Essa caracterização do colonialismo digital “não deixa de ser atravessada pelas antigas cisões de raça, classe e gênero que marcaram o desenvolvimento do capitalismo”.⁵⁸ O capitalismo também é conhecido por criar desigualdades econômicas significativas, com a concentração de riqueza nas mãos de poucos.

⁵⁶ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023. p. 124.

⁵⁷ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023. p. 78.

⁵⁸ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023. p. 65.

No contexto do colonialismo digital, isso se reflete na capacidade de grandes empresas e corporações dominarem a coleta e o uso de dados, muitas vezes em detrimento dos direitos e interesses de classes menos privilegiadas.

Neste momento em que as distâncias e os tempos parecem distorcidos pela aceleração da velocidade de rotação do capital, o racismo e a xenofobia se tornam mais importantes do que jamais foram, atuando como critério biopolítico de diferenciação entre quem é e quem não é cidadão, quem é quem não é nacional, quem está dentro e quem está fora da ética, da política e da estética, quem é humano e quem é matável, mas também quem tem acesso e, sobretudo, controle dos novos meios (informacionais) de validação da própria existência e quem não tem.⁵⁹

A relação entre a forma subjetiva e a biopolítica ilustra como o controle sobre as preferências das pessoas muitas vezes transcende a estrutura de poder e de direito, tornando-se uma ferramenta de governança de dimensões consideravelmente maiores.

A biopolítica como tecnologia de poder é um conceito desenvolvido por Michel Foucault que se refere à maneira como o poder é exercido sobre a vida e a população em uma sociedade. A biopolítica difere das formas tradicionais de poder, como a soberania, que se concentrava no controle do soberano.

Em vez disso, a biopolítica se concentra na regulamentação e gestão da vida da população como um todo. O sujeito biopolítico é propriamente um sujeito coletivo, a população. “A população, por sua vez, é composta de singularidades que compõem um todo coeso, mas apenas na medida em que se representam como parte desse todo”.⁶⁰

A biopolítica em substituição ao poder soberano envolve paradigma de governança diferente, baseado em um regime de cooperação entre os indivíduos. De acordo com Antonio Negri⁶¹, a única forma de democracia já experimentada é a democracia corporativa. Uma democracia genuína seria aquela em que todos colaboram e produzem em conjunto.

⁵⁹ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023. p. 66.

⁶⁰ NETO, Leon Farhi. Biopolítica como tecnologia de poder. **INTERthesis: Revista Internacional Interdisciplinar**, v. 5, n. 1, 2008, p. 62-63.

⁶¹ NEGRI, Antonio. **Kairós, Alma Venus, Multitudo**: nove lições ensinadas a mim mesmo. Tradução: Orlando dos Reis e Marcello Lino Rio de Janeiro: DP&A, 2003. p. 175.

Atualmente, as pessoas estão contribuindo para o sistema e para a economia, mas não para si mesmas. Não estão cooperando para um benefício coletivo; em vez disso, estão disponibilizando dados que são utilizados por terceiros.

Ao reconhecer que, ao mesmo tempo em que os usuários alimentam os algoritmos, eles são submetidos às influências dessas ferramentas, surge a necessidade premente de reavaliar o papel desempenhado por esse conjunto de indivíduos no ecossistema digital.

Byung-Chul Han argumenta que a psicopolítica é uma evolução da biopolítica, em que o foco se desloca da gestão dos corpos para a gestão das mentes e das subjetividades.

A biopolítica é a forma de governo da sociedade disciplinar. No entanto, é totalmente inadequada para o regime neoliberal, que explora principalmente a psique. A biopolítica, que se utiliza da estatística populacional, não tem nenhum acesso ao psíquico. Não fornece nenhum material para o psicoprograma da população. A demografia não é uma psicografia. Não explora a psique. Nisso reside a diferença entre a estatística e o Big Data. A partir do Big Data, é possível construir não apenas o psicoprograma individual, mas também o psicoprograma coletivo, talvez até o psicoprograma do inconsciente. Dessa forma, seria possível iluminar e explorar a psique até o inconsciente.⁶²

Nesse contexto, as tecnologias de informação desempenham um papel fundamental na criação de uma sociedade onde os indivíduos são constantemente monitorados e incentivados a se autorregular.

Além disso, o filósofo observa que, na sociedade contemporânea, a produção de subjetividade não necessariamente leva à libertação individual, mas muitas vezes resulta em formas de autoexploração e autoopressão. Em vez de ser um meio de libertação, a produção psíquica contribui para a intensificação da pressão sobre o indivíduo.

Na modernidade este fenômeno aconteceu por meio da apropriação capitalista ou estatal e no pós-moderno a cooperação produtiva é imposta pela intelectualidade massificada.

Mas, se a produção é produção de subjetividade, quer dizer, se são subjetivos o produtor e o produto, e o processo produtivo coincide com a esfera lingüística do intelecto geral biopolítico, então podemos explicar o nome comum "cooperação" como aquela força que reúne os produtores

⁶² HAN, Byung-Chul. **Psicopolítica**: O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte, MG: Âyiné, 2018. p. 35-36.

umentando sua capacidade produtiva e que, portanto, permite que a produção singular de subjetividade se torne potência produtiva. Isso quer dizer que não haveria produção se não houvesse cooperação.⁶³

É essencial compreender que a participação ativa em plataformas digitais implica na co-construção de narrativas e realidades. Os usuários devem considerar estratégias que promovam uma relação equitativa, com ênfase na cooperação solidária entre eles, visando romper com padrões de exploração subjacentes ao capitalismo digital.

A cooperação se torna problemática quando se direciona para alimentar algoritmos, em vez de focar na colaboração intrínseca para evadir as ciladas que tais algoritmos podem representar.

E assim, ao utilizar a cooperação a seu favor, os indivíduos podem evitar tornar-se os elementos-chave que atuam como “roteadores”, direcionando o fluxo e a dinâmica do capitalismo de vigilância.

No século XXI, a ascensão de uma intelectualidade massificada se desdobra por meio da revolução da chamada “big data”. Big data é um termo que se refere a conjuntos de dados extremamente grandes e complexos que não podem ser facilmente processados ou gerenciados com as ferramentas de processamento de dados tradicionais.

Essa revolução de dados em larga escala tem um impacto de como as informações são coletadas, analisadas e utilizadas.

O termo big data foi utilizado inicialmente no início do século XXI por astrônomos e geneticistas, a partir do momento em que a memória dos computadores não era capaz de armazenar a enorme quantidade de informação disponível, obrigando, assim, a se pensar em novas formas e instrumentos a análise dos gigantes bancos de dados.⁶⁴

As preocupações surgem quando os dados pessoais formam big datas, pois será “possível conhecer a personalidade, as atividades públicas e privadas, perfil, etc,

⁶³ NEGRI, Antonio. **Kairós, Alma Venus, Multitudo**: nove lições ensinadas a mim mesmo. Tradução: Orlando dos Reis e Marcello Lino Rio de Janeiro: DP&A, 2003. p. 179.

⁶⁴ SZINVELSKI, Martín Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. **Perspectivas em Ciência da Informação**, v. 24, 2020. p. 132-144.

muitas vezes, invadindo uma esfera estritamente pessoal de seu titular por natureza, o indivíduo”.⁶⁵

Os sistemas de informações tradicionais não eram mais suficientes para lidar com a magnitude desse influxo de dados. Isso levou à necessidade de repensar a maneira como esses dados seriam gerenciados e analisados.

Uma vez coletados, os dados podem ser usados para influenciar o comportamento e as decisões das pessoas. Empresas usam análises de dados para direcionar publicidade, enquanto governos podem usar informações para moldar políticas públicas.

Nesse sentido, essas práticas demonstram a debilidade do direito, que acaba sendo uma barreira fragilizada perante esses acontecimentos.

As novas tecnologias da informação e comunicação (TICs) permitem o estabelecimento de novas relações sociais, assim como o surgimento de problemas igualmente novos, o que, conseqüentemente, faz surgir um espaço vazio de regulamentação que não pode ser preenchido pelo tradicional direito, que, historicamente ligado a uma perspectiva centrada no Estado, se encontra incapaz de preencher essa lacuna. Nessa linha de raciocínio, em virtude desse vácuo regulatório, ocorre a apropriação do espaço digital pelo poder privado, o que amplia, ainda mais, a coleta, armazenamento e processamento de dados em larga escala (big data).⁶⁶

As dimensões de poder podem influenciar diretamente quem tem acesso aos dados e de que maneira eles são obtidos. Grandes empresas de tecnologia e agências governamentais frequentemente detêm considerável poder para coletar informações, muitas vezes sem o pleno consentimento dos indivíduos.

A coleta massiva de dados, a inteligência artificial e a automação estão redefinindo as relações de poder, transformando a maneira como as organizações e os indivíduos interagem e influenciam uns aos outros. Essa revolução tecnológica molda as dinâmicas em vários setores, desde a economia e a política até a sociedade em geral.

⁶⁵ RUARO, R.; MAÑAS, J.; MOLINARO, C. **Privacidade e Proteção de Dados Pessoais na Sociedade Digital**. Editora FI, 2017. p. 30.

⁶⁶BOLZAN DE MORAIS, José Luis; JACOB NETO, Elias; ALVES, Fabrício G.; GOMES, Igor da Silva. Accountability, transparência e assimetria das relações de visibilidade virtuais: análise dos aspectos antidemocráticos das novas tecnologias da informação e comunicação a partir da ideia de filtro bolha. *In.: Direito, Estado e Sociedade*, n. 53, 2018. p. 63.

Faustino e Lippold⁶⁷ explanam que para reverter o domínio tecnológico e enfrentar a missão civilizatória reinterpretada em uma abordagem tecnológica moderna envolve, em primeiro lugar, questionar os impactos prejudiciais do sistema de produção capitalista em todas as suas formas.

Descolonizar a tecnologia e confrontar a mission civilisatrice em novos moldes high-tech, é antes de qualquer coisa, colocar em xeque o caráter destrutivo do modo de produção capitalista em todas as suas dimensões sutis e declaradas. Essa crítica radical, no entanto, não nos isenta de nos posicionarmos diante de um campo que ainda está em construção e, portanto, permeável a uma série de disputas. Impõe-se como tarefa lutar – utilizando todos os meios necessários – pela democratização do acesso ao conhecimento, na direção da produção de uma ciência popular, assim como faz o site Sci-Hub, criado por Alexandra Elbakyan, ou como fez Aaron Swartz ao expropriar o monopólio do JSTOR, site que cobra quarenta dólares pelo download de um arquivo em formato PDF.⁶⁸

Como citado na seção 2.1 deste trabalho, poder também é conhecimento e a descolonização da tecnologia pode envolver a democratização do acesso ao conhecimento e do próprio poder relacionado à tecnologia⁶⁹.

Hackerspaces desempenham um papel fundamental na democratização do acesso ao conhecimento e na descolonização da tecnologia. Eles oferecem um ambiente colaborativo e inclusivo onde o conhecimento é compartilhado e amplamente acessível.

Hackerspaces, também conhecidos como *hacklabs*, são espaços físicos colaborativos onde entusiastas da tecnologia, artistas, programadores e outros interessados se reúnem para compartilhar conhecimentos, criar projetos, experimentar tecnologia e aprender uns com os outros. Esses locais são frequentemente caracterizados por um ambiente, onde a criatividade, a inovação e a colaboração são incentivadas.

O estabelecimento de um *LabHacker* na Câmara de Deputados do Brasil é um exemplo de como a demanda pública e a necessidade de inovação tecnológica podem influenciar o desenvolvimento de tais espaços.⁷⁰

⁶⁷ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023, p. 188.

⁶⁸ FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023, p. 189.

⁶⁹ RUIZ, Castor M. M. Bartolomé. 2004. **Os labirintos do poder**: o poder do simbólico e os modos de subjetivação. Porto Alegre: Escritos Editora, 281, p. 25

⁷⁰ CANUTO, L. C. Câmara inaugura Laboratório Hacker nesta quarta-feira. Câmara Notícias, 18 fev. 2014. Disponível em: Acesso em: 3 out. 2023.

Em meio à crise política e social que atingiu o Brasil em 2013, houve um crescente clamor por maior transparência, participação cidadã e inovação na política. Como resultado, o estabelecimento de um *hackerspace* na Câmara de Deputados foi uma resposta a essas demandas e às necessidades emergentes. Inclusive, participaram ativamente do projeto de lei que regulamentou o Marco Civil da *Internet*.

Essa iniciativa demonstrou a importância de incorporar conhecimentos técnicos e tecnológicos na formulação de leis relacionadas à *Internet* e à privacidade. Objetivando a proteção dos direitos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural.

O envolvimento do *hackerspace* no projeto de regulamentação do Marco Civil da *Internet* ajudou a garantir que a legislação refletisse as necessidades e os valores da sociedade em relação à *Internet* e à proteção dos direitos dos usuários. Além disso, enfatizou a participação cidadã e a colaboração na elaboração de políticas que moldam o ambiente online.

Embora o *hackerspace* seja uma das estratégias para descolonizar a tecnologia, é fundamental reconhecer que a cultura hacker e os princípios que ela representa, como abertura, transparência e inovação, podem ser objeto de apropriação e cooptação pelo capitalismo informacional.

A construção de sentido para as novas estéticas do capitalismo informacional vai, portanto, se alimentar do discurso contra-hegemônico e antiautoritário de diversas atitudes hackers para se coligar às narrativas de representatividade atuais. É característica do capitalismo como sistema absorver culturas e práticas críticas, cooptando-as e as absorvendo para seus objetivos de mercado.⁷¹

O capitalismo é conhecido por sua capacidade de assimilar culturas e práticas críticas, absorvendo-as e adaptando-as para seus próprios objetivos comerciais. Nesse contexto, as narrativas de representatividade e antiautoritarismo que frequentemente estão associadas às atitudes hackers podem ser utilizadas para atender aos interesses do mercado.

A representatividade dos movimentos sociais é fundamental para a participação nas normativas relacionadas à governança de dados. É por meio da inclusão de

⁷¹ FARIAS, Camila Cavalcante et al. **Que vírus é esse?** Reflexos da cultura hacker na vida política brasileira. 2022. p. 74.

diversas perspectivas e vozes, muitas vezes ausentes das decisões sobre dados, que se rompe com o eurocentrismo e se promove uma governança mais justa e inclusiva⁷².

A exploração de dados para fins lucrativos pode acentuar a divisão econômica, ampliando a concentração de riqueza em detrimento das classes menos favorecidas. A “uberização” é um termo que se originou a partir do nome da empresa Uber, que revolucionou a indústria de transporte ao criar um modelo de negócios baseado em aplicativos móveis, conectando motoristas independentes a passageiros por meio de uma plataforma digital⁷³.

A uberização se torna uma tendência no século XXI não apenas em empresas de transporte, como a Uber, mas também em setores de entrega de alimentos, hospedagem, serviços de limpeza, assistência domiciliar e em várias outras áreas.

O trabalho nas plataformas digitais (aplicativos) tem representado um novo laboratório para os experimentos do capital e para a luta de classes contra o combo datificação-financeirização sob a ordem neoliberal. No entanto, apesar de apresentar contornos novos, esse laboratório não nasceu com a uberização, sendo uma materialização e consequência de um processo histórico que combina: capitalismo rentista, ideologia do Vale do Silício, extração de dados e gestão neoliberal.⁷⁴

Essa transformação não se baseia apenas nas relações de trabalho, mas se estende a relações sociais mercantilizadas de maneira mais ampla, ou seja, a relações de dados que serão explanadas no capítulo três.

Conforme mencionado anteriormente, este fenômeno caracteriza-se como uma manifestação do capitalismo de cooperação, que emprega a mão de obra dos indivíduos, criando uma ilusória sensação de autonomia.

A uberização, ao mesmo tempo em que precariza o trabalho também é responsável pela extração de dados dos usuários registrados nas plataformas correspondentes.

Isto é, a partir das ações, dos cliques na rede e dos itinerários, as empresas armazenam dados de mais de milhões de pessoas e produzem análises que servem para delinear padrões de comportamento futuros, e, a partir disso,

⁷² FAUSTINO, Deivison; LIPPOLD, Walter. **Colonialismo digital**: Por uma crítica hacker-fanoniana. Boitempo Editorial, 2023. p. 189.

⁷³ ABÍLIO, Ludmila Costhek; AMORIM, Henrique; GROHMANN, Rafael. Uberização e platformização do trabalho no Brasil: conceitos, processos e formas. *Sociologias*, v. 23, p. 26-56, 2021.

⁷⁴ GARCEZ, R. M. **Plataformas digitais e uberização do trabalho**: Uma distopia no capitalismo contemporâneo. Disponível em http://www.joinpp.ufma.br/jornadas/joinpp2021/images/trabalhos/trabalho_submissaold_850_850612c1fa375549.pdf. Acesso em: 5 nov. 2023.

venda de publicidade. Se no capitalismo industrial o trabalho tornou-se uma forma abstrata da mercadoria, no capitalismo atual há uma transformação completa “da vida humana em uma nova forma social abstrata que também está pronta para a mercantilização: os dados.”⁷⁵

A vida humana, incluindo ações cotidianas e preferências, é transformada em uma "nova forma social abstrata" que pode ser comercializada, ou seja, os dados pessoais estão prontos para serem usados com fins lucrativos. Essa perspectiva será melhor abordada no capítulo três.

A relação entre biopolítica, capitalismo de cooperação, *hackerspaces* e uberização destaca a insuficiência das normativas tradicionais em conter os avanços significativos que estão moldando a sociedade contemporânea. As estruturas regulatórias muitas vezes lutam para acompanhar o ritmo das inovações e transformações em curso.

A biopolítica, por exemplo, desafia as fronteiras convencionais das regulamentações de saúde e segurança, à medida que as questões de controle sobre a vida e o corpo se tornam cada vez mais complexas. A uberização, por sua vez, ilustra a forma como as normativas trabalhistas muitas vezes falham em proteger os direitos dos trabalhadores em um mundo de trabalho em constante mutação.

O direito, embora essencial para a organização da sociedade e a garantia de direitos individuais e coletivos, muitas vezes se depara com a rápida evolução e complexidade das interações econômicas, tecnológicas e sociais. As novas roupagens do capitalismo histórico apresentam desafios que ultrapassam os limites das estruturas legais tradicionais.

Nesse sentido, é importante reconhecer que o direito não representa o ponto mais alto da estrutura e, frequentemente, se mostra incapaz de lidar eficazmente com os desafios que surgem em diversas dimensões de poder. Esse problema se torna ainda mais evidente na contemporaneidade, em particular, na era do capitalismo de vigilância.

⁷⁵ BRANCO, Pedro Mendonça Castelo; DA SILVA, Sidney Jard. Uberização: as quatro facetas do controle. **Revista Tecnologia e Sociedade**, v. 19, n. 56, p. 303-318, 2023.

3 A ERA DO CAPITALISMO DE VIGILÂNCIA NA PERSPECTIVA DA PROTEÇÃO DE DADOS

O conceito de “Capitalismo de Vigilância” foi cunhado pela autora Shoshana Zuboff em seu livro “*The Age of Surveillance Capitalism*” (A Era do Capitalismo de Vigilância), publicado em 2018. A autora propôs essa teoria para descrever uma nova forma de capitalismo que surgiu na era digital, na qual a coleta massiva de dados pessoais se tornou o principal recurso econômico e a base para a geração de lucro.

A discussão sobre o impacto dessa era se tornou uma questão premente, uma vez que suscita preocupações éticas, legais e políticas sobre a privacidade individual, a segurança dos dados e o equilíbrio entre inovação tecnológica e proteção de direitos fundamentais.

A realidade capitalista pode ser compreendida como uma fonte de poder que merece ser incluída na discussão. Uma das principais consequências desse panorama nas dimensões sociais é a maneira como o capitalismo se manifesta e coordena os processos que permeiam a existência. Um exemplo notável dessa manifestação é o capitalismo de vigilância, que representa uma das formas peculiares pelas quais o sistema capitalista se apresenta.

Uma forma de controle, uma forma de manter o capitalismo neste cenário, é através do fenômeno do capitalismo de vigilância. Esse modelo não apenas explora a coleta massiva de dados pessoais, mas também cria um ambiente onde a vigilância constante se torna uma parte intrínseca da vida cotidiana.

Ao monitorar e analisar incessantemente nossos comportamentos, preferências e interações, o capitalismo de vigilância alimenta uma lógica que busca otimizar a eficiência econômica à custa da privacidade individual. Poderes e formas de controle que passam por cima de regulamentações, como por exemplo a Lei Geral de Proteção de Dados.

Na primeira seção, o objeto de estudo será o termo capitalismo de vigilância originado pela autora Shoshana Zuboff. Essa expressão reflete a fusão intrincada entre a busca pelo ganho financeiro e o controle de dados, delineando uma realidade onde a coleta e análise de informações se tornaram peças-chave na engrenagem do capitalismo moderno.

Na segunda seção, será realizada uma análise de como essas outras dimensões de poder, mais especificamente o capitalismo de vigilância, se configuram como um complemento das formas tradicionais do capitalismo já existente.

E, por fim, será abordada a necessidade de adotar abordagens complementares à regulamentação para a proteção de dados no contexto do atual capitalismo. Essas abordagens complementares visa equilibrar a inovação e o desenvolvimento econômico com a proteção efetiva da privacidade e dos direitos individuais em um cenário marcado pelo capitalismo de vigilância.

Isso decorre do reconhecimento de que o arcabouço legal, por si só, não representa o ápice da estrutura de defesa diante da crescente influência do capitalismo de vigilância. As abordagens regulatórias, embora essenciais, mostram-se vulneráveis frente aos desafios impostos por esta era.

3.1 CAPITALISMO DE VIGILÂNCIA: A FUSÃO ENTRE LUCRO E CONTROLE DE DADOS

O termo “capitalismo de vigilância” foi conceituado por Shoshana Zuboff, que é professora e autora norte-americana. Ela introduziu esse conceito em seu livro *“The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”*, publicado em 2018.

Neste livro, Zuboff desenvolveu a conceituação do capitalismo de vigilância e explorou como as empresas coletam e utilizam dados pessoais em larga escala para obter lucro e influenciar o comportamento das pessoas.

O capitalismo de vigilância é a essência do capitalismo histórico em novas roupagens. Karl Marx em O capital sustentava que, o capitalismo como um sistema econômico baseado na propriedade privada dos meios de produção, busca pelo lucro e exploração da força de trabalho.

O capital não tem, por isso, a mínima consideração pela saúde e duração da vida do trabalhador, a menos que seja forçado pela sociedade a ter essa consideração. Às queixas sobre a degradação física e mental, a morte prematura, a tortura do sobretrabalho, ele responde: deveria esse martírio nos martirizar, ele que aumenta nosso gozo (o lucro)? De modo geral, no entanto, isso tampouco depende da boa ou má vontade do capitalista individual. A

livre-concorrência impõe ao capitalista individual, como leis eternas inexoráveis, as leis imanentes da produção capitalista.⁷⁶

Da mesma forma como o capital tradicional muitas vezes desconsidera a saúde e a vida dos trabalhadores em busca do lucro, o capitalismo de vigilância pode desconsiderar a privacidade individual em prol do benefício comercial. A coleta constante de dados sem consentimento explícito pode levar à exposição excessiva e, em alguns casos, à manipulação das escolhas dos usuários.

No cenário atual, onde as fronteiras do conhecimento se expandem a cada instante, percebe-se que o melhor ponto de exploração é a tecnologia. Essa constante evolução não se limita apenas ao desenvolvimento de dispositivos mais sofisticados, mas abrange a criação e a aplicação de algoritmos inteligentes, a exploração da inteligência artificial e a interconexão global através da *internet*.

Na era da *internet*, o ato de armazenar dados revelou-se mais vantajoso do que descartá-las. Na concepção de Lévy, os desafios e riscos associados à virtualização da sociedade e a acumulação excessiva de informações pode resultar em alienação e perda de autenticidade nas experiências.⁷⁷

Como já citado no capítulo 2.2, Han aborda a sociedade do desempenho e a cultura da positividade na contemporaneidade. O autor argumenta que a sociedade neoliberal, com sua ênfase no desempenho, na produtividade e na positividade constante, gera novas formas de opressão e alienação.

As críticas de Byung-Chul Han à psicopolítica neoliberal se concentram em como a sociedade contemporânea, guiada por valores econômicos e de desempenho, afeta a subjetividade, a liberdade e o bem-estar psicológico dos indivíduos. “O sujeito do regime neoliberal parece com o imperativo da otimização de si, ou seja, ele morre da obrigação de produzir cada vez mais desempenho”.⁷⁸

O paradigma neoliberal, ao estabelecer a performance como critério central de valor, cria um ciclo em que a autoestima e a identidade pessoal estão ligadas à produtividade e ao sucesso material. A pressão constante para otimizar o desempenho individual gera uma série de consequências psicológicas e sociais.

⁷⁶ MARX, Karl. **O Capital**: Crítica da Economia Política: Livro I: O Processo de Produção do Capital. Tradução de Rubens Enderle. 2. ed. São Paulo, SP: Boitempo, 2017. p. 432.

⁷⁷ LÉVY, Pierre. **O que é o virtual?**. Editora 34, 2011.

⁷⁸ HAN, Byung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Áyiné, 2018. p. 48.

Essas consequências que o autor aborda na obra de Psicopolítica também são aprofundadas em sua obra “Sociedade do Cansaço”. Ao conectar os pontos entre esses dois trabalhos, Byung-Chul Han evidencia a persistência e a ampliação dos desafios psicológicos e sociais em um mundo impregnado pelos princípios do neoliberalismo.

Os três autores (Karl Marx, Byung Chul Han e Shoshana Zuboff) compartilham uma crítica ao capitalismo, embora sob diferentes perspectivas e contextos. Marx elaborou uma crítica abrangente destacando as fábricas como o produto mais aprimorado da exploração capitalista, visando desvelar os fundamentos do capitalismo para determinar as bases do Capital.

Atualmente, pensadores contemporâneos, em especial Han e Zuboff, deparam-se com uma ferramenta de trabalho renovada, confrontando novas configurações dessa exploração. Essa evolução ressalta a importância de não apenas compreender as críticas clássicas, mas também analisar as adaptações e transformações do sistema capitalista ao longo do tempo.

Assim como Marx questionava ironicamente se o sofrimento dos trabalhadores deveria martirizar o capital, no capitalismo de vigilância, há uma interrogação sobre os impactos sociais do controle extensivo de dados. No capitalismo de vigilância, os indivíduos muitas vezes têm uma falta significativa de controle sobre como suas informações pessoais são coletadas e usadas.

Embora o capitalismo de vigilância seja a essência do capitalismo histórico, ambos não possuem o mesmo conceito. “O capitalismo evolui em resposta às necessidades das pessoas em determinada época e lugar”.⁷⁹

Enquanto o capitalismo histórico tem suas raízes profundas na Revolução Industrial e nas transformações sociais que a acompanharam, o capitalismo de vigilância representa uma manifestação contemporânea que levanta questões específicas relacionadas à privacidade, autonomia individual e o papel das grandes empresas de tecnologia na sociedade.

Marx, no século XIX, conceituou o capitalismo como um sistema econômico em que os meios de produção eram controlados pela classe capitalista, enquanto os trabalhadores, que não possuíam esses meios, eram explorados pela extração de

⁷⁹ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 46.

mais-valia. Essa exploração ocorria no contexto da produção material, com os trabalhadores vendendo sua força de trabalho em troca de salários.

Quando Marx aborda essas questões, ele refere-se à produtividade, associada a maquinário e dinheiro. O que essas empresas contemporâneas realizam não se resume apenas à acumulação de capital financeiro; a expansão delas ocorre em termos de território e acesso, buscando obter cada vez mais recursos.

A busca por acesso a uma variedade mais ampla de informações e recursos transcende a mera acumulação monetária, evidenciando uma expansão em termos de alcance e influência no espaço econômico e digital.

A crítica de Marx permanece relevante, mesmo que não se deva ficar rigidamente preso a conceitos enraizados na era das fábricas. Está sendo testemunhada uma nova forma de poder no capitalismo contemporâneo, uma busca por expansão em um patamar diferente.

O controle sobre a subjetividade não pode ser equiparado simplesmente ao roubo de dados; em um capitalismo de vigilância, há acesso a essas dinâmicas.

O capitalismo de vigilância traz uma nova dimensão à exploração. Em vez de se concentrar apenas na produção física, esse modelo econômico se baseia na extração de dados pessoais. As empresas que atuam no capitalismo de vigilância coletam informações sobre as atividades online e *off-line* dos usuários, transformando esses dados em mercadorias valiosas para análise e previsão de comportamento.

Para Shoshana Zuboff (2021) a democracia é ignorada em favor do suporte às grandes corporações de tecnologia e ao sistema financeiro, com conteúdo avaliados de acordo com os termos de uso corporativo, em vez de normas democráticas, tornando o capitalismo de vigilância um verdadeiro “parasita” que se assemelha à visão de Karl Marx (1996) sobre o capitalismo do século XIX, quando ele o comparou a um vampiro que se alimenta do trabalho. Assim, a única diferença prática entre ambas as vertentes capitalistas é que ao invés do trabalho, o capitalismo de vigilância alimenta-se da experiência humana para prever, manipular e explorar comportamentos futuros dos indivíduos.⁸⁰

A comparação com a imagem que Karl Marx desenhou do capitalismo como um vampiro que se alimenta do trabalho adiciona uma dimensão crítica à análise.

⁸⁰ROSA, Nelson Sanchez; DORNELES, Lucio Faccio. Capitalismo de vigilância e dignidade humana: tecnologia, dados e exclusão na sociedade do século XXI. **LexCult: revista eletrônica de direito e humanidades**, v. 7, n. 3, 2023. p. 5.

Antigamente, cada trabalhador tinha domínio sobre como realizava suas tarefas no trabalho. No entanto, com o capitalismo de vigilância conceituado por Shoshana Zubbof, essa dinâmica muda. No século XXI, os trabalhadores não apenas executam suas funções, mas são dominados e controlados pelo processo produtivo como um todo, que se desenvolve socialmente.

Enquanto Marx se referia à exploração da força de trabalho, o capitalismo de vigilância estende essa exploração para além do trabalho formal. Agora, a extração de valor ocorre através da coleta de dados que abrange todos os aspectos da vida cotidiana, incluindo preferências, comportamentos, relações sociais e até mesmo emoções.

No contexto do capitalismo de vigilância, a exploração não ocorre apenas no processo de produção, mas também na esfera da privacidade individual. As empresas buscam extrair valor não apenas da força de trabalho, mas também da informação íntima dos usuários, muitas vezes sem o pleno entendimento ou consentimento desses usuários.

[...] se antes o trabalhador individual tinha o domínio e o controle do processo de trabalho, na sociedade capitalista desenvolvida, o trabalhador passa a ser dominado e controlado pelo processo produtivo em sua totalidade socialmente desenvolvida, e o desenvolvimento tecnológico exerce uma determinação fundamental neste processo.⁸¹

Esse tipo de exploração digital redefine as relações entre empresas e consumidores, introduzindo um novo tipo de controle que vai além das dinâmicas tradicionais do capitalismo.

Nesse cenário, a autonomia do consumidor muitas vezes é comprometida, uma vez que suas interações digitais são monitoradas e utilizadas para moldar estratégias empresariais. O desenvolvimento tecnológico, que antes exercia influência fundamental na reconfiguração do processo produtivo, agora também se estende para a esfera do consumo.

No contexto digital, direitos fundamentais, como o direito à privacidade e à dignidade humana, são potencialmente ameaçados pela aplicação de conhecimentos do campo da neurociência (e neuromarketing) na programação dos algoritmos de aplicativos e serviços digitais. Com isso, o fenômeno de modificação (induzida) de postura do indivíduo perante o

⁸¹ ARAUJO, Wecio Pinheiro. Marx e a indústria 4.0: trabalho, tecnologia e valor na era digital. **Revista Katálysis**, v. 25, 2022. p. 28.

compartilhamento espontâneo de informações historicamente atinentes às esferas da intimidade e da privacidade nas mídias sociais, como também as mídias sociais realizam a coleta massiva de dados pessoais com falta de transparência em seu uso, representando uma ameaça significativa à privacidade dos indivíduos.⁸²

Essa falta de transparência e controle sobre o uso dos dados pessoais representa uma ameaça significativa à privacidade e à autonomia dos indivíduos em um cenário digital em constante evolução.

Os estudos da neurociência e *neuromarketing* na programação de algoritmos de aplicativos e serviços digitais levantam questões sobre como essas práticas podem impactar o comportamento e as decisões dos indivíduos⁸³.

Ainda, o mais valor não pode ser equiparado ao conceito de "lucro", da mesma forma que o capital de vigilância não se limita a ser apenas uma versão aprimorada de "marketing".

A autora Shoshana, ao introduzir o conceito de "capitalismo de vigilância", oferece uma crítica para analisar essas questões. O termo "capitalismo de vigilância" como já citado, descreve uma forma de capitalismo em que as práticas de monitoramento constante das atividades digitais dos usuários desempenham um papel na geração de lucro e no controle social.⁸⁴

Zuboff denomina o capitalismo de vigilância com base em três momentos que eclodiram em agosto de 2011. Primeiramente, o marco inicial no Vale do Silício com a Apple, que acabou ultrapassando a maior capitalização do mundo.

Em segundo lugar, um tiroteio com a participação de policiais deflagrou protestos em Londres. E, por fim, a autora traz a situação envolvendo os espanhóis e o direito de esquecimento, desafiando o próprio Google⁸⁵.

O Vale do Silício tornou-se um epicentro global para inovação e desenvolvimento tecnológico. Além do domínio econômico da Apple, o cenário tecnológico na região também é marcado pelo protagonismo do Google. A apple em

⁸² ROSA, Nelson Sanchez; DORNELES, Lucio Faccio. Capitalismo de vigilância e dignidade humana: tecnologia, dados e exclusão na sociedade do século XXI. **LexCult: revista eletrônica de direito e humanidades**, v. 7, n. 3, 2023. p. 163.

⁸³ ROSA, Nelson Sanchez; DORNELES, Lucio Faccio. Capitalismo de vigilância e dignidade humana: tecnologia, dados e exclusão na sociedade do século XXI. **LexCult: revista eletrônica de direito e humanidades**, v. 7, n. 3, 2023. p. 163.

⁸⁴ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.

⁸⁵ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p.42.

2011 “prometeu um sonho digital com novas soluções para velhos problemas sociais e econômicos, e finalmente ultrapassou Exxon Mobil com a corporação mais capitalizada do mundo”.⁸⁶

O sucesso da Apple foi impulsionado pelo lançamento de produtos populares, como o iPhone e o iPad, que contribuiriam significativamente para o aumento do valor das ações da empresa.

Ao mesmo tempo que a ascensão da Apple parecia ratificar as reivindicações dos indivíduos da segunda modernidade, as ruas de Londres narravam o sombrio legado de um experimento de três décadas em crescimento econômico implicando exclusão social.⁸⁷

A Apple, com seus produtos inovadores, design elegante e estratégias de marketing eficazes, personificou muitos dos valores da segunda modernidade, onde a tecnologia não apenas atendia às necessidades práticas, mas também se tornava uma expressão de estilo de vida e identidade. A ascensão da empresa simbolizou a capacidade dos indivíduos de moldar suas vidas e experiências por meio da tecnologia. No entanto, enquanto a Apple prosperava, as ruas de Londres contavam uma história diferente⁸⁸.

A desigualdade social, a falta de oportunidades equitativas e a marginalização de certas comunidades podem ter sido resultados diretos desse experimento econômico. Nesse sentido, “apesar de uma década de explosivo crescimento digital que incluía o milagre da Apple e a entrada da *internet* na vida cotidiana, perigosas divisões sociais sugeriam um futuro ainda mais estratificado e antidemocrático”.⁸⁹

Diversas suposições foram feitas sobre os elementos que poderiam ter influenciado o surgimento dos protestos populares em agosto de 2011. Em relação aos motivos de cunho socioeconômico, são considerados desde a falta de emprego e a redução nos investimentos sociais do governo até as plataformas digitais, a cultura musical influente ou a ocorrência esporádica de delitos.

⁸⁶ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 42.

⁸⁷ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 59.

⁸⁸ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 59.

⁸⁹ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 60.

Paralelo a isso “em nome do ‘direito de ser esquecido’, os espanhóis haviam entrado na praça de touros brandindo capas vermelhas, resolvidos a dominar o mais feroz dos touros: o Google, o grande monstro do capitalismo de vigilância”.⁹⁰

O “direito de ser esquecido” refere-se à ideia de que as pessoas têm o direito de ter informações pessoais obsoletas ou irrelevantes removidas da esfera pública, especialmente no ambiente digital.

A Agência Espanhola de Proteção de Dados reconheceu que nem toda informação é digna de imortalidade. Algumas deveriam ser esquecidas porque isso é apenas humano. E não foi surpresa quando o Google questionou a ordem da agência perante a Suprema Corte espanhola, que selecionou um dos noventa casos, o do advogado Mario Costeja González, como referência para a Corte de Justiça da União Europeia. Ali, em maio de 2014, após demoradas e notáveis deliberações, a Corte de Justiça anunciou sua decisão de afirmar o direito de ser esquecido como um princípio fundamental da legislação da União Europeia.⁹¹

As reivindicações sociais tomaram conta da União Europeia, enquanto a ascensão da Apple representava a face triunfante da tecnologia na segunda modernidade, a resistência espanhola ao Google aponta para a consciência crescente sobre os desafios éticos e sociais associados ao capitalismo de vigilância.

Cada um dos noventa cidadãos tinha uma reivindicação exclusiva. Uma mulher fora intimidada pelo ex-marido e não queria que ele descobrisse na internet seu endereço. A privacidade de informação era essencial para sua paz de espírito e sua segurança física. Uma senhora de meia-idade estava constrangida por ter sido presa em seus tempos de estudante universitária. Um dos requerentes era um advogado, Mario Costeja González, que anos antes fora despejado de sua casa. Embora a questão já tivesse sido resolvida havia muito tempo, uma busca pelo nome do advogado no Google continuava a mostrar links para a notificação de despejo, o que, segundo ele, prejudicava sua reputação.⁹²

O Tribunal de Justiça da União Europeia (TJUE) decidiu somente em 2014 que os cidadãos têm o direito de solicitar a remoção de links para informações pessoais desatualizadas ou inadequadas nos resultados dos motores de busca, em certas condições.

⁹⁰ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p.77.

⁹¹ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p.78-79.

⁹² ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p.78.

No Brasil, como citado no capítulo primeiro, a Constituição Federal de 1988 assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas como direitos fundamentais. Além disso, o Marco Civil da *Internet*, a Lei Geral de Proteção de Dados Pessoais (LGPD) e outros dispositivos legais oferecem proteções relacionadas à privacidade e à utilização de dados pessoais na *internet*.

A jurisprudência brasileira também tem tratado de casos nos quais a proteção da privacidade é um elemento central, embora o termo “direito ao esquecimento” em si possa não ser utilizado de maneira explícita. Em alguns casos, tribunais brasileiros têm reconhecido o direito de pessoas de buscar a remoção de informações pessoais inadequadas ou desatualizadas em determinados contextos.

Embora não haja uma legislação unificada sobre o direito de esquecimento, algumas jurisdições, principalmente na União Europeia, têm reconhecido e regulamentado o direito ao esquecimento como parte dos direitos de privacidade.

O modelo econômico do capitalismo de vigilância se baseia na coleta massiva de dados dos usuários por meio de serviços digitais, como mecanismos de busca, redes sociais e dispositivos conectados. Tais informações são então utilizadas para personalizar anúncios e serviços, gerando receitas substanciais para as empresas do Vale do Silício.

O impacto do capitalismo de vigilância não se restringe apenas ao âmbito econômico. Ele permeia a sociedade, influenciando o comportamento online e moldando a forma como as pessoas interagem com a tecnologia. Assim como não se restringe apenas ao fator econômico, também se diferencia do termo tecnologia. Isso porque “essa nova lógica de acumulação não pode ser reduzida a uma única companhia ou a um grupo de companhias”.⁹³

Em sua análise, Zuboff destaca que o capitalismo de vigilância não é simplesmente sobre a coleta de dados, mas sobre a extração de valor a partir do comportamento humano monitorado. As empresas não apenas observam o que as pessoas fazem, mas usam esses dados para prever e influenciar comportamentos futuros, moldando assim as atividades das pessoas de maneiras que são muitas vezes invisíveis para elas.

O cenário contemporâneo revela uma evolução desse paradigma econômico, dando origem a uma forma de organização social com o chamado capitalismo de

⁹³ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 38.

vigilância. Esse fenômeno, descrito por pensadores como Shoshana Zuboff, transcende as fronteiras tradicionais da produção e da distribuição econômica.

Esse modo de acumulação de capital se estende para além do âmbito econômico, influenciando também as esferas política, cultural e social. Enquanto o capitalismo histórico enfrentou resistência por meio de movimentos sindicais e lutas trabalhistas, o capitalismo de vigilância apresenta desafios complexos para a defesa dos direitos individuais e coletivos.

Frequentemente, as pessoas fornecem seus dados sem perceber totalmente o valor dessas informações ou sem receber uma compensação direta. Isso ocorre frequentemente em troca de serviços gratuitos, como redes sociais, motores de busca ou aplicativos, onde os dados dos usuários servem como pagamentos de forma implícita.

A problemática da questão do capitalismo de vigilância não está somente nas empresas, mas também se estende a todos os setores que têm a *internet* como base. Nessa seara é importante distinguir que “assim como o capitalismo de vigilância não é o mesmo que tecnologia, essa nova lógica de acumulação não pode ser reduzida a uma única companhia ou a um grupo de companhias”.⁹⁴

Shoshana Zuboff, critica a prática desses setores que, em busca de lucro, invadem a privacidade de forma arbitrária, comprometendo os direitos individuais e influenciando escolhas sem o pleno consentimento dos usuários. “O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais”.⁹⁵

Nesse contexto, apesar da importância inegável das legislações para o ordenamento jurídico, é fundamental reconhecer que seu impacto se estende para além do âmbito legal. Isso implica uma necessidade premente de compreender as complexas dinâmicas de poder, os interesses econômicos envolvidos e as práticas de vigilância que permeiam a coleta e utilização de dados.

Por mais que a vigência dessa lei venha a significar um marco jurídico para a proteção de dados pessoais no Brasil, ela precisa ser visto no contexto da

⁹⁴ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 38.

⁹⁵ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 21.

economia política que lhe recebe, que é da mercantilização dos dados em uma economia da vigilância.⁹⁶

Assim, a análise crítica dessas leis deve abarcar não apenas seu impacto legal imediato, mas também sua eficácia em enfrentar os dilemas éticos e sociais que permeiam a relação entre poder, informação e proteção de dados. Afinal “O capitalismo de vigilância age por meio de assimetrias nunca antes vistas referentes ao conhecimento e ao poder que dele resulta”.⁹⁷

Esse fenômeno, inserido numa economia da vigilância, impõe desafios consideráveis à preservação da privacidade individual e à busca por um equilíbrio entre inovação tecnológica e proteção de direitos.

3.2 OS NOVOS SENHORES DO CAPITAL: PODER, INFORMAÇÃO E PROTEÇÃO DE DADOS

No segundo capítulo, ao adentrar na evolução dos poderes, observa-se que as novas roupagens dos “senhores do capital” se configuram como um complemento aos modelos tradicionais de poder existentes até o momento.

Destaca-se a ascensão do capitalismo de vigilância, que transcende as fronteiras convencionais e opera em diferentes dimensões de poder, especialmente na predominante era da informação.

O capitalismo de vigilância, conforme mencionado na seção 3.1, tem se expandido cada vez mais, tanto no âmbito econômico quanto na esfera social e política.

A respectiva seção não tem a pretensão de exaurir a complexidade das respectivas temáticas, mas abordar os principais impactos quando o estudo envolve dimensões de poder, informação e proteção de dados.

A primeira abordagem é sobre a grande influência da perfirização e consumo, onde as características individuais e padrões de consumo desempenham um papel significativo.

⁹⁶ 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 Práxis**, v. 12, 2021. p. 1006.

⁹⁷ ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 25.

No contexto da proteção de dados, a perfilização muitas vezes envolve a análise de informações sensíveis, como preferências pessoais, comportamentos online e até mesmo características biométricas.

A perfilização, conhecida como *profiling*, consiste na coleta e análise sistemática de dados para identificar padrões comportamentais e tornou-se uma ferramenta essencial para as entidades envolvidas nesse sistema.

Este pequeno ato individual de busca, que se assemelha aos cliques, likes e compartilhamentos em outras redes, ajuda a criar um gigantesco banco de dados de comportamento humano, que é a principal matéria-prima superavitária — a sobra da informação que as plataformas precisam para entender o que usuário procura — do novo regime.⁹⁸

O uso da perfilização em larga escala por entidades comerciais pode levar à criação de perfis extensos de consumidores, muitas vezes sem seu pleno conhecimento ou consentimento. Esses perfis podem ser utilizados para direcionar publicidade de maneira altamente personalizada.

No âmbito do consumo, a perfilização é frequentemente aplicada em estratégias de marketing e publicidade. Empresas utilizam dados para criar perfis detalhados dos consumidores, permitindo a personalização de campanhas publicitárias e o direcionamento de ofertas específicas com base nos interesses e comportamentos identificados.

O controle exercido pelo capitalismo de vigilância pode ser compreendido como uma forma avançada de publicidade na era biopolítica. Nesse contexto, o objetivo não é mais simplesmente seduzir um cliente, mas sim governar a possibilidade de alternativas para o cidadão.

Esse novo paradigma reflete a ênfase não apenas na persuasão individual, mas na regulação das escolhas coletivas, evidenciando a complexidade e amplitude do impacto do capitalismo de vigilância na sociedade contemporânea.

Entretanto, a indústria dos dados tem utilizado os algoritmos sem as preocupações ora mencionadas, especialmente para fins de classificações, perfilações e predições, fenômeno que também é reflexo do fato de que a

⁹⁸ SCOFIELD JR, Gilberto. Extração secreta de dados, lucro e manipulação: A lógica econômica do capitalismo de vigilância. **Revista Eco-Pós**, v. 26, n. 01, 2023. p. 580.

utilização da inteligência artificial em várias searas vem ocorrendo sem o correspondente e necessário debate ético e jurídico.⁹⁹

Assim, o capitalismo de vigilância transcende a esfera do mercado, transformando-se em um mecanismo de controle social que influencia não apenas o consumo, mas também as dinâmicas políticas e culturais.

Como vem sendo mencionado, a simples proteção jurídica, desprovida de uma abordagem inclusiva, revela-se inadequada para lidar com os desafios que essa dimensão apresenta.

Principalmente com a chegada inteligência artificial, mecanismo este que vem para revolucionar diversos fatores. E que ainda, não se tem normativa no Brasil a fim de regulamentar a questão.

Esta lacuna normativa realça a dificuldade do direito em manter-se no ápice da pirâmide regulatória diante de avanços tecnológicos que transcendem as estruturas legais existentes.

Grande parte da personalização proporcionada por algoritmos nas aplicações de Internet mais populares adota uma forma de inteligência artificial. A recomendação de novas músicas (de acordo com o histórico de audições), a seleção de quais postagens irão aparecer primeiro no feed de notícias de uma rede social (com base nas interações prévias) e mesmo o melhor caminho a seguir em um aplicativo de trânsito (com base nas informações sobre engarrafamentos na cidade) são aplicações de inteligência artificial. Essas aplicações se tornam ainda mais interessantes para o debate sobre ética e implicações legais quando incorporadas em um robô, servindo como um verdadeiro hardware que interage com o ambiente externo. Os questionamentos trazidos pela popularização dos robôs inteligentes desafia (e desafiará) o Direito de forma diferente daquela experimentada com a expansão da Internet nas últimas duas décadas.¹⁰⁰

Os casos citados por Doneda, como o histórico de audições, a organização de postagens e as manipulações de dados, especialmente em aplicativos de trânsito, conforme será abordado mais adiante, evidenciam de que a esfera tecnológica está avançando à frente no século XXI.

A evolução acelerada dos algoritmos, o surgimento de novos modelos de aprendizado de máquina e a diversificação das aplicações da inteligência artificial tornam desafiador para as normativas tradicionais acompanhar.

⁹⁹ FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 1 ed. São Paulo: Thomson Reuters Brasil, 2019. p. 35.

¹⁰⁰ DONEDA, Danilo Cesar Maganhoto et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar-Revista de Ciências Jurídicas**, v. 23, n. 4, 2018. p. 7.

A manipulação de dados pode moldar percepções, influenciar escolhas individuais e coletivas, e até mesmo afetar questões relacionadas à saúde, educação e outros aspectos da vida cotidiana.

No capítulo 3.1, foram citados exemplos que afetaram tanto no contexto de saúde (dados sensíveis) quanto político com as chamadas fake News. Na educação, o exemplo é claro quando o Google, assume caráter cada vez mais dependente e condicionante.

Inserida em uma era que “pode ter como epíteto o tráfego de dados em forma de hiperinformação, a calamidade, a catástrofe, a situação emergencial ou epidêmica, traz consigo ares de uma rediviva e notável oportunidade para o reforço dos exercícios de poder e controle”.¹⁰¹

Principalmente na pandemia do Covid-19 em 2020, em que houve a presença dominante do Google no campo educacional, com ferramentas como *Google Classroom* e *Google Meet*.

Essa integração está gerando uma dependência considerável, enquanto simultaneamente o Google armazena vastas quantidades de dados.

No caso das universidades públicas brasileiras analisadas, as parcerias não envolvem o pagamento direto pela utilização desses serviços. Afirma-se que os serviços são oferecidos gratuitamente, ignorando os custos operacionais e de pessoal das instituições educacionais. Sabemos, no entanto, que a oferta e manutenção desses serviços, que envolvem centenas de milhares de contas com espaço “ilimitado” em servidores, têm um alto custo no mercado. Neste caso, quais são as possíveis vantagens que a empresa pode obter nesta parceria? Quanto vale e quanto “custa” o gratuito?¹⁰²

A gratuidade dessa educação não se traduz em ausência de custos, uma vez que os dados gerados nesse processo são valiosos para a empresa, contribuindo para seu vasto ecossistema de informações.

Além disso, ao comparar os custos associados à contratação de serviços para gerenciar o e-mail institucional de uma universidade brasileira, a mesma pesquisa destacou a disparidade econômica entre as opções disponíveis.

¹⁰¹ LUZ, A. F.; CHINI, M.; DIVAN, G. A. Poder, Discurso Científico e Biopolítica: leitura inicial da perspectiva de calamidades globais sob o conceito de onicrise. *In.*: PILAU SOBRINHO, L. L.; CALGARO, C.; ROCHA, L. S. (Org.). **COVID-19: democracia e poder**. 1ed. Itajaí/SC: Univali, 2020. p. 99.

¹⁰² PARRA, Henrique et al. Infraestruturas, economia e política informacional: o caso do Google Suite for Education. **Mediações-Revista de Ciências Sociais**, 2018. p. 79.

Enquanto a G Suite do Google oferecia funcionalidades semelhantes de maneira gratuita, os custos incorridos pela universidade ao escolher outras soluções foram substancialmente mais elevados.

Nesse sentido, plataformas como *Google Classroom* e *Google Meet*, a educação se torna cada vez mais vinculada à infraestrutura e políticas de dados do Google. Essa "oferta gratuita" é, na verdade, um investimento estratégico para o Google, que acumula valiosas informações sobre usuários e comportamentos.

Nos documentos que analisamos da GSuite há diferentes versões sobre a forma de gestão dos dados e da comunicação. No geral, a Google afirma que nos serviços educacionais oferecidos não haverá publicidade dirigida ao usuário. Mas ao analisarmos os documentos referentes aos termos de serviço e à política de privacidade do GSuite, não conseguimos esclarecer essa dúvida.¹⁰³

Emergem muitas discussões sobre essas novas formas de manipulação, onde o Google não apenas responde a interesses já existentes, mas também os molda ativamente.

Essa capacidade de moldar ativamente os interesses e comportamentos dos usuários suscita inquietações sobre o poder e a influência que grandes empresas de tecnologia podem exercer principalmente na esfera educacional.

Este processo cria, de maneira biopolítica, uma conexão entre os interesses do Google e a noção de verdade, destacando uma complexa relação entre poder, informação e manipulação.

Os termos "*Big Data*" e "*Big Techs*" possuem aspectos distintos, mas que se complementam na era tecnológica. Big data como também já mencionado nos capítulos iniciais, refere-se à enorme quantidade de dados gerados diariamente em diversas fontes e formatos.

Por outro lado, as "*Big Techs*" são grandes empresas tecnológicas que são responsáveis por desenvolver, manter e inovar em produtos e serviços tecnológicos.

Os chamados novos senhores do capital emergem principalmente das grandes empresas de tecnologia, nas *Big Techs*, como *Google*, *Apple*, *Facebook*, *Amazon* e *Microsoft*. Estas empresas não apenas dominam os mercados globais, mas também exercem uma influência nas inovações tecnológicas.

¹⁰³ PARRA, Henrique et al. Infraestruturas, economia e política informacional: o caso do Google Suite for Education. **Mediações-Revista de Ciências Sociais**, 2018. p. 80.

Os produtos e serviços do capitalismo de vigilância não são objeto de uma bolsa de valores. Não estabelecem reciprocidades construtivas produtor-consumidor. Em vez disso, são “ganchos” que seduzem usuários para suas operações extrativas nas quais nossas experiências pessoais são sucateadas e empacotadas como meios para fins de outros.¹⁰⁴

O capitalismo de vigilância concede aos novos senhores do capital, apelidados de "monstros" por Zuboff, uma capacidade sem precedentes. A estratégia agora se baseia em políticas de “aceito termos”, eliminando a exigência de uma grande ideia para exercer influência sobre as pessoas.

O domínio do capitalismo, que antes era exercido, agora se intensifica de forma mais potencializada, expandindo-se para novas áreas. A possibilidade que o capitalismo de vigilância oferece a eles, nenhum domínio proporcionou anteriormente. Os dados permitem aos novos senhores.

Dessa maneira, o capitalismo de vigilância gera uma nova espécie de poder que chamo de instrumentarismo. O poder instrumentário conhece e molda o comportamento humano em prol das finalidades humanas. Em vez de armamentos e exércitos, ele faz valer sua vontade através do meio automatizado de uma arquitetura computacional cada vez mais ubíqua composta de dispositivos, coisas e espaços “inteligentes” conectados em rede.¹⁰⁵

Esse é um tipo de capitalismo que não depende mais dos atributos tradicionais. Antigamente, era necessário investir em pesquisas publicitárias, mas hoje acontece por meio da vasta extração de dados. Os novos senhores, detêm o controle através da análise de informações, tornando-se os senhores supremos nesse contexto.

Enquanto a Primeira Revolução Industrial foi baseada em água e vapor para mecanizar a produção, e a Segunda usou energia elétrica para criar produção em massa; a Terceira Revolução Industrial alavancou a eletrônica e a tecnologia da informação para automatizar a produção. Agora, devido ao número de tecnologias que, progressivamente, estão se integrando no nosso dia a dia (variando de robótica e inteligência artificial à biotecnologia e à Internet das coisas), estamos na Quarta Revolução Industrial que, alimentada por dados, está eliminando as fronteiras entre a Física e a Biologia.¹⁰⁶

¹⁰⁴ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 24.

¹⁰⁵ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 22.

¹⁰⁶ DONEDA, Danilo Cesar Maganhoto et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar-Revista de Ciências Jurídicas**, v. 23, n. 4, 2018. p. 10.

Uma característica marcante dessa quarta fase é a ênfase nos dados, indicando que a revolução atual está sendo impulsionada pela coleta, processamento e utilização de informações.

A integração de tecnologias avançadas, aliada à capacidade de processar grandes volumes de dados, está moldando cada vez mais a sociedade do século XXI.

Ao praticar essa forma de controle, os detentores de poder acabam por utilizar a biopolítica como uma ferramenta para direcionar e influenciar as decisões e comportamentos dos indivíduos. Isso influencia diretamente a abordagem de perfis, transcendendo os limites da mera publicidade.

A conexão digital é agora um meio para fins comerciais de terceiros. Em sua essência, o capitalismo de vigilância é parasítico e autorreferente. Ele revive a velha imagem que Karl Marx desenhou do capitalismo como um vampiro que se alimenta do trabalho, mas agora com uma reviravolta. Em vez do trabalho, o capitalismo de vigilância se alimenta de todo aspecto de toda a experiência humana.¹⁰⁷

Exemplo disso é a “uberização”, que tem se propagado em diversos setores. Existem duas vertentes desse fenômeno: a exploração do trabalho com o conceito de cooperação, como já exposto no segundo capítulo, e a extração de dados que é o objeto de estudo desse capítulo.

Em 2016 aconteceu um dos eventos mais notáveis envolvendo os dados dos passageiros e motoristas da empresa Uber. Nesse incidente, a empresa foi acusada de ocultar um vazamento massivo de dados de usuários e motoristas, revelando as vulnerabilidades inerentes à coleta e gestão de informações na era digital.

“A Uber se vale largamente dessa prática, isso porque, além de explorar o trabalho dos motoristas, a empresa também obtém retorno financeiro do enorme banco de dados que possui das viagens de milhões de usuários”.¹⁰⁸

A empresa Uber possui conhecimento preciso sobre localização e horário, sendo capaz de realizar promoções e insistir remotamente (online) para que o indivíduo acione o aplicativo, algo semelhante ao que a Amazon faz.

¹⁰⁷ ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 23.

¹⁰⁸ BRANCO, Pedro Mendonça Castelo; DA SILVA, Sidney Jard. Uberização: as quatro facetas do controle. **Revista Tecnologia e Sociedade**, v. 19, n. 56, 2023. p. 308.

Sobre a extração de dados, “o que salta aos olhos em todo o controle até aqui descrito é a enorme quantidade de dados que a Uber utiliza, dados que não são só dos motoristas, mas também dos passageiros”.¹⁰⁹

A conscientização sobre segurança cibernética e a educação sobre a importância da proteção de dados tornam-se componentes essenciais na construção de uma postura preventiva contra essas violações de privacidade.

Shoshana Zubooff, argumenta que o modelo de negócios de vigilância representa uma mudança fundamental na dinâmica econômica e social, onde a extração de dados se torna uma fonte dominante de valor econômico.

A promessa de recompensas financeiras é, para ela, uma isca que atrai organizações ávidas por um enriquecimento rápido, sem se importar com as implicações corrosivas para a privacidade e autonomia individual.

Tanto empresas novas quanto estabelecidas de todos os setores — inclusive de varejo, refeições, fitness, seguros, automotivo, de viagens, hospedagem, saúde e educação — estão aderindo ao curso migratório para as receitas de vigilância, seduzidas pelo magnetismo do crescimento e lucro desmedidos e a promessa da pródiga recompensa que somente os mercados financeiros são capazes de proporcionar.¹¹⁰

Zuboff adverte sobre os impactos sociais e éticos desse tipo de prática, destacando preocupações com a privacidade, manipulação comportamental e poder desproporcional nas mãos das empresas que controlam esses vastos conjuntos de dados.

Em sua visão crítica, o capitalismo de vigilância não apenas representa uma mudança nas dinâmicas econômicas, mas uma ameaça substancial aos princípios democráticos, colocando o controle dos dados nas mãos de empresas que priorizam o lucro em detrimento do bem-estar e da liberdade individuais.

O capitalismo de vigilância não é somente uma transformação nos modelos de negócios, mas uma ameaça à integridade das sociedades, minando a confiança, ampliando desigualdades e comprometendo os alicerces democráticos ao permitir que empresas controlem indiscriminadamente vastos conjuntos de dados.

¹⁰⁹ BRANCO, Pedro Mendonça Castelo; DA SILVA, Sidney Jard. Uberização: as quatro facetas do controle. **Revista Tecnologia e Sociedade**, v. 19, n. 56, 2023. p. 308.

¹¹⁰ ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 213.

As empresas que detêm vastos conjuntos de dados não só exercem um poder desproporcional sobre os consumidores, mas também reforçam disparidades socioeconômicas ao consolidar recursos e influências em suas mãos.

A expansão desenfreada do capitalismo de vigilância, na perspectiva da autora, contribui para a ampliação das desigualdades. Isso cria um ciclo, onde os mais poderosos se tornam ainda mais dominantes, marginalizando aqueles que não têm acesso ou controle sobre seus próprios dados.

A proteção dos dados pessoais não deve ser encarada apenas como uma questão técnica, mas sim como um imperativo ético e social. À medida que os consumidores compartilham informações cada vez mais sensíveis em troca de conveniência e serviços personalizados, é importante que as empresas assumam a responsabilidade de garantir a segurança e a privacidade desses dados.

A humanidade vive um período denominado Sociedade da Informação, dado que, dentre suas características, encontrar-se o fato de as comunicações, principalmente aquelas realizadas por meio da Internet, terem se massificado e atingindo grandes contingentes populacionais ao redor do mundo. O problema é que o usuário deixa dados ao utilizar a internet, dados esses de caráter pessoal, acessíveis a terceiros que os utilizarão para diversas finalidades, não apenas para o mercado de consumo.¹¹¹

A denominada sociedade da informação está ligada ao avanço das tecnologias da informação e comunicação (TICs) e à rápida expansão da internet. Na sociedade da informação, o acesso e o controle sobre dados e conhecimento tornaram-se fundamentais para o desenvolvimento econômico, social e político.

A sociedade da informação não se limita meramente ao avanço tecnológico; ela confronta desafios associados ao controle, utilização ética e salvaguarda dos dados.

A proposta deste trabalho não se limita a abordar apenas os aspectos negativos da internet; pelo contrário, visa enfatizar que essa nova era, representada pelo capitalismo de vigilância, está transformando a forma como os dados dos usuários são protegidos.

¹¹¹ MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Revista Eletrônica Direito e Sociedade-REDES**, v. 7, n. 3, 2019. p. 136.

Busca-se explorar as implicações dessa transformação na dinâmica entre usuários e plataformas digitais, questionando como a proteção de dados pode ser efetivamente assegurada diante desse novo paradigma de vigilância.

Destaca-se a complexidade desse cenário, onde a coleta massiva de dados muitas vezes ultrapassa os limites da privacidade individual, suscitando preocupações.

Inclusive a era da sociedade da informação, trouxe muitos benefícios e inovações, a disseminação de informações tornou-se mais eficiente, possibilitando o acesso rápido a conhecimentos diversos e promovendo avanços significativos em diversas áreas, como medicina, ciência, educação e negócios.

Principalmente no âmbito da medicina, a sociedade da informação possibilitou um cenário de rápida de pesquisas e avanços científicos. O compartilhamento instantâneo de informações médicas contribui para diagnósticos mais precisos e tratamentos personalizados.

A colaboração entre profissionais de saúde em diferentes partes do mundo tornou-se mais acessível, favorecendo a troca de conhecimentos e experiências clínicas, resultando em benefícios tangíveis para pacientes e comunidades.

Nesse sentido, a era da sociedade da informação desencadeou uma revolução em como compartilhar, acessar e aplicar o conhecimento, impactando positivamente diversos setores.

Embora a era tecnológica tenha trazido tantas inovações, há uma série de efeitos colaterais que os novos senhores do capital carregam como já citado em todos os capítulos, sendo os principais: riscos à privacidade, manipulações, desigualdade digital, falta de transparência e insegurança cibernética.

A transparência nas práticas dessas gigantes tecnológicas é de extrema importância. Os usuários precisam compreender como seus dados são coletados, utilizados e compartilhados, possibilitando escolhas informadas sobre sua participação nesse ecossistema digital.

A falta de transparência pode resultar em um ambiente em que a assimetria de informações favorece as empresas em detrimento dos consumidores, ampliando os desequilíbrios de poder já existentes.

Além disso, a desigualdade digital surge da disparidade no acesso e domínio da tecnologia. Aqueles que não têm as mesmas oportunidades de participar

plenamente na era digital ficam à margem, aprofundando as divisões sociais e econômicas.

O aparato ubíquo opera por meio da coerção e de um comportamento sub-reptício. Nosso progresso na vida necessariamente nos faz atravessar o universo digital, onde a renderização voluntária tem se tornado um fato inescapável. Somos deixados com poucos direitos para saber, ou para decidir quem sabe, ou para decidir quem decide. A divisão anormal da aprendizagem é criada e sustentada por um decreto secreto, implementado por métodos invisíveis e dirigido por companhias sujeitas aos imperativos econômicos de uma estranha nova forma de mercado. Capitalistas de vigilância impõem sua vontade dos bastidores, enquanto os atores encenam suas cantigas de transparência e concordância para o público.¹¹²

Essa falta de transparência é apontada como um elemento fundamental do modus operandi das empresas envolvidas no capitalismo de vigilância, que, agem de maneira oculta enquanto proclamam publicamente princípios de transparência e consentimento.

A crítica ressoa na ideia de que os capitalistas de vigilância impõem sua vontade nos bastidores, operando fora do escopo do entendimento público, enquanto as empresas apresentam uma fachada de transparência e conformidade.

Seja na oferta de serviços educacionais pela Google ou nas transações cotidianas pela Uber, a proteção dos dados pessoais torna-se primordial para preservar a confiança dos usuários e garantir a integridade das interações digitais na sociedade da informação.

Nesse contexto, a questão é: por que considerá-los os novos senhores? Isso caracteriza o que podemos chamar hoje de manipulação. Eles aspiram a ser a fonte e o curso d'água, exercendo controle sobre tudo.

3.3 A NECESSIDADE DE ABORDAGENS COMPLEMENTARES À REGULAMENTAÇÃO NA PROTEÇÃO DE DADOS NO CAPITALISMO DE VIGILÂNCIA

No capítulo 1, abordou-se a historicidade das principais normativas do Brasil relacionadas à proteção de dados. Na análise da historicidade das normativas, identificou-se padrões e tendências que podem ter influenciado a elaboração das leis.

¹¹² ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 306.

Ao explorar a historicidade das normativas, é possível compreender as mudanças legislativas, a criação de novos órgãos reguladores, e como as normativas foram influenciadas pelos avanços tecnológicos.

Além disso em 2022, foi promulgada a Emenda Constitucional 115 que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais previstos na Constituição Federal. Inclusive foi citada pelo deputado Orlando Silva, relator da emenda, como parte da arquitetura digital ao lado do Marco Civil da Internet e da Lei Geral de Proteção de Dados.¹¹³

A inclusão da proteção de dados como direito fundamental representa um reconhecimento da importância da privacidade e do controle sobre as informações pessoais na atual sociedade.

Quanto aos efeitos gerados por essa proteção, alinhando-a ao conceito de autodeterminação informativa, é possível pensá-los a partir de uma dupla dimensão. De um lado, essa proteção se desdobra como liberdade negativa do cidadão oponível perante o Estado, demarcando seu espaço individual de não intervenção estatal (dimensão subjetiva). De outro lado, ela estabelece um dever de atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva).¹¹⁴

A proteção de dados, alinhada ao conceito de autodeterminação informativa, não apenas preserva a liberdade individual frente ao Estado, mas também demanda uma postura ativa por parte do Estado para garantir que esse direito fundamental seja efetivamente respeitado e aplicado na prática.

Na data 27/12/2023, na finalização deste capítulo, o Presidente da República Luiz Inácio Lula da Silva, sancionou a Lei nº 14.533/2023 que estipula a política nacional de educação digital.

O objetivo é propiciar a todos os alunos uma educação igualitária. Nas instituições privadas, muitas já utilizam a chamada educação 4.0, que abrange a inteligência artificial, gamificação no ensino, entre outras inovações.

¹¹³ Câmara dos Deputados. **Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão.** Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/>. Acesso em: 02/01/2023.

¹¹⁴ MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**, São Paulo, v. 130, jul./ago. 2020. p. 3.

A respectiva Lei visa permitir uma mudança cultural para que todos possam ter acesso à educação digital. A Lei 14.533/2023, “altera a Lei de Diretrizes e Bases da Educação (LDB) para fixar a educação digital como dever do Estado por meio da garantia de conectividade à internet de alta velocidade de todas as instituições públicas de ensinos básico e superior”.¹¹⁵

Segundo o Presidente da República, a normativa é uma política pública para proporcionar a todos as mesmas oportunidades, no que diz respeito aos avanços tecnológicos.

Destaca-se a importância da igualdade de oportunidades no acesso à tecnologia, a iniciativa visa criar um ambiente inclusivo que permite a todos usufruir dos benefícios proporcionados pelo avanço tecnológico.

Ainda em 2023, a Rede Nacional de Ensino e Pesquisa (RNP), o SENAI-SP e a Softex, com apoio do Ministério da Ciência, Tecnologia e Inovações, criaram um curso gratuito em cibersegurança, do básico ao avançado, justamente para incentivar a proteção de dados.¹¹⁶

A educação digital é considerada primordial quando o assunto é proteção de dados, sendo uma ferramenta essencial para capacitar os cidadãos a navegarem de maneira segura e consciente na era digital.

Na seção 1.1, que discorre sobre a regulamentação da proteção de dados no Brasil e seus elementos históricos, foram mencionados os princípios que norteiam a Lei Geral de Proteção de Dados, os quais incluem garantias de medidas preventivas contra incidentes.

Uma dessas medidas consiste na promoção da educação digital, visando conscientizar os usuários sobre a importância e o manuseio de seus dados pessoais.

Assim, a educação digital perfaz a ideia de consciência de preservação de dados, mas também a permissão, através do consentimento, de escolhas com racionalidade, livres e informadas sobre o tratamento de seus dados pessoais, incluindo-se aí a finalidade com que tais dados serão utilizados. Ademais, faz-se imperativo que tal declaração de vontade seja inequívoca,

¹¹⁵ Câmara dos Deputados. **Lula sanciona com vetos lei que cria a Política Nacional de Educação Digital**. Disponível em: Lula sanciona com vetos lei que cria a Política Nacional de Educação Digital - Notícias - Portal da Câmara dos Deputados (camara.leg.br). Acesso em: 02 jan. 2023.

¹¹⁶ Ministério da Ciência, Tecnologia e Inovações. **Programa "Hackers do Bem" vai fortalecer a cibersegurança no país**. Disponível em <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2023/05/programa-hackers-do-bem-vai-fortalecer-a-ciberseguranca-no-pais>. Acesso em: 15 jan. 2024.

por assim dizer, de maneira expressa e específica, afastando quaisquer inseguranças possíveis no tratamento de dados pessoais.¹¹⁷

Nesse sentido, uma estratégia essencial é a promoção da educação digital, que busca conscientizar os usuários sobre a importância da privacidade online e capacitá-los para fazer escolhas informadas sobre o compartilhamento e o uso de suas informações pessoais.

A educação digital contribui para fortalecer a autonomia dos indivíduos no uso da tecnologia, capacitando-os a tomar decisões informadas sobre como proteger suas informações pessoais em um ambiente digital em constante evolução.

Todas essas alternativas servem para complementar ainda mais os efeitos da LGPD e do Marco Civil da Internet. Nesse contexto, cabe analisar que as normativas existentes, embora desempenhem um papel importante, não são suficientes por si só.

Diante desse panorama, surge a necessidade de adotar abordagens complementares. Além das regulamentações convencionais, é vital explorar estratégias inovadoras que possam resistir à voracidade do capitalismo de vigilância.

Uma dessas abordagens é, justamente iniciativas promovendo a educação digital, desenvolvida em colaboração com a sociedade para conscientizar a todos sobre as consequências do uso excessivo.

Essas iniciativas buscam não apenas fornecer conhecimento técnico, mas também promover uma compreensão crítica do impacto das tecnologias digitais na sociedade, incentivando uma participação informada. Além disso, a questão da acessibilidade nos termos de uso também é uma forma complementar de abordagem.

Os documentos que estabelecem as condições de utilização de plataformas digitais devem ser redigidos de forma clara e acessível, garantindo que todas as pessoas, independentemente de suas habilidades ou limitações, possam compreender e usufruir dos serviços online.

A promoção da acessibilidade nos termos de uso contribui não apenas para a inclusão, mas também para a construção de uma sociedade digital mais ética e responsável.

¹¹⁷ MARQUET, Helena Maria; DE GREGORI, Isabel Christine Silva. A educação digital como instrumento eficaz da proteção de dados pessoais. **Universidade Regional Integrada do Alto Uruguai e das Missões (URI)**, 2021. p. 169.

Da mesma forma, ao promover a acessibilidade nos termos de uso, busca-se assegurar que a proteção de dados seja acessível a todos, independentemente de suas habilidades ou condições.

Isso não apenas fortalece a inclusão digital, mas também reforça a ideia de que a proteção de dados é um direito fundamental que deve ser respeitado e preservado por toda a sociedade.

Essas abordagens buscam criar um ambiente no qual a proteção de dados não seja apenas uma obrigação legal, mas também uma parte integrante da cultura organizacional e social.

Nos capítulos anteriores destacou-se sobre a evolução dos poderes até chegar nos novos senhores do capital, conhecido como capitalismo de vigilância, conceituado por Shoshana Zuboff. A exploração intensiva dos dados pessoais alimenta um ciclo contínuo de monitoramento e influência.

Meu objetivo aqui é desacelerar a ação a fim de expandir o espaço para tal debate e desmascarar as tendências dessas novas criações, uma vez que elas aumentam a desigualdade, intensificam a hierarquia social, exacerbam a exclusão, usurpam os direitos e despem a vida pessoal daquilo que a torna pessoal para você ou para mim. Se é para o futuro digital ser o nosso lar, então cabe a nós torná-lo o nosso lar. E precisaremos saber. E precisaremos decidir. E precisaremos decidir quem decide. Essa é a nossa luta por um futuro humano.¹¹⁸

A crítica vai além das implicações sociais e aborda a invasão da esfera pessoal, ressaltando como essas tecnologias podem despojar a vida privada de sua autenticidade e singularidade, transformando-a em algo mais impessoal e suscetível a manipulações externas.

No entanto, existem outras questões que demandam abordagens culturais e políticas para serem efetivamente tratadas. No contexto da biopolítica, isso pode ser interpretado como uma extensão do controle sobre a vida cotidiana das pessoas.

A crítica mencionada anteriormente, que destaca como essas tecnologias podem despojar a vida privada de autenticidade e singularidade, alinha-se com as preocupações biopolíticas citadas ao longo deste trabalho.

¹¹⁸ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.p. 82.

A interconexão dessas informações permite não apenas o monitoramento das atividades individuais, mas também a análise preditiva de comportamentos e preferências como citadas na seção anterior.

“Diante dessa grande quantidade de dados colhidos dos indivíduos por diversos cadastros, sensores, câmeras, entre outros dispositivos tecnológicos, verifica-se uma biopolítica nunca antes imaginada”.¹¹⁹ Nesse cenário, a importância das normativas torna-se evidente, pois são essenciais para orientar o uso ético dessas informações.

Contudo, a velocidade exponencial das transformações tecnológicas muitas vezes supera a capacidade das normativas tradicionais de acompanharem tais fenômenos.

O surgimento constante de novas tecnologias e práticas de coleta de dados desafia a capacidade regulatória existente, criando um hiato entre a inovação e a adequação das normas.

A ascensão do capitalismo de vigilância, entrelaçado com a lógica do neoliberalismo, configura-se como uma intrincada racionalidade que penetra e expande-se entre as esferas do que é considerado normativo.

O neoliberalismo se impõe e se alastra como uma verdadeira racionalidade que se instala dentre aquilo que é tido como normalidade e opera conjuntamente de forma biopolítica para condicionar a totalidade do nosso modo de vida.¹²⁰

Esse fenômeno não apenas impõe uma forma específica de organização econômica, mas também opera de maneira biopolítica, influenciando e condicionando a totalidade do modo de vida.

Assim como o neoliberalismo busca consolidar sua hegemonia por meio de políticas econômicas, o capitalismo de vigilância se estabelece na coleta incessante de dados.

O deslocamento de uma instância irradiadora de poder (efetivo) do Estado – visto sob a forma usual – para uma série não precisa e centralizada de órgãos, poderes, loci circunstanciais é a tônica de um preenchimento governamental não mais estipulado política e juridicamente a partir de

¹¹⁹ SOUZA, Gabriel Scudeller de; ESTÊVÃO, Roberto da Freiria. Compliance e proteção de dados na sociedade da informação: biopoder ou biopolítica. *Scientia Iuris*, Londrina, v. 26, n. 3, p. 10-31, nov. 2022. p. 14.

¹²⁰ DIVAN, Gabriel Antinolfi. **Revolução permanente**: ensaio crítico sobre o discurso garantista e a racionalidade neoliberal. Porto Alegre: Elegancia Juris, 2020. p. 78.

posições fixas sob um parâmetro calcado em uma razão aliada ao direito e/ou a um cerne emanado constitucionalmente.¹²¹

Essa transformação não se baseia mais em posições fixas, regidas por parâmetros calcados estritamente em uma razão aliada ao direito e/ou a um cerne emanado constitucionalmente.

Em vez disso, a ênfase recai sobre uma dinâmica, na qual o exercício do poder ocorre de maneira dispersa e adaptativa, desafiando as noções tradicionais de autoridade.

A gestão política in abstracto dos indivíduos a partir da soberania (poder punitivo e, em última análise, poder de decidir sobre a vida e a morte) passa a ser cada vez mais uma gestão de sujeitos, de modo disciplinar e autodisciplinar (regras de conduta e práticas de sociabilidade introjetadas) em um primeiro momento (na modernidade tardia) e biopolítica (gestão da própria vida e a vivência tomadas literalmente, como objeto do governo – poder sobre os corpos, a vida, e não abstratamente mediado sobre indivíduos).¹²²

Este fenômeno implica um poder mais abrangente sobre os corpos e a existência, indo além da abstração e exercendo influência direta sobre a experiência individual.

Assim, a gestão disciplinar e autodisciplinar descrita inicialmente na modernidade tardia é potencializada e intensificada pelo papel central das tecnologias digitais na contemporaneidade.

A vigilância constante, agora realizada por meio de plataformas digitais e algoritmos, não apenas molda comportamentos através da internalização de regras, mas também se apropria dos dados biométricos e das escolhas pessoais, consolidando uma forma de controle.

Veja-se que a temática dos dados atinge, a partir da LGPD, o tratamento dado aos empregados, clientes e parceiros externos do ambiente corporativo, de forma que a concentração dessas informações nas mãos do capital pode favorecer a construção de uma nova cultura organizacional, permitindo-se a produção biopolítica do comum e em comum, por meio do bom tratamento de tais dados, seguindo as orientações principiológicas da Constituição, dos direitos humanos e da própria LGPD. Por outro lado, a utilização desses conteúdos de forma a excluir direitos sociais, tendo em vista o favorecimento dos interesses econômicos, pode colaborar para um programa de fachada

¹²¹ DIVAN, Gabriel Antinolfi. **Revolução permanente**: ensaio crítico sobre o discurso garantista e a racionalidade neoliberal. Porto Alegre: Elegancia Juris, 2020. p. 82.

¹²² DIVAN, Gabriel Antinolfi. **Revolução permanente**: ensaio crítico sobre o discurso garantista e a racionalidade neoliberal. Porto Alegre: Elegancia Juris, 2020. p. 88.

que não traduzirá o valor da dignidade humana e se caracterizará num biopoder centralizador e violador das garantias individuais.¹²³

Dentro do escopo da Lei Geral de Proteção de Dados, a gestão de dados não se restringe apenas à aderência às normas legais; ela envolve, aspectos éticos e culturais que moldam a abordagem das organizações em relação às informações que possuem.

Essa disparidade entre a rapidez das mudanças tecnológicas e a elaboração de normativas apropriadas suscita preocupações sobre a capacidade de proteção dos direitos fundamentais e a salvaguarda da proteção de dados na sociedade digital.

Ao transformar dados pessoais em commodities manipuláveis, há uma ameaça à autonomia individual e à própria identidade. A vida privada, em vez de ser um espaço íntimo e autêntico, pode ser moldada por algoritmos e interesses externos, comprometendo a liberdade e a diversidade de experiências.

A disseminação de informações aos níveis superiores da hierarquia destaca como esses dados, muitas vezes coletados de maneira indiscriminada, podem ser utilizados para influenciar decisões em escalas amplas, reforçando a dinâmica de poder característica do capitalismo de vigilância.

Com a disseminação da peste pela Europa, surgiu um mecanismo de controle, uma espécie de máquina de informações, onde os dados ficaram expostos e susceptíveis a manipulações.

Essas técnicas que misturam ou combinam biopolítica e gestão de dados são antigas e, na realidade, indispensáveis uma à outra. A questão do exemplo que Foucault traz sobre a organização de dados relacionados aos infectados pela peste na Europa medieval estabelece um paralelo com as preocupações relativas a eventos contemporâneos que simulam a mesma oportunidade dessa junção, como a situação da pandemia da COVID-19 e as relações de perfilizações já demonstradas. Nessa linha de pensamento:

Um verdadeiro organograma informativo lastreado nessa possibilidade de aquisição totalizante de dados era transmitido em escalas aos intendentess e superiores políticos, que tinham em mãos, na estratégia eficiente de controle epidêmico, embutida também a possibilidade de um grau de gerência e conhecimento não propiciado por qualquer tipo de pacto ou acordo usual. Havia uma fragmentação administrativa lógica, ainda que o compartilhamento

¹²³ SOUZA, Gabriel Scudeller de; ESTÊVÃO, Roberto da Freiria. Compliance e proteção de dados na sociedade da informação: biopoder ou biopolítica. *Scientia Iuris*, Londrina, v. 26, n. 3, p. 10-31, nov. 2022. p. 12-13.

informativa por vezes se apresentasse como fluxos de coesão que se auto articulam e se auto compõem como uma corporificação indistinta. A esquemática não se exhibia enquanto ideia ou possibilidade de trato – dentre tantas. Apresentava-se tal estratégia não apenas possível, como irremediável. É uma figuração grandiosa de como o poder pode se acoplar a uma dinâmica situacional para soar não enquanto técnica imposta, mas enquanto resquício óbvio de algo naturalizado.¹²⁴

Na dinâmica do “Capitalismo de Vigilância”, as interações sociais se tornam parte de um jogo sofisticado, onde as empresas e entidades detentoras do poder empregam estratégias de coleta de dados para moldar comportamentos e influenciar decisões.

O usuário fornece “livremente” os seus dados pessoais na expectativa de receber gratuitamente serviços personalizados. Os serviços desse capitalismo digital aparentemente cumprem tal promessa ao se moldarem à cada usuário, contudo, ocultam a relação econômica que os mantém, isto é, a publicidade, condicionamento do comportamento humano e sobretudo produção de dados promovida pela expropriação e alienação de informações pessoais. Essa técnica de poder pouco é afetada por regimes jurídicos, e não pode ser desativada simplesmente por regulação ou mais acesso a informações em termos e condições dos serviços. Ela explora justamente o projeto de liberdade que se abriga no âmago do ímpeto neoliberal. A limitação do Estado ambicionada pelos liberais clássicos converteu-se em uma nova forma de submissão, muito mais eficiente e indiscernível.¹²⁵

Os usuários fornecem voluntariamente seus dados pessoais na expectativa de receber serviços personalizados sem custo aparente.

Embora esses serviços pareçam cumprir a promessa ao adaptarem-se a cada usuário, há uma complexidade oculta que permeia essa interação. A relação econômica, envolvendo publicidade, manipulação do comportamento humano e a coleta de dados através da expropriação e alienação de informações pessoais, permanece muitas vezes despercebida pelos usuários.

A notável resistência dessas práticas às regulamentações jurídicas destaca uma questão crítica: a ameaça opera em bases que escapam ao alcance da proteção

¹²⁴ LUZ, A. F.; CHINI, M. ; DIVAN, G. A. Poder, Discurso Científico e Biopolítica: leitura inicial da perspectiva de calamidades globais sob o conceito de onicrise. *In.*: PILAU SOBRINHO, L. L.; CALGARO, C.; ROCHA, L. S.(Org.). COVID-19: democracia e poder. 1ed. Itajaí/SC: Univali, 2020, v. I, p. 96.

¹²⁵ SALLES, Eduardo BC; AMARAL, Augusto Jobim. Máquinas de subjetivação, capitalismo de vigilância e algoritmos: uma aproximação desde o caso brasileiro. *In.*: **III Congresso Internacional Move. net sobre Movimientos Sociales y TIC (2020)**, pp. 9-18. Grupo Interdisciplinario de Estudios en Comunicación, Política y Cambio Social de la Universidad de Sevilla (COMPOLÍTICAS), 2020. p. 14.

legal, desafiando as tentativas de controle por meio de regulamentações ou do aumento do acesso a informações nos termos e condições dos serviços.

Essa técnica de poder, ao explorar o anseio pela liberdade no cerne do ímpeto neoliberal, transformasse a aspiração de limitar o papel do Estado, conforme preconizado pelos liberais clássicos, em uma forma mais eficiente e indiscernível de submissão.

A dicotomia entre a busca pela liberdade individual e as armadilhas do neoliberalismo digital revela um desafio. A limitação do Estado, inicialmente concebida para proteger a autonomia do indivíduo, torna-se uma vulnerabilidade explorada por estruturas digitais, que desafiam as noções tradicionais de soberania e jurisdição.

Se quer ir a um restaurante em Paris, veja as avaliações quantificadas e obtenha os dados de qualidade do restaurante. Se quer contratar tal funcionário, investigue seus deslocamentos, seus perfis em redes sociais, as imagens e textos por ele veiculadas que constituem dados de si mesmo. Se quer apurar fatos políticos, acione sistemas de delação e faça da sanção uma estratégia para alcance de novos dados criminais. Em todos os casos, o que está em jogo é um mundo para fora, para o exterior, para a exposição, desnudo, aberto, transparente, sem proteção, sem sombra, sem lado de dentro.¹²⁶

No contexto do capitalismo de vigilância, essa manipulação psicológica é utilizada para incentivar os indivíduos a compartilhar cada vez mais informações pessoais em troca de conveniência ou status social.

No âmbito do neoliberalismo, há uma ênfase na maximização do mercado livre e na minimização da intervenção estatal na economia. Isso se traduz em uma cultura que valoriza a competitividade, a individualidade e a busca incessante pelo sucesso material.

Algoritmos são projetados para personalizar o conteúdo com base nas preferências e no comportamento passado do usuário, criando uma bolha de filtro que reforça determinadas visões de mundo e limita a exposição a perspectivas alternativas. Isso pode ter o efeito de reforçar preconceitos, polarizar opiniões e criar divisões na sociedade.

Nesse contexto, a quantificação e a mercantilização de várias esferas da vida social são comuns, como exemplificado na citação anterior. Assim, o Big Data decreta

¹²⁶ BENEVIDES, Pablo Severiano. Neoliberalismo, Psicopolítica e Capitalismo da transparência. **Psicologia & Sociedade**, v. 29, 2018, p. 8.

o fim da vontade livre, da privacidade, do segredo e da autonomia. É uma máquina de transparência que oculta suas próprias regras.¹²⁷

A adaptação dos instrumentos regulatórios tradicionais é imperativa diante desse desafio em constante evolução.

O futuro é nebuloso, se não houver uma guinada no processo de conhecimento do fenômeno e das maneiras de lidar com o ferramental adequado. Tudo passa pela educação digital. Apesar de ser uma solução com eficácia a longo prazo, se faz necessária para a emancipação dos usuários no meio digital, promovendo mais segurança, conscientização e liberdade.¹²⁸

Essa naturalização é uma característica comum do capitalismo de vigilância, onde a coleta e análise de dados tornaram-se parte integrante das operações cotidianas.

Nesse sentido, essa prática, muitas vezes conduzida de forma discreta, transcende as fronteiras tradicionais entre o público e o privado, criando uma lógica imanente que sustenta as operações desse sistema.

O descortinar puro e simples das parafuncionalidades dinâmicas e das formas de jogar o “jogo” ainda obedece a uma lógica imanente que pode ser transcendida quando da análise política e desses fatores de estrutura: há outros “jogos” e outros conjuntos de regras simul-tâneas e consubstanciadas.¹²⁹

Ao examinar os fatores políticos e estruturais associados a esse sistema, torna-se possível ir além das aparências e compreender as influências que moldam as regras do jogo e as dinâmicas sociais envolvidas.

A coleta massiva de dados, a vigilância constante e a manipulação de informações pessoais podem ser vistas como mecanismos que vão além dos limites da esfera jurídica, atuando na regulação e controle dos corpos e das vidas individuais em níveis mais profundos.

¹²⁷ BENEVIDES, Pablo Severiano. Neoliberalismo, Psicopolítica e Capitalismo da transparência. **Psicologia & Sociedade**, v. 29, 2018, p. 8.

¹²⁸ LEITE SAMPAIO, José Adércio; FURBINO, Meire; ASSIS BOCCHINO, Lavínia. Capitalismo de vigilância e tecnopolítica: os direitos fundamentais de privacidade e liberdade de expressão sob ataque. **Opinião Jurídica**, v. 20, n. 42, 2021, p. 525.

¹²⁹ DIVAN, Gabriel Antinolfi. Revolução permanente: ensaio crítico sobre o discurso garantista e a racionalidade neoliberal. **Porto Alegre: Elegancia Juris**, 2020, p.103.

O direito tem limitações em seu controle e proteção abrangentes, não abarcando todas as dimensões da sociedade. “O Direito se fragiliza enquanto limite que deveria impor, e passa também a ser veículo para o poder”.¹³⁰

Sua capacidade de tutelar está diretamente ligada à sua legalização, regulamentando aquilo que está dentro de sua esfera de competência. O equilíbrio entre a utilização ética dos dados e a prevenção dos incidentes dessas informações torna-se crucial.

Exemplo disso, é que recentemente, foi divulgado pelo Google um alerta preocupante sobre as potenciais ameaças à privacidade que se avizinham para o ano de 2024. A empresa identificou uma variedade de estratégias adotadas por cibercriminosos para tirar proveito das brechas nas regulamentações de privacidade, visando assim a coleta ilícita de dados pessoais.

A principal preocupação do Google é com o aumento do uso de “malware de espionagem”. Esse tipo de malware é projetado para se infiltrar em dispositivos e roubar dados confidenciais, como senhas, informações bancárias e até mesmo conversas privadas. Os cibercriminosos estão usando uma variedade de métodos para distribuir esse malware, incluindo: E-mails de phishing: E-mails que parecem ser de empresas legítimas, mas que na verdade são links maliciosos. Anúncios fraudulentos: Anúncios online que direcionam os usuários para sites infectados com malware. Aplicativos infectados: Aplicativos baixados de fontes não confiáveis que contêm malware.¹³¹

Esse anúncio evidencia ainda mais a crescente sofisticação e audácia dos ataques cibernéticos, revelando uma urgente necessidade de medidas adicionais para proteger a privacidade dos usuários online.

Mais uma vez, a suposta regulamentação, longe de assegurar proteções sólidas, é colocada em xeque, sua aplicação pode ser insuficiente ou até mesmo comprometida.

Nos Estados Unidos, a maioria dos aplicativos de saúde e de condicionamento físico não está sujeita às leis de privacidade da área de

¹³⁰ LUZ, A. F.; CHINI, M.; DIVAN, G. A. Poder, Discurso Científico e Biopolítica: leitura inicial da perspectiva de calamidades globais sob o conceito de onicrise. In: PILAU SOBRINHO, L. L.; CALGARO, C.; ROCHA, L. S. (Org.). COVID-19: democracia e poder. 1ed. Itajaí/SC: Univali, 2020, v. I, p. 99.

¹³¹ WINDER, Davey. Aviso do Google revela ameaça global à privacidade em 2024: você está em risco. **Forbes Tech**, São Paulo, 12 fev. 2024. Disponível em: <https://forbes.com.br/forbes-tech/2024/02/aviso-do-google-revela-ameaca-global-a-privacidade-em-2024-voce-esta-em-risco/#:~:text=Em%20um%20comunicado%20recente%2C%20o,dados%20pessoais%20de%20forma%20ilegal.Acesso em: 25 fev. 2024.>

saúde, e as leis que de fato existem não levam em conta da forma adequada nem as capacidades do universo digital nem a ferocidade das operações capitalistas de vigilância.¹³²

A análise crítica avança ao considerar as garantias fundamentais como barreiras intencionais, sugerindo que, em vez de funcionarem como salvaguardas inquestionáveis, são desenhadas de maneira a se tornarem suscetíveis a influências externas.

Nesse contexto, a fragilidade dessas garantias é particularmente evidente na era do capitalismo de vigilância, onde práticas massivas de coleta de dados e monitoramento contínuo ameaçam minar os princípios fundamentais do direito.

A visão apresentada vai além, questionando a suposta supremacia do direito na estrutura social. Longe de ser o ápice da ordem, as garantias legais são percebidas como fracas diante das forças do capitalismo de vigilância, que moldam e desafiam a eficácia dessas proteções.

Na busca por eficácia na proteção de dados no atual cenário do capitalismo, torna-se cada vez mais evidente a necessidade de abordagens complementares à regulamentação. A complexidade das práticas de coleta de dados exige estratégias que ultrapassem as fronteiras normativas, incorporando elementos como educação digital e acessibilidade nos termos de uso.

A educação digital é uma das ferramentas de prevenção. Capacitar os indivíduos para compreenderem as implicações de suas interações online e as práticas de coleta de dados é fundamental.

Isso envolve não apenas conscientização sobre os riscos, mas também o desenvolvimento de habilidades para uma participação informada na sociedade digital. Programas educacionais abrangentes podem cultivar uma cultura de responsabilidade digital, capacitando as pessoas a tomarem decisões conscientes em relação à sua privacidade.

Além disso, a acessibilidade nos termos de uso é uma peça essencial do quebra-cabeça. Muitos usuários enfrentam desafios na compreensão das políticas complexas de privacidade e termos de serviço.

¹³² ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021. p. 299.

Tornar esses documentos mais acessíveis, utilizando linguagem clara e estrutura compreensível, é crucial. Isso promove a transparência e garante que os usuários possam fazer escolhas informadas sobre o compartilhamento de seus dados.

Essas abordagens, quando integradas à regulamentação, oferecem uma defesa abrangente contra o capitalismo de vigilância. A educação digital capacita os indivíduos a serem agentes ativos na proteção de sua privacidade, enquanto a acessibilidade nos termos de uso garante que a informação seja acessível a todos, independentemente do nível de familiaridade com termos técnicos.

Em conjunto, essas estratégias buscam remodelar o paradigma atual, onde a proteção de dados não é apenas imposta por normativas, mas internalizada como parte fundamental da cultura digital.

Afinal, “nada se resolverá sem que haja uma reeducação para o mundo digital. Certo, pode não ser um beco sem saída, mas há ainda um horizonte de incertezas pela frente. Os direitos estão em risco”.¹³³

¹³³ LEITE SAMPAIO, José Adércio; FURBINO, Meire; ASSIS BOCCHINO, Lavínia. Capitalismo de vigilância e tecnopolítica: os direitos fundamentais de privacidade e liberdade de expressão sob ataque. *Opinión Jurídica*, v. 20, n. 42, 2021, p. 524.

CONSIDERAÇÕES FINAIS

Os avanços tecnológicos, juntamente com as ameaças que deles surgem, são resultados inevitáveis da evolução. Diante desse cenário em constante transformação, é incumbência da sociedade e do sistema jurídico acompanhar essas mudanças de forma a preservar a dignidade da pessoa humana.

Essa perspectiva reconhece que o progresso tecnológico é uma força motriz intrínseca ao desenvolvimento humano. No entanto, também ressalta a necessidade de uma resposta ativa por parte da sociedade e do sistema legal para mitigar os riscos e impactos negativos que podem surgir dessas inovações.

Ao reconhecer a importância de se adaptar a essas mudanças, a sociedade assume um papel proativo na proteção dos valores fundamentais, como a dignidade da pessoa humana.

A visão do capitalismo de vigilância, relacionado por Shoshana Zuboff, aponta o Google como o principal fenômeno que eclodiu com a conceituação. Sua análise examina como as práticas de coleta e análise de dados pelas grandes corporações moldaram não apenas o mercado digital, mas também as dinâmicas sociais e políticas.

O capitalismo de vigilância, embora se apresente como uma forma de poder aparentemente distinta, está ligado às estruturas do capitalismo tradicional. Nesse contexto, a proteção jurídica assume um papel importante na mitigação dos potenciais abusos e na garantia dos direitos individuais dos cidadãos.

No entanto, as estruturas legais e regulatórias existentes não estão preparadas para lidar com os desafios específicos apresentados por essas novas dinâmicas. A rápida evolução da tecnologia e a proliferação de dados pessoais criaram lacunas significativas na proteção jurídica, deixando os cidadãos vulneráveis a violações de privacidade, discriminação algorítmica e manipulação de informações.

A ineficácia jurídica frente às dimensões de poder, particularmente diante do capitalismo de vigilância, é uma preocupação crescente na contemporaneidade. Enquanto o capitalismo de vigilância se expande e se torna cada vez mais intrusivo nas vidas das pessoas, o sistema jurídico se mostra frágil para lidar com os desafios que ele apresenta.

Investir na educação digital não apenas capacita os indivíduos a protegerem sua própria privacidade, mas também os torna mais conscientes dos impactos sociais e políticos do capitalismo de vigilância. Ao promover a alfabetização digital, os indivíduos se tornam participantes ativos no debate sobre as políticas de proteção de dados e influenciar positivamente a formulação de leis e regulamentos mais eficazes.

Além da importância das leis e regulamentos específicos, é fundamental reconhecer que a eficácia da proteção de dados na administração pública e nas instituições privadas vai além da simples conformidade legal.

A capacitação adequada dos operadores do sistema é importante para garantir a implementação efetiva das políticas de proteção de dados. Essa capacitação não apenas envolve o conhecimento das leis e regulamentos de proteção de dados, mas também a compreensão dos princípios fundamentais de segurança da informação e privacidade.

Os *hackerspaces*, ou espaços colaborativos de tecnologia e inovação, representam exemplos concretos de como a educação digital pode ser eficaz na capacitação dos indivíduos e na promoção de uma participação ativa na sociedade. No Brasil, esses espaços têm desempenhado um papel importante na democratização do acesso ao conhecimento tecnológico.

Por meio de *workshops*, palestras e outras atividades educativas, esses espaços capacitam os participantes a entenderem melhor os desafios apresentados pelo capitalismo de vigilância e a tomarem medidas para protegerem seus dados.

Ao mesmo tempo, os *hackerspaces* também servem como centros de engajamento cívico, onde os participantes podem se envolver ativamente no debate público sobre políticas de proteção de dados e influenciar positivamente a formulação de leis e regulamentos mais eficazes.

Os espaços colaborativos desempenham um papel vital na promoção da alfabetização digital e na proteção de dados, capacitando os indivíduos a participar ativamente da sociedade digital e a contribuir para um ambiente seguro. Investir nesses espaços e promover sua participação é fundamental para construir uma sociedade digital mais equitativa e inclusiva.

Ao entender melhor como seus dados são coletados, armazenados e utilizados, os usuários podem tomar decisões mais informadas sobre quais plataformas e serviços digitais optam por utilizar, exercendo assim uma forma de poder de escolha em relação ao capitalismo de vigilância.

Nesse sentido, o direito precisa lutar pelo seu papel político. Essa luta deve ser realizada com prudência e realismo, evitando a utopia de acreditar que o Direito tem poder absoluto onde, na verdade, não o possui.

Os dados pessoais são a essência que alimenta esse sistema, e as consequências vão além do âmbito econômico, penetrando em aspectos fundamentais da existência, moldando percepções, decisões e até mesmo relações sociais.

A proteção dos dados pessoais não é apenas uma questão técnica ou jurídica, mas uma questão essencial para a preservação da autonomia, dignidade e liberdade individuais na era digital.

Existe um complexo sistema de poder, não exatamente paralelo, mas operando em uma esfera não política, conhecido como biopolítica, que não age de forma oculta, mas sim em harmonia com os sistemas de poder legitimados e visíveis.

Este fenômeno é fundamental no contexto do capitalismo contemporâneo - e ao mencionar o capitalismo, não se refere apenas a um sistema econômico isolado, mas sim ao modo como as formas sociais são constituídas e como a subjetividade é produzida.

A entrada em vigor da LGPD ocorre em meio a uma intensa discussão, uma vez que os dados desempenham um papel fundamental no que é considerado o novo capital. Proteger dados não deve ser apenas encarado como uma questão de troca, venda e distribuição de dados, o impacto vai além desses aspectos diretos.

Além disso, ao considerar a psicopolítica de Han, que destaca como os indivíduos são influenciados e manipulados psicologicamente pelos dispositivos digitais, torna-se evidente que a principal moeda nesse momento de algoritimização é a vida.

Em suas considerações finais, Shoshana Zuboff conclui que o tempo dirá como os indivíduos lidarão com esse fenômeno para reivindicar um futuro digital. Além disso, menciona que as normativas devem ser pensadas levando em consideração os usuários, que estão em uma condição vulnerável em relação ao sistema.

A pergunta que permanece é: como esses indivíduos serão inseridos no sistema? O trabalho identificou que é possível realizar essa inserção através de reivindicações, educação digital e capacitação. A resposta aponta para o fato de que apenas as normativas não serão suficientes para conter os avanços do capitalismo de vigilância.

Essa forma do capitalismo está no topo da pirâmide, tornando o direito uma barreira frágil diante desse grande fenômeno. Para conter suas consequências devastadoras, os usuários precisam se tornar os protagonistas, principalmente com seu próprio consentimento, bem como legisla a LGPD.

Apenas mencionar que os indivíduos são vulneráveis a esse sistema, como narrado por Zuboff, não contribui para a solução do problema. É necessário que os usuários saibam como prevenir incidentes envolvendo os dados pessoais, e isso só será possível quando entenderem o que é proteção de dados.

O capitalismo de vigilância é uma vertente do sistema econômico que escapa à regulamentação legal, atuando em uma posição avançada, além das barreiras convencionais: lida com um volume sem precedentes de dados privilegiados disponíveis na história da indústria e, sobretudo, permeia - ou até mesmo molda - a subjetividade.

A vulnerabilidade dos mais vulneráveis, aqui, não é só a mesma de um consumidor que é enganado ou de alguém que tem direito a ter “segredos” privados e está sofrendo investidas de acesso. É uma vulnerabilidade que - ao mesmo e irônico tempo - expõe o “capitalismo de vigilância”: expõe onde ele está, o quão ele está próximo, porque expõe onde ele já chegou.

É essa vulnerabilidade que deixa a ferida do direito aberta: ele protege os indivíduos em relação a uma disputa onde o outro lado precisa jogar limpo e dentro dos parâmetros. O sistema jurídico deve evoluir para abordar questões éticas e legais emergentes, garantindo que os princípios fundamentais não se percam no avanço tecnológico desenfreado.

Nesse contexto, a relação entre o capitalismo de vigilância e a proteção jurídica não se limita apenas à implementação de regulamentações. Ela também abarca a promoção da educação digital e a conscientização sobre questões de privacidade e segurança online.

Esse conjunto se resume em práticas de resistências ao capitalismo de vigilância, pois propõe estratégias que limitam a exploração indiscriminada de dados pessoais para fins comerciais.

Ao priorizar a proteção da privacidade, essas práticas contribuem para frear o avanço do capitalismo de vigilância, fortalecendo o controle dos cidadãos sobre seus dados.

Portanto, estas abordagens complementares as legislações, principalmente a Lei Geral de Proteção de Dados, são fundamentais para lidar com os dilemas que surgem em decorrência do capitalismo de vigilância.

REFERÊNCIAS

- ABÍLIO, Ludmila Costhek; AMORIM, Henrique; GROHMANN, Rafael. Uberização e plataformização do trabalho no Brasil: conceitos, processos e formas. *Sociologias*, v. 23, p. 26-56, 2021.
- ARAUJO, Wecio Pinheiro. Marx e a indústria 4.0: trabalho, tecnologia e valor na era digital. *Revista Katálysis*, v. 25, p. 22-32, 2022.
- BRANCO, Pedro Mendonça Castelo; DA SILVA, Sidney Jard. Uberização: as quatro facetas do controle. *Revista Tecnologia e Sociedade*, v. 19, n. 56, 2023.
- BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28 out. 2022.
- BRASIL. **Código Penal**. Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 out. 2022.
- BRASIL. Serviço Federal de Processamento de Dados. **Princípios LGPD**. Brasília, DF, 2020. Disponível em: <https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd>. Acesso em: 08 set. 2022.
- BRASIL. Serviço Federal de Processamento de Dados. **O que são dados pessoais, segundo a lgpd**. Brasília, DF, 2020. Site. Disponível em: <https://www.serpro.gov.br/lgpd/>. Acesso em: 08 set. 2022.
- BRASIL. Serviço Federal de Processamento de Dados. **Guia de Boas Práticas da Lei Geral de Proteção de Dados**. Brasília, DF, 2020. Site. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>. Acesso em: 10 out. 2022.
- BRANCO, Pedro Mendonça Castelo; DA SILVA, Sidney Jard. Uberização: as quatro facetas do controle. *Revista Tecnologia e Sociedade*, v. 19, n. 56, p. 303-318, 2023.
- BENEVIDES, Pablo Severiano. Neoliberalismo, Psicopolítica e Capitalismo da transparência. *Psicologia & Sociedade*, v. 29, 2018.
- BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. Rio de Janeiro: Grupo GEN, 2019. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530983291/>. Acesso em: 06 out. 2022.
- BOLZAN DE MORAIS, José Luis; JACOB NETO, Elias; ALVES, Fabrício G.; GOMES, Igor da Silva. **Accountability, transparência e assimetria das relações de visibilidade virtuais**: análise dos aspectos antidemocráticos das novas tecnologias da informação e comunicação a partir da ideia de filtro bolha. In:

Direito, Estado e Sociedade, n. 53, 2018.

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência (Florianópolis)**, Florianópolis, n. 68, p. 109-127, jun 2014. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S217770552014000100006&lng=en&nrm=iso. Acesso em 18 out. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018.p. 13.

Câmara dos Deputados. **Promulgada PEC que inclui a proteção de dados pessoais entre direitos fundamentais do cidadão**. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/noticias/850028-promulgada-pec-que-inclui-a-protecao-de-dados-pessoais-entre-direitos-fundamentais-do-cidadao/>. Acesso em: 02 jan. 2023.

Câmara dos Deputados. **Lula sanciona com vetos lei que cria a Política Nacional de Educação Digital**. Disponível em: Lula sanciona com vetos lei que cria a Política Nacional de Educação Digital - Notícias - Portal da Câmara dos Deputados (camara.leg.br). Acesso em: 02 jan. 2023.

CANUTO, L. C. **Câmara inaugura Laboratório Hacker nesta quarta-feira**. Câmara Notícias, 18 fev. 2014. Disponível em: Acesso em: 03 out. 2023.

CASTELLS, Manuel. **O poder da identidade: A era da informação economia, sociedade e cultura**. V. 2. 6. ed. São Paulo: Paz e Terra, 2008.

CASTELLS, Manuel. **Fim de milênio: a era da informação: economia, sociedade e cultura**. Trad. Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 1999. v.3.p.46.

DE OLIVEIRA FORNASIER, Mateus; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista Direito em Debate**, v. 29, n. 53, p. 189, 2020.

DIVAN, Gabriel Antinolfi. **Revolução permanente: ensaio crítico sobre o discurso garantista e a racionalidade neoliberal**. Porto Alegre: **Elegantia Juris**, 2020.

DONEDA, Danilo. **Privacidade e Proteção de Dados Pessoais**. Brasília, Ministério da Transparência, Fiscalização e Controladoria Geral da União, 2017. Disponível em: <https://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2017/5-anos-da-lei-de-acesso/arquivos/mesa-3-danilo-doneda.pdf>. Acesso em: 23 out. 2022.

DONEDA, Danilo Cesar. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade**. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm#_ftn1.

Acesso em: 23 out. 2022.

DONEDA, Danilo Cesar Maganhoto *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar-Revista de Ciências Jurídicas**, v. 23, n. 4, p. 1-17, 2018.

DONEDA, Danilo. Privacidade e transparência no acesso à informação pública. *In.*: MEZZARROBA, Orides; GALINDO, Fernando. **Democracia eletrônica**. Zaragoza: Prensas Universitarias de Zaragoza, 2010.

FARIAS, Camila Cavalcante *et al.* **Que vírus é esse?** Reflexos da cultura hacker na vida política brasileira. 2022.

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 Práxis**, v. 12, p. 1002-1033, 2021.

FRAZÃO, Ana. **O alcance da LGPD e repercussões para a atividade empresarial**, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-alcance-da-lgpd-e-repercussoes-para-a-atividade-empresarial-05092018>. Acesso em: 27 ago.2022.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 1 ed. São Paulo: Thomson Reuters Brasil, 2019. Kindle ebook.

GARCEZ, R. M. **Plataformas digitais e uberização do trabalho: Uma distopia no capitalismo contemporâneo**. Disponível em http://www.joinpp.ufma.br/jornadas/joinpp2021/images/trabalhos/trabalho_submissa_old_850_850612c1fa375549.pdf. Acesso em: 05 nov. 2023.

FOUCAULT, Michel. **Microfísica do Poder**. Organização e tradução de Roberto Machado. 18 ed. Rio de Janeiro: Edições Graal, 1979.

GONCALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Rev. direito GV**, São Paulo, v. 14, n. 2, p. 20, ago 2018.

Disponível em:

http://www.scielo.br/scielo.php?script=sci_arttext&pid=S180824322018000200513&lng=pt&nrm=iso. Acesso em: 28 nov. 2022.

LEITE SAMPAIO, José Adércio; FURBINO, Meire; ASSIS BOCCHINO, Lavínia. Capitalismo de vigilância e tecnopolítica: os direitos fundamentais de privacidade e liberdade de expressão sob ataque. **Opinião Jurídica**, v. 20, n. 42, 2021.

LEMES, Delwin. Lei Geral de Proteção De Dados Pessoais (LGPD): O setor público e vazamentos de dados pessoais. **revista eixo**, v. 12, n. 2, p. 109-118, 2023.

LÉVY, Pierre. **O que é o virtual?**. Editora 34, 2011.

LIMA, Cintia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 28 nov. 2022

LUZ, A. F. ; CHINI, M. ; DIVAN, G. A. . Poder, Discurso Científico e Biopolítica: leitura inicial da perspectiva de calamidades globais sob o conceito de onicrise. In: PILAU SOBRINHO, L. L.; CALGARO, C.; ROCHA, L. S.. (Org.). COVID-19: democracia e poder. 1ed.Itajaí/SC: Univali, 2020, v. I, p. 94-113.

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

HAN, Byung-Chul. **O que é poder?**. Tradução Lucas Machado. Petrópolis: Vozes, 2018.

HAN, Byung-Chul. Psicopolítica: **O neoliberalismo e as novas técnicas de poder**. Tradução de Maurício Liesen. Belo Horizonte, MG: Âyiné, 2018b.

MACHADO, Joana de Moraes Souza. **A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil**. Porto Alegre, RS: Editora Fi, 2018. Ebook. Disponível em: <https://www.editorafi.org/494joana>. Acesso em: 28 nov. 2022.

MARQUET, Helena Maria; DE GREGORI, Isabel Christine Silva. A EDUCAÇÃO DIGITAL COMO INSTRUMENTO EFICAZ DA PROTEÇÃO DE DADOS PESSOAIS. **Universidade Regional Integrada do Alto Uruguai e das Missões (URI)**, 2021.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Revista Eletrônica Direito e Sociedade-REDES**, v. 7, n. 3, p. 136, 2019.

MARX, Karl. **O Capital: Crítica da Economia Política: Livro I: O Processo de Produção do Capital**. Tradução de Rubens Enderle. 2. ed. São Paulo, SP: Boitempo, 2017.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**, São Paulo, v. 130, jul./ago. 2020.

NASCIMENTO, Valéria Ribas do. Direitos fundamentais da personalidade na era da sociedade da informação: transversalidade da tutela à privacidade. **Revista de Informação Legislativa**, Brasília, v. 54, n. 213, p. 265-288, jan./mar. 2017. Disponível em: http://www12.senado.leg.br/ril/edicoes/54/213/ril_v54_n213_p265. Acesso em: 20 jan. 2023.

NETO, Leon Farhi. Biopolítica como tecnologia de poder. **INTERthesis: Revista Internacional Interdisciplinar**, v. 5, n. 1, 2008.

PARRA, Henrique et al. Infraestruturas, economia e política informacional: o caso do Google Suite for Education. **Mediações-Revista de Ciências Sociais**, p. 63-99, 2018.

PETERS, Michael. **Financeirização, o ácido que corrói a democracia**. IHU On-Line, v. 472, n. 15, p. 26-32, set. 2015.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

ROSA, Nelson Sanchez; DORNELES, Lucio Faccio. Capitalismo de vigilância e dignidade humana: tecnologia, dados e exclusão na sociedade do século XXI. **LexCult: revista eletrônica de direito e humanidades**, v. 7, n. 3, 2023.

RUARO, R.; MAÑAS, J.; MOLINARO, C. **Privacidade e Proteção de Dados Pessoais na Sociedade Digital**. Editora FI, 2017.

RUIZ, Castor M. M. Bartolomé. **Os labirintos do poder**: O poder (do) simbólico e os modos de subjetivação. Porto Alegre: Ed. Escritos, 2004.

SALLES, Eduardo BC; AMARAL, Augusto Jobim. Máquinas de subjetivação, capitalismo de vigilância e algoritmos: uma aproximação desde o caso brasileiro. *In.*: **III Congresso Internacional Move. net sobre Movimientos Sociales y TIC (2020)**, pp. 9-18. Grupo Interdisciplinario de Estudios en Comunicación, Política y Cambio Social de la Universidad de Sevilla (COMPOLÍTICAS), 2020.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018)**. Trabalho de Conclusão de Curso (Graduação em Direito). Centro Universitário de Brasília, Brasília, 2019. p. 20. Disponível em: < <https://repositorio.uniceub.br/jspui/handle/prefix/13802> > Acesso em: 04 out 2023.

SARLET, Ingo Wolfgang (org.). **Dimensões da dignidade**: ensaios de filosofia do direito e direito constitucional. 2. ed. rev. e ampl. - Porto Alegre: Livraria do Advogado Editora, 2005.

SOUZA, Gabriel Scudeller de; ESTÊVÃO, Roberto da Freiria. Compliance e proteção de dados na sociedade da informação: biopoder ou biopolítica. **Scientia Iuris**, Londrina, v. 26, n. 3, p. 10-31, nov. 2022.

SCOFIELD JR, Gilberto. Extração secreta de dados, lucro e manipulação: A lógica econômica do capitalismo de vigilância. **Revista Eco-Pós**, v. 26, n. 01, 2023.

SZINVELSKI, Martín Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. **Perspectivas em Ciência da Informação**, v. 24, p. 132-144, 2020.

ZANETTI, Dalton; DE OLIVEIRA, Ana Paula; LIMA, Flávio Santos. A Lei Geral de Proteção de Dados Brasileira na Prática Empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR** / Ordem dos Advogados do Brasil. Seção do Paraná; Escola Superior de Advocacia; Curitiba, PR, v.4, n.1, p. 177, mai. 2019. Disponível em: <http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-9.pdf#page=172>. Acesso em: 28 nov. 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.

UNICEF. **Declaração Universal Dos Direitos Humanos**. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 11 jan. 2024.

WINDER, Davey. Aviso do Google revela ameaça global à privacidade em 2024: você está em risco. **Forbes Tech**, São Paulo, 12 fev. 2024. Disponível em: <https://forbes.com.br/forbes-tech/2024/02/aviso-do-google-revela-ameaca-global-a-privacidade-em-2024-voce-esta-em-risco/#:~:text=Em%20um%20comunicado%20recente%2C%20o,dados%20pessoais%20de%20forma%20ilegal>. Acesso em: 25 fev. 2024.