

FACULDADE DE TECNOLOGIA DE SÃO PAULO

PEDRO HENRIQUE FRANCISCO SILVA

**DOS RASTROS DIGITAIS AO PODER DE INFLUÊNCIA: O VAZAMENTO DE DADOS
E A MANIPULAÇÃO DE COMPORTAMENTOS NAS REDES SOCIAIS**

SÃO PAULO
2025

FACULDADE DE TECNOLOGIA DE SÃO PAULO

PEDRO HENRIQUE FRANCISCO SILVA

**DOS RASTROS DIGITAIS AO PODER DE INFLUÊNCIA: O VAZAMENTO DE
DADOS E A MANIPULAÇÃO DE COMPORTAMENTOS NAS REDES SOCIAIS**

Trabalho submetido como exigência
parcial para a obtenção do Grau de
Tecnólogo em Análise e
Desenvolvimento de Sistemas
Orientador: Profº Marcelo Aoki

SÃO PAULO
2025

AGRADECIMENTOS

Primeiramente, agradeço a mim mesmo pelo esforço e apoio emocional nos 4 anos de faculdade e por ter conseguido chegar no fim dessa história.

A todos os funcionários da FATEC-SP.

E, principalmente, ao professor e orientador Marcelo Aoki, por todo apoio durante o desenvolvimento desse trabalho e durante o curso.

RESUMO

SILVA, Pedro Henrique Francisco. Dos Rastros ao Poder de Influência: O Vazamento de Dados e a Manipulação de Comportamentos nas Redes Sociais. 2025. 46 f. Graduação. Tecnologia em Análise e Desenvolvimento de Sistemas. Faculdade de Tecnologia de São Paulo. FATEC-SP. São Paulo, 2025.

Esta monografia tem como objetivo abordar como os rastros digitais gerados em redes sociais de compartilhamento de conteúdo são utilizados por sistemas algorítmicos, com foco nos algoritmos de recomendação, em práticas que podem comprometer a privacidade dos usuários. A pesquisa parte de uma abordagem bibliográfica e exploratória para investigar os impactos da coleta invisível de dados, analisando os termos de uso das plataformas e a compreensão limitada por parte dos usuários. Também são considerados aspectos relacionados à vigilância digital e à manipulação comportamental. A investigação propõe refletir sobre os desafios legais e sociais quanto à proteção dos dados e à transparência no uso das informações coletadas.

Palavras-chave: Rastros digitais; Dados; Privacidade; Redes sociais; Algoritmos de recomendação; Termos de uso.

ABSTRACT

SILVA, Pedro Henrique Francisco. From Traces to Influencing Power: Data Leaks and Behavior Manipulation on Social Media. 2025. 46 p. Graduation. Technology in Systems Analysis and Development. Faculdade de Tecnologia de São Paulo. FATEC-SP. São Paulo, 2025.

This monograph aims to address how digital traces generated on content-sharing social networks are used by algorithmic systems, with a focus on recommendation algorithms, in practices that may compromise users' privacy. The research is based on a bibliographic and exploratory approach to investigate the impacts of invisible data collection, analyzing the terms of use of platforms and the limited understanding by users. Aspects related to digital surveillance and behavioral manipulation are also considered. The research proposes to reflect on the legal and social challenges regarding data protection and transparency in the use of collected information.

Keywords: Digital traces; Data; Privacy; Social networks; Recommendation algorithms; Terms of use.

LISTA DE ABREVIATURAS E SIGLAS

GDPR – Regulamento Geral sobre a Proteção de Dados

LGPD – Lei Geral de Proteção de Dados Pessoais

FTC – Comissão Federal de Comércio

LISTA DE FIGURAS

FIGURA 1 – Tabela com as políticas de privacidade de redes sociais analisadas por Mustafa Büyük.....	19
FIGURA 2 – Quadro x Resumo Teórico.....	33
FIGURA 3 – Tempo médio diário de uso por plataforma (estimativas globais, 2022-2023).....	34
FIGURA 3.1 – Tempo médio diário de uso por plataforma em formato de gráfico.....	35
FIGURA 4 – Vazamentos e exposições de dados em plataformas sociais.....	36
FIGURA 5 - Métricas referente aos termos de serviço das redes sociais.....	38
FIGURA 6 - Quadro comparativo das abordagens teóricas de Zuboff, Fuchs e Büyük.....	42

SUMÁRIO

1. INTRODUÇÃO	10
1.1 Contextualização.....	10
1.2 Questões de pesquisa	10
1.3 Hipóteses de pesquisa	10
1.4 Objetivo geral	11
1.5 Metodologia	11
2. FUNDAMENTAÇÃO TEÓRICA.....	13
2.1 Capitalismo de vigilância.....	13
2.2 Privacidade de dados nas redes sociais.....	15
2.3 Políticas de privacidade e consentimento do usuário	17
2.4 Vazamento de dados em redes sociais de compartilhamento de conteúdo	20
2.5 Algoritmos de recomendação	24
2.6 Legislações e parâmetros legais para a proteção de dados	28
3. ANÁLISE DE DADOS.....	34
3.1. Tempo de uso dos usuários nas redes sociais e seu engajamento nessas plataformas.	34
3.2. Vazamento de dados em redes sociais	36
3.3. Manipulação do comportamento de usuários em redes sociais	37
3.4. Compreensão dos termos de uso de redes sociais	38
3.5. Critérios de seleção, análise e discussão dos artigos.....	39
4. CONCLUSÃO	43
5. REFERÊNCIAS.....	44

1. INTRODUÇÃO

1.1 Contextualização

As redes sociais de compartilhamento de conteúdo integram o cotidiano de milhões de pessoas, impactando a comunicação, o consumo e as relações interpessoais. Entretanto, seu uso intensivo levanta questões relevantes sobre privacidade, segurança e o tratamento de dados pessoais.

1.2 Questões de pesquisa

Diante desse cenário, surgem as seguintes perguntas centrais desta pesquisa:

Questão 1: É possível que os algoritmos de recomendação em redes sociais de compartilhamento de conteúdo (como *TikTok* e *Instagram*) podem estar relacionados à coleta invisível de rastros digitais dos usuários e à sua possível exposição ou vazamento?

Questão 2: Os termos de uso das redes sociais de compartilhamento de conteúdo são válidos e eficientes na proteção dos dados, e são de fato compreendidos pelos usuários?

1.3 Hipóteses de pesquisa

Hipótese para a primeira questão: As plataformas de redes sociais coletam e monitoram sistematicamente os rastros digitais dos usuários (dados pessoais e comportamentais) em grande escala, muitas das vezes além do que um usuário comum imagina ou compreende, criando perfis detalhados que permitem prever e até influenciar preferências e comportamentos futuros dos indivíduos.

Hipótese para a segunda questão: A maioria dos usuários não lê ou não entende completamente os termos de uso e políticas de privacidade das redes sociais, de modo que o consentimento dado para uso de seus dados é apenas formal. Na prática, há uma aceitação não informada, o que facilita às empresas no

uso amplo (e possivelmente antiético) dos dados, sem percepção ou resistência por parte dos usuários.

1.4 Objetivo geral

O estudo tem como objetivo geral investigar de que forma os rastros digitais deixados por usuários em redes sociais de compartilhamento de conteúdo são coletados e utilizados por algoritmos de recomendação para influenciar comportamentos individuais, bem como analisar os riscos e as situações previamente ocorridas de vazamento dessas informações.

Os objetivos específicos são:

Conceituar rastros digitais e contextualizar sua geração e utilização em redes sociais de compartilhamento de conteúdo.

Analisar o funcionamento dos algoritmos de recomendação, investigando como utilizam os rastros digitais para prever e influenciar o comportamento dos usuários.

Investigar como ocorre a coleta invisível de dados pelas plataformas e os riscos associados à exposição ou vazamento dessas informações.

Avaliar a eficácia e a transparência dos termos de uso e políticas de privacidade das redes sociais na proteção dos dados dos usuários.

Verificar o nível de compreensão dos usuários sobre os termos de uso, destacando o grau de consentimento informado ou não informado na aceitação dessas políticas.

1.5 Metodologia

A metodologia adotada para este estudo foi a pesquisa bibliográfica, de caráter exploratório, para fundamentar teoricamente e coletar evidências acerca do problema proposto. Foram selecionados trabalhos acadêmicos (artigos científicos,

livros, monografias) com o objetivo de alcançar os objetivos anteriormente delineados.

2. FUNDAMENTAÇÃO TEÓRICA

A pesquisa parte de uma base teórica que contempla as transformações provocadas pelas redes sociais de compartilhamento de conteúdo, com foco na coleta de dados, no uso de algoritmos de recomendação e nos impactos dessas práticas sobre a privacidade dos usuários. São considerados conceitos como o capitalismo de vigilância, a economia dos dados e os termos de uso, com o intuito de compreender como essas estruturas moldam o comportamento digital e favorecem a exploração comercial das informações pessoais.

2.1 Capitalismo de vigilância

O capitalismo de vigilância, termo conceituado por Shoshana Zuboff, representa um modelo econômico em evolução que utiliza a experiência humana como matéria-prima gratuita para prever, influenciar e controlar o comportamento humano, especialmente no cenário do consumo. Este modelo inédito de capitalismo surgiu com a popularização da tecnologia digital e as práticas invasivas realizadas por grandes empresas de tecnologia, como o *Facebook*, que obtém grandes volumes de dados comportamentais a partir das interações digitais dos usuários deixados naquele serviço (ZUBOFF, 2019).

Rastros digitais são marcas deixadas pelas interações online dos usuários, sendo classificados em ativos (dados fornecidos diretamente) e passivos (dados capturados automaticamente). Rastro digital ativo é todo dado gerado de forma direta, ou seja, aqueles dos quais o usuário tem consciência de suas ações. Rastro digital passivo é todo dado gerado de forma indireta, isto é, sem o envolvimento direto do usuário ou com pouco ou até mesmo sem conhecimento das suas ações e de que seus dados foram coletados e armazenados.

Com a evolução de tecnologia, a percepção sobre esses dados evoluiu, o que antes era considerado um simples resíduo informativo passou a ter um valor estratégico, construindo o que ZUBOFF (2019) chama de "excedente comportamental" (*behavioral surplus*). Esses excedentes são utilizados para prever o comportamento dos usuários. A partir disso, as empresas moldam decisões

individuais, utilizando previsões comportamentais para maximizar lucros (ZUBOFF, 2019).

Segundo a autora, as empresas frequentemente afirmam que coletam dados para melhorar seus serviços aos usuários, o que, embora parcialmente correto, não apresenta o cenário completo. Uma parte significativa desses dados é principalmente utilizada na criação e no treinamento de modelos que identificam padrões no comportamento humano de usuários, permitindo que as plataformas digitais determinem com precisão as ações dos indivíduos, influenciando suas decisões futuras e os conduzindo a padrões de comportamento vantajosos para o mercado comercial em que as redes sociais estão envolvidas (ZUBOFF, 2019).

A pesquisadora também traz à tona a existência de um grande equívoco na mentalidade disseminada de um grupo de usuários que afirmam "não ter nada a esconder" e, portanto, não se preocupam com a coleta de seus dados. ZUBOFF (2019), alerta que as informações pessoais compartilhadas de forma consciente pelos usuários (dados pelos quais eles não demonstram preocupação) são, na verdade, as informações menos importantes para as empresas que administram isso. A situação se apresenta crítica quando se reconhece que os dados mais valiosos são aqueles coletados involuntariamente, através de rastros digitais deixados em diversas redes sociais e em ambientes online como um todo, proporcionando às plataformas a compreensão aprofundada dos interesses, amizades, hobbies e dependendo até estados emocionais dos usuários (ZUBOFF, 2019).

No contexto das redes sociais, é possível citar como exemplo a situação em que um usuário realiza uma pesquisa no *Google* por "artigos de motocicleta" e, em seguida, começa a receber anúncios relacionados ao tema em outras plataformas, como o *Facebook*, mesmo sem ter feito buscas nessas plataformas. Esse acontecimento evidência o poder dos dados coletados de forma muitas vezes involuntária e utilizados para alimentar sistemas de publicidade personalizada. Embora muitos usuários considerem essa prática útil e apropriada, na verdade ela mascara os mecanismos invasivos envolvidos nesse processo de segmentação.

Portanto, o capitalismo de vigilância é mais que um simples evento econômico, ele representa uma intensa transformação social e política. Empresas que administram essas informações acumulam um poder inovador, que tem a capacidade

de não apenas prever, mas também de moldar o comportamento dos usuários, interferindo diretamente na autonomia pessoal e na base institucional das democracias modernas.

2.2 Privacidade de dados nas redes sociais

Mustafa Böyük em seu artigo “*User Data and Digital Privacy: Privacy Policies of Social Media Platforms*” (2024), afirma que redes sociais de compartilhamento de conteúdo implementam políticas de privacidade que traçam extensivamente quais informações do usuário são coletadas (dados fornecidos no perfil, conteúdos postados, interações como curtidas e comentários, dados de dispositivos, localização, histórico de navegação dentro da plataforma etc.) e com que finalidade essas informações são usadas (BÖYÜK, 2024).

O autor ressalta que todas as cinco plataformas analisadas em seu artigo (*Facebook, Instagram, X/Twitter, YouTube e TikTok*) afirmam, em suas políticas, se responsabilizar com a proteção dos dados dos usuários e seguir as legislações de privacidade como o Regulamento Geral de Proteção de Dados (GDPR) e Lei Geral de Proteção de Dados Pessoais (LGPD) (BÖYÜK, 2024).

O *Twitter* (agora chamado de *X*) após implementação de legislações adotou uma postura de maior transparência sobre o que coleta e incorporou ferramentas para que o usuário possa gerenciar seus dados e personalizar suas configurações de privacidade de forma relativamente acessível (BÖYÜK, 2024). Essa iniciativa é citada por FUCHS (2021) como um movimento positivo, permitindo que os usuários tenham algum controle sobre a utilização de seus dados pessoais pela plataforma (BÖYÜK, 2024; FUCHS, 2021).

O *YouTube*, declara coletar dados de histórico de vídeos assistidos, buscas realizadas e informações do dispositivo, os usando para otimizar recomendações de conteúdo e direcionamento de anúncios (BÖYÜK, 2024). A plataforma assegura que qualquer compartilhamento de dados com terceiros é feito mediante consentimento do usuário, em conformidade com as condutas exigidas por leis, o que indica uma preocupação da empresa em demonstrar conformidade regulatória (BÖYÜK, 2024).

No caso do *TikTok*, plataforma mais recente e em rápido crescimento, BÖYÜK

(2024) indica que a política de privacidade menciona a coleta intensiva de dados sobre o conteúdo gerado pelo usuário, comportamento de visualização e engajamento, bem como dados do dispositivo e rede (BÖYÜK, 2024). Pesquisas revelaram que, em 2022, o *TikTok* integrava um rastreador capaz de capturar cada tecla digitada pelos usuários em seu navegador interno, o que significa que ao abrir um link externo dentro do *TikTok*, tudo que o usuário preenche poderia ser registrado.

Isso comprova o nível de detalhamento que o serviço de coleta possuía como no caso do *TikTok*, assim como em outros aplicativos com enfoque semelhante, não há limites claramente estabelecidos quanto à extensão do registro das ações dos usuários dentro da própria rede social. Essa vigilância pode se expandir para além da plataforma, permitindo o monitoramento do comportamento dos indivíduos em outros sites e aplicativos externos. (CARDOSO, 2022).

Embora as empresas argumentem que tal coleta aprimora a experiência do usuário, autores como ZUBOFF (2019) apontam que ela também eleva riscos à privacidade (ZUBOFF, 2019). A necessidade de um algoritmo altamente responsivo aos mínimos sinais de interação do usuário comprova esse padrão. Cada segundo de visualização, pausa ou hesitação é cuidadosamente registrado e utilizado para refinar as próximas recomendações de conteúdo (MILNE, 2024; TIKTOK, 2024).

Uma observação importante que BÖYÜK (2024) apresenta é que, apesar das diferenças de enfoque entre redes sociais, cada uma delas seguem o objetivo de o maior volume de informações pessoais e de uso, e todas já enfrentaram incidentes ou violações de privacidade significativas no passado recente. Isso sugere que as políticas documentadas nem sempre se refletem na proteção efetiva dos dados de fato (BÖYÜK, 2024).

Certamente, o estudo de BÖYÜK (2024) menciona casos de violações graves como o escândalo de *Cambridge Analytica* envolvendo o *Facebook* em 2018, um vazamento de dados de contatos do *Instagram* em 2019, um incidente de segurança de senhas no *Twitter* em 2018, uma violação de privacidade relacionada a dados de crianças no *YouTube* em 2019, repetida no mesmo ano, que logo progrediu para outra infração cometida pela plataforma em 2020, também envolvendo a violação da privacidade dos usuários (BÖYÜK, 2024).

Cada uma dessas situações revelou dificuldades, falhas ou aberturas na forma

como essas empresas protegiam (ou compartilhavam) os dados dos usuários, muitas vezes em contradição com o que suas próprias diretrizes alegavam. Embora as plataformas mencionadas declarem políticas de privacidade robustas, existe uma incongruência entre a teoria e a prática no que diz respeito à garantia de proteção à privacidade do usuário (BÖYÜK, 2024).

Em síntese, do ponto de vista teórico, redes sociais permanecem com políticas de coleta de dados extensivas, justificadas como melhorias de serviço e a necessidade de uma sustentação financeira via publicidade direcionada. Elas afirmam buscar obedecer às leis de proteção de dados e garantir consentimento, porém estudos indicam complexidades e riscos.

Como apontado por SOLOVE (2009), proteger a privacidade na era digital se tornou um desafio cada vez mais complexo, pois os usuários muitas vezes não estão suficientemente informados sobre os processos de coleta de dados (SOLOVE, 2009; BÖYÜK, 2024). Isso dificulta o consentimento plenamente consciente e abre brechas para violações. BÖYÜK (2024) conclui informando que existe sim a necessidade de medidas mais vigorosas de segurança e de controles amigáveis ao usuário para preservar a privacidade, bem como a responsabilização das plataformas em casos de uso indevido dos dados (BÖYÜK, 2024).

2.3 Políticas de privacidade e consentimento do usuário

BÖYÜK (2024) em seu artigo, destaca uma preocupação amplamente discutida na literatura sobre privacidade, o autor comenta que há uma desconexão entre o que os usuários concordam e os que realmente compreendem os termos que as redes sociais divulgam. BÖYÜK (2024) diz que, apesar das plataformas de tentarem se adequar ao Regulamento Geral de Proteção de Dados (GDPR), muitas políticas de privacidade continuam a ser carregadas de termos jurídicos e técnicos BÖYÜK (2024).

Tais diretrizes, frequentemente longas e complexas, dificultam a leitura integral e a noção clara por grande parte dos usuários. Como consequência, embora formalmente os usuários tenham “concordado” com a coleta e uso de seus dados, na prática não há um consentimento consciente (BÖYÜK, 2024; PRIVACYTOOLS, 2022).

O pesquisador destaca que essa má compreensão coloca em vulnerabilidade o princípio do consentimento informado, o qual é fundamentado em legislações como o Regulamento Geral de Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD), pois grande parte dos usuários não tem convicção do que autorizou ao utilizar aquele serviço, dificultando inclusive que exerça direitos como optar por não fornecer determinados dados, ou revogar permissões BÖYÜK (2024). Essa evidência é reforçada quando pesquisas de opinião e experimentos são analisadas.

Em 2017, a empresa Deloitte realizou uma pesquisa onde identificou que 91% dos usuários aceitam termos sem ler e apenas 9% dos restantes habitualmente fazem a leitura dos termos de privacidade (CORASSA, 2024; PRIVACYTOOLS, 2022). Na mesma linha, Lorrie Cranor (professora especialista em privacidade) estimou que seria necessárias cerca de 244 horas por ano para que um indivíduo leia todas as políticas de privacidade que os sites e aplicativos online compartilham, um esforço claramente inviável para muitos usuários. Dessa forma, consolida-se o que alguns autores denominam de ‘ilusão de consentimento’, um fenômeno que acontece no ato em que os usuários aceitam os termos de uso sem a compreensão real de seu conteúdo (CRANOR, 2008; SOLOVE, 2008; BÖYÜK, 2024).

Ainda que regularmente aceitos, os termos legais frequentemente carecem de clareza prática, dificultando a compreensão real pelo usuário médio. Legalmente, os termos de uso são considerados válidos, são contratos de adesão aceitos voluntariamente por usuários. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) reconhece a validade do consentimento para tratamento de dados, desde que haja informação adequada ao titular. O problema está na avaliação do que seria “adequado”.

Como observado na coluna de CORASSA (2024), pelo ponto de vista jurídico, os termos de uso seguem o modelo de “aviso e consentimento”, e salvo abusividades específicas, sua eficácia costuma ser reconhecida nos tribunais CORASSA (2024). Entretanto, a eficácia jurídica não afeta o desempenho prático ao comunicar limites de uso ao usuário. Ou seja, mesmo que do ponto de vista legal a plataforma esteja coberta pela aceitação dos termos, isso não significa que o usuário esteja consciente das implicações, o que se torna um problema de transparência e ética.

Figura 1 - Tabela com as políticas de privacidade de redes sociais analisadas por Mustafa Böyük

Platform	Data Encryption Method	Data Storage Centers	Collected Personal Information	Collected Device Information	Data Retention Period	User Control	Legal Compliance
Facebook/Meta	TLS 1.3	US	Name, email address, interests	Advertising analytics, text chat	Advertising and analytics	Users can download data or delete	GDPR, KVKK
Instagram	TLS 1.3	US	Name, email address, interests	Advertising analytics	Advertising analytics	Users can issue data, delete accounts	GDPR, KVKK
X/Twitter	TLS 1.3	US	Name, email address, interests	OS, browser details	Advertising analytics	Issue a data deletion request	GDPR, KVKK
YouTube	TLS 1.3	US	Name, email address, comments	OS, browser location	30 days after account deletion	Delete their content	GDPR, KVKK

Fonte: User Data and Digital Privacy: Privacy Policies of Social Media Platforms (BÖYÜK, 2024).

Complementando a fundamentação deste estudo, na figura 1, BÖYÜK (2024) apresenta uma tabela detalhada em seu estudo contendo as principais políticas de privacidade das redes sociais analisadas em seu artigo, *Facebook*, *Instagram*, *X (Twitter)*, *YouTube* e *TikTok*. De acordo com a análise realizada pelo autor, todas essas plataformas atualmente empregam o protocolo de criptografia TLS 1.3, que é reconhecido por proporcionar maior segurança na proteção dos dados transmitidos.

Apesar disso, ainda coletam extensivamente dados pessoais como histórico de mensagens, conteúdos compartilhados, interações dos usuários, bem como informações detalhadas dos dispositivos utilizados, incluindo sistema operacional, tipo de navegador, localização geográfica via GPS, conexões Wi-Fi e Bluetooth, etc (BÖYÜK, 2024).

Outro ponto apresentado anteriormente pelo autor, e reforçado novamente é que as redes sociais frequentemente compartilham dados pessoais dos usuários com terceiros, visando principalmente fins comerciais e analíticos (BÖYÜK, 2024).

O escritor também menciona diferenças no período pelo qual os dados são

armazenados, enquanto *Facebook* e *Instagram* mantêm os dados coletados por até 90 dias, *X (Twitter)* e *TikTok* armazenam por até 30 dias, e o *YouTube* por até 60 dias. Essa oscilação comprova que, apesar das plataformas se apresentarem alinhadas às legislações internacionais de proteção de dados como o Regulamento Geral de Proteção de Dados (GDPR), o controle efetivo sobre a privacidade acaba sendo repassado para os próprios usuários. Teoricamente, usuários tem a possibilidade de baixar, excluir ou congelar suas informações pessoais armazenadas pelas plataformas, contudo, na prática, poucos estão plenamente cientes desses direitos ou sabem como utilizá-los adequadamente (BÖYÜK, 2024).

Em vista disso, torna-se evidente a necessidade de reavaliar os mecanismos de comunicação entre plataformas e usuários. Mais do que garantir o cumprimento formal das normas, é fundamental assegurar que o consentimento seja compreensível, acessível e significativo. Do contrário, a proteção da privacidade continuará sendo limitada por barreiras técnicas e informacionais que colocam os usuários em situação de vulnerabilidade frente ao uso de seus dados pessoais.

2.4 Vazamento de dados em redes sociais de compartilhamento de conteúdo

Segundo o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), vazamentos de dados consistem na divulgação não autorizada de informações confidenciais para fora do ambiente no qual deveriam estar protegidas, basicamente, qualquer brecha/incidente de segurança que leve à destruição, perda, alteração ou divulgação não autorizada, seja ela acidental ou ilícita, de dados pessoais pode ser considerada como vazamento de dados (UNIÃO EUROPEIA, 2016).

Segundo (BÖYÜK, 2024), a violação de dados em redes sociais está relacionada ao uso indevido de APIs e integrações com aplicativos de terceiros. O escândalo da *Cambridge Analytica* exemplifica esse tipo de falha. Por meio de um aplicativo aparentemente inofensivo, denominado de “*This Is Your Digital Life*”, desenvolvido por Aleksandr Kogan da Universidade de Cambridge, onde foram coletados dados não apenas dos usuários que interagiram com o aplicativo, mas também das informações de seus contatos na plataforma. Estima-se que até 87 milhões de perfis tenham sido comprometidos. Esses dados foram, então, repassados

à *Cambridge Analytica*, que utilizou as informações para criar perfis psicográficos detalhados, aplicando técnicas de microsegmentação para influenciar eleitores em campanhas políticas, como a de Donald Trump em 2016. Ao todo, dados de aproximadamente 50 milhões de usuários foram utilizados de maneira indevida, sem o consentimento explícito dos titulares, configurando uma grave violação de privacidade (BÖYÜK, 2024; ZUBOFF, 2019).

Esse episódio, que causou grande repercussão pública, ilustra como falhas estruturais e a negligência das plataformas podem resultar na exposição massiva de dados pessoais, afetando milhões de usuários. A violação teve consequências legais e institucionais, forçando o *Facebook* a adotar medidas emergenciais para restaurar a confiança dos usuários.

No mesmo ano, outra falha de segurança foi revelada, envolvendo a exploração de *tokens* de acesso, que expôs os dados de mais de 30 milhões de contas. Mark Zuckerberg, CEO do *Facebook*, reconheceu publicamente a falha na proteção dos dados e classificou o episódio como uma "*ruptura de confiança grave*". Como resultado, em 2019, o *Facebook* foi multado em 5 bilhões de dólares pela Comissão Federal de Comércio (FTC) devido às violações à privacidade dos usuários (BÖYÜK, 2024; UNITED STATES, 2022).

Esses casos evidenciam a gravidade dos vazamentos de dados e a importância de adotar mecanismos eficazes de controle e monitoramento, especialmente quando dados são compartilhados com parceiros externos sem a devida transparência e segurança (BÖYÜK, 2024).

Ainda em 2019, o *Instagram*, que na época já era uma plataforma administrada pelo *Facebook*, agora *Meta Platforms*, enfrentou um grave incidente de segurança ao ter uma base de dados contendo informações de cerca de 49 milhões de usuários, incluindo e-mails e números de telefone, exposta publicamente sem qualquer proteção por senha. Tal exposição levou a plataforma a revisar seus protocolos de segurança, promovendo ajustes como a adoção da autenticação em dois fatores e o aprimoramento das diretrizes de privacidade (BÖYÜK, 2024).

Outro caso relevante ocorreu com o *Twitter*, em 2018, quando a empresa revelou uma falha interna que resultou no armazenamento de senhas de aproximadamente 330 milhões de usuários em texto simples nos logs do sistema, sem

qualquer forma de criptografia. Embora não tenham sido registradas evidências de acessos indevidos, a plataforma orientou todos os usuários a alterarem suas senhas como medida preventiva (REUTERS, 2018).

No cenário de proteção de dados de crianças, tanto o *YouTube* quanto o *TikTok* estavam envolvidos em casos de violação de privacidade infantil. Em 2019, o *YouTube* foi acusado de coletar dados pessoais de crianças menores de 13 anos sem o consentimento dos responsáveis legais, prática que contraria legislações como a Lei de Proteção da Privacidade On-line das Crianças (COPPA) e o próprio Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Como consequência, a empresa foi multada em 170 milhões de dólares pela Comissão Federal de Comércio (FTC). Após o fato, a plataforma reformulou suas políticas relativas ao conteúdo infantil, visando adequação legal (BÖYÜK, 2024; THE GUARDIAN, 2019; UNITED STATES, 2022).

De forma semelhante, o *TikTok*, na época ainda operando sob o nome de Musical.ly, também foi responsabilizado por práticas ilegais de coleta de dados de menores de idade. Em 2019, a empresa foi multada em 5,7 milhões de dólares pela Comissão Federal de Comércio (FTC) e obrigada a implementar mudanças estruturais para garantir o consentimento dos pais e proteger usuários com menos de 13 anos, em conformidade com as legislações vigentes (BÖYÜK, 2024; THE VERGE, 2019; UNITED STATES, 2022).

Evidentemente, todos os casos apresentam a fragilidade que muitas redes sociais possuem diante da responsabilidade de proteger dados pessoais, bem como a necessidade de fiscalização contínua e regulamentação mais eficiente diante do avanço das tecnologias de coleta e análise de informações.

Por fim, o uso de engenharias sociais, que é uma técnica de manipulação psicológica para explorar usuários, onde serve como porta de entrada para acessos indevidos a informações de usuários. A extração de credenciais por meio de golpes de *phishing* ou pelo uso de senhas fracas e reutilizadas. A ausência de autenticação multifator e outras formas de verificação aumenta consideravelmente o risco, tornando os usuários mais vulneráveis (STEEL, 2023)

Os impactos desses vazamentos vão além das perdas materiais e atingem aspectos sensíveis da vida digital e psicológica dos usuários. Em termos de

privacidade, as exposições comprometem dados que deveriam estar protegidos por confidencialidade, revelando conversas, preferências, localização, imagens e outros registros que compõem a identidade digital do indivíduo (BÖYÜK, 2024).

Diante dessas ameaças, diversas medidas de segurança são recomendadas para prevenir ou controlar vazamentos. A criptografia de dados, tanto em repouso quanto em trânsito, é uma das práticas fundamentais. Dados armazenados em servidores devem ser protegidos por algoritmos robustos, como o AES-256, e a comunicação entre usuários e servidores deve ser cifrada por meio de protocolos como TLS. Dessa forma, mesmo que os dados sejam acessados indevidamente, permanecerão ilegíveis para terceiros não autorizados (CYERA, 2023).

Outra medida essencial é o uso de *hashing* seguro para senhas, que jamais devem ser armazenadas em texto puro. A falha do *Twitter* em 2018 demonstrou como o armazenamento indevido de credenciais pode expor usuários a riscos desnecessários. As entidades também precisam adotar políticas de controle de acesso baseadas na restrição máxima de privilégios, autenticação multifator e políticas de revisão e auditoria de acessos. Ferramentas como SIEM (*Security Information and Event Management*) e DLP (*Data Loss Prevention*) ajudam a monitorar movimentações suspeitas e impedir que dados saiam do ambiente protegido. A realização de testes de intrusão e auditorias periódicas garante que falhas sejam identificadas antes que possam ser exploradas (BÖYÜK, 2024; IBSEC, 2024).

Além disso, a atuação de terceiros nas plataformas sociais representa um vetor relevante de risco. Como destacado por BÖYÜK (2024), APIs mal gerenciadas e permissões excessivas concedidas a aplicativos externos podem permitir a extração indevida de dados. Casos como o da *Cambridge Analytica* apresentam esse cenário, em casos como esse, a falha não ocorreu diretamente na infraestrutura das plataformas, mas sim nos parceiros que armazenaram as informações de forma insegura. Como consequência, o controle sobre os dados foi perdido, mesmo que sua origem fosse legítima (BÖYÜK, 2024). Diante desse histórico, percebe-se que, apesar das medidas regulatórias, as redes sociais ainda apresentam vulnerabilidades significativas na proteção de dados, o que reforça a urgência de mecanismos técnicos e legais mais efetivos.

2.5 Algoritmos de recomendação

Algoritmos de recomendação em redes sociais se tornaram fontes centrais na forma como informações e mídias são consumidas online. Tais algoritmos filtram e personalizam o conteúdo exibido a cada usuário com base em seus dados e interações prévias, construindo um fluxo de informações personalizado. A princípio, essa personalização busca aumentar a relevância e o engajamento, o usuário tende a ver mais do que lhe interessa, entretanto, estudos apontam que esses sistemas não são neutros. Pelo contrário, eles atuam com lógicas empresariais que visam condicionar o comportamento do usuário e maximizar objetivos comerciais das plataformas ZUBOFF (2019).

Nessa lógica, o conhecimento gerado sobre o indivíduo é utilizado para orientar seu comportamento em direções lucrativas para terceiros. De fato, recursos comuns nas redes sociais, como notificações, “curtidas” e rolagem infinita de conteúdo, funcionam como mecanismos de estímulo comportamental contínuo, como notificações e rolagem infinita, que geram hábito e engajamento compulsivo e reforçam hábitos de uso compulsivo. Essa forma de engajamento programado não é acidental, na realidade se refere a um design persuasivo cuidadosamente arquitetado para capturar e manter a atenção do usuário (ZUBOFF, 2019).

A autora afirma que, após inseridos no código algorítmico e em dispositivos inteligentes, os ‘*nudges*’ (estímulos de incentivo) se tornaram a base de uma nova ciência de modificação comportamental em grande volume, atuando de maneira ubíqua e, muitas vezes, imperceptível ao usuário. Assim, o ambiente digital passa a agir sobre o usuário de forma abusiva e controladora, guiando suas escolhas sem que ele se dê conta. Importante destacar que essa influência se fortalece na falta de clareza de:

“[...] a consciência humana é uma ameaça às receitas da vigilância, pois a conscientização põe em risco o projeto mais amplo de modificação de comportamento (ZUBOFF, 2019, p. 196)”

Ou seja, quanto menos usuários perceberem as tentativas de direcionar seu agir, mais eficaz se torna o algoritmo como instrumento de controle.

Sob outra perspectiva crítica, FUCHS (2014) analisa os algoritmos de

recomendação no contexto da economia política das mídias sociais, enfatizando seu papel na mercantilização da comunicação e na alienação do usuário. Para o autor, redes sociais se apropriam do trabalho digital não-pago dos usuários, seu tempo de uso, seus dados e conteúdos gerados, e o convertem em valor econômico por meio da publicidade direcionada. FUCHS (2014) descreve esse fenômeno como ‘trabalho digital’, a atenção coletiva dos usuários é tratada como mercadoria a ser vendida, e os algoritmos são os mecanismos que gerenciam a captação e a exploração máxima dessa atenção. Ou seja, ao usuário, ao usufruir de um serviço aparentemente “gratuito”, na verdade paga com sua atenção e privacidade, tornando-se ele próprio o produto oferecido aos anunciantes (FUCHS, 2014).

Assim, os sistemas de recomendação favorecem conteúdos mais adequados aos interesses comerciais, reduzindo o campo informativo do usuário ao que é lucrativo para a plataforma. Nesse processo, o escritor entende que os algoritmos personalizados são como instrumentos de manipulação ideológica discreta, que promovem a obediência aos padrões de consumo e pensamento alinhados aos interesses do capital, aprofundando a alienação. O usuário é mantido engajado, porém em um engajamento de baixa reflexividade, muitas vezes sem consciência crítica de que suas escolhas estão sendo guiadas e limitadas (FUCHS, 2014).

Um aspecto fundamental dessa dinâmica é a microsegmentação do público e a publicidade direcionada viabilizadas pelos algoritmos. Cada ação nas redes sociais alimenta modelos de personalização detalhada, segmentando os usuários em categorias minuciosas de preferências, traços de personalidade e tendências de consumo (FUCHS, 2014). Com base nesses perfis, anunciantes podem direcionar mensagens específicas a nichos extremamente particulares, processo conhecido como *microtargeting*.

ZUBOFF (2019) ressalta que não se trata apenas de mostrar um produto que o usuário possivelmente compraria, mas criar condições para que ele faça a compra, explorando vulnerabilidades e desejos individuais com precisão algorítmica (ZUBOFF, 2019). Recompensas e conteúdos são continuamente adaptados conforme a reação do usuário, em um ciclo contínuo de experimentação comportamental automatizada, realizada.

Isso gera preocupações éticas e sociais, especialmente quando técnicas

similares são aplicadas fora do âmbito comercial. A manipulação política e da opinião pública via algoritmos de recomendação emergiu como um dos efeitos mais graves referente aos sistemas (ZUBOFF, 2019). Ao incentivar bolhas informativas e *feeds* personalizados, as plataformas podem isolar os usuários em bolhas ideológicas, nas quais crenças existentes são reforçadas e opiniões divergentes são abafadas (FUCHS, 2014). Essa dinâmica cria um terreno produtivo para campanhas de desinformação e propaganda dirigida. FUCHS (2014) já alertava que as redes sociais, ao priorizarem conteúdo sensacionalista e engajador, podem comprometer o debate democrático, pois a lógica comercial privilegia a atenção em vez da veracidade ou da pluralidade (FUCHS, 2014).

BÖYÜK (2024) apresenta evidências recentes desse fenômeno ao estudar o papel do algoritmo do *TikTok* na divulgação de discursos extremistas. Segundo o autor, a estrutura algorítmica da plataforma amplifica conteúdos populares de forma automática, o que significa que, se um usuário interage com conteúdo de ódio ou desinformação, receberá progressivamente mais do mesmo. Esse efeito de reforço gera um processo de normalização do discurso extremista e de polarização da opinião pública, conteúdo antes insignificante e polêmico pode ganhar ampla visibilidade e aceitação em certas comunidades online graças ao empurrão algorítmico (BÖYÜK, 2024).

Resumidamente, os sistemas de recomendação podem ser explorados para manipular percepções coletivas, seja pela propagação direcionada de notícias falsas ou pela criação de agendas personalizadas que desviam a atenção de temas de interesse público. O resultado é uma potencial distorção na formação de opinião e da vontade popular, já que decisões individuais, como o voto ou apoio a causas, passam a refletir a influência invisível desses mecanismos.

Os impactos causados pelos algoritmos de recomendação destacam como eles podem exercer uma influência direta na tomada de decisão do usuário. Dessa maneira, a liberdade de escolha do usuário é sutilmente comprometida, ele escolhe entre opções que lhe foram apresentadas de forma estratégica.

Estudos de caso comprovam que pequenas mudanças nos algoritmos podem alterar significativamente decisões dos usuários, por exemplo, a ordem dos resultados de busca no *Google* pode influenciar quais notícias o público lê sobre um candidato

(afetando opiniões políticas), ou a forma como o *YouTube* auto-reproduz vídeos pode levar um usuário de entretenimento leve a teorias da conspiração em poucas horas (BÖYÜK, 2024; ZUBOFF, 2019). A persuasão automatizada opera em nível detalhado, adaptando em tempo real às respostas do indivíduo, o que confere a esses sistemas um poder de manipulação bem superior aos meios de comunicação de massa tradicionais.

Por fim, se torna crucial abordar esses fenômenos pela visão da economia de atenção. Na estrutura comercial atual, a atenção do usuário é o recurso escasso e valioso a ser capturado, quanto mais tempo as pessoas passam conectadas e engajadas, maior o volume de impressões publicitárias e de dados comportamentais coletados.

Em vista disso, plataformas e seus algoritmos estão envolvidos em uma verdadeira disputa pelo tempo de uso do indivíduo. FUCHS (2014) descreve que o elemento principal das redes sociais é justamente esse engajamento contínuo, a infraestrutura algorítmica otimizada para reter a atenção do usuário o máximo possível, mantê-lo clicando, rolando e interagindo, num ciclo incessante de consumo de conteúdo. Isso explica por que conteúdos emocionalmente carregados, polêmicos, alarmantes ou altamente agradáveis, tendem a ser promovidos, eles prendem a atenção mais do que informações equilibradas ou neutras (FUCHS, 2014).

A consequência, apontada criticamente por ZUBOFF (2019), é o esgotamento da atenção consciente e a captura da vida cotidiana pelas telas, os indivíduos têm sua atenção cronicamente sequestrada pelas plataformas, que estruturam experiências digitais com base em ciclos viciosos de recompensa e engajamento, muitas vezes indo além do que pretendiam, impulsionados por mecanismos de recomendação viciantes. Estabelece, assim, uma forma de dominação comportamental na qual o tempo do usuário é apropriado em benefício das empresas, muitas vezes em prejuízo de seu bem-estar ou autonomia.

A economia da atenção gera efeitos colaterais socialmente, como o comprometimento da capacidade de foco e atenção, o excesso de informações e a crescente dependência tecnológica (ZUBOFF, 2019). Em uma análise crítica, é possível afirmar que os algoritmos de recomendação funcionam como instrumentos de poder que operam na dimensão do comportamento, ao controlar a alocação da

atenção humana, eles influenciam preferências, decisões e padrões de interação em grande proporção, consolidando uma nova forma de governança algorítmica sobre a conduta dos usuários (FUCHS, 2014; ZUBOFF, 2019).

Em suma, os algoritmos de recomendação vão além de filtros de conveniência, constituindo mecanismos de influência e dominação comportamental na vida digital. Por meio do design persuasivo, da segmentação direcionada e da manipulação da atenção, esses sistemas impactam a autonomia, a cultura e a democracia. Assim, a compreensão crítica desses processos é essencial para expor as relações de poder e promover a proteção dos usuários frente às novas arquiteturas digitais de controle.

2.6 Legislações e parâmetros legais para a proteção de dados

As dinâmicas de exploração de dados pessoais nas plataformas digitais desencadearam, nos últimos anos, respostas regulatórias significativas, especialmente na Europa e no Brasil. Autores como Shoshana Zuboff enfatizam que a evolução do capitalismo de vigilância ocorreu em um cenário de fragilidade jurídica, o que permitiu grandes empresas de tecnologia acumularem poder e conhecimento sem supervisão adequada. Nesse cenário, a proteção da privacidade tornou-se uma preocupação central, levando à elaboração de normas jurídicas abrangentes para preservar os dados dos usuários (ZUBOFF, 2019; FUCHS, 2014).

Dentre essas normas, destacam-se o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelecem parâmetros rigorosos para o tratamento de informações pessoais. Essas legislações representam uma mudança de paradigma ao transferir ao âmbito jurídico garantias antes inexistentes, procurando frear os excessos da economia da informação e reequilibrar a relação de poder entre plataformas e usuários (ZUBOFF, 2019). Conforme observado por Christian Fuchs, a implementação de regulamentações rigorosas é imprescindível para impor limites às práticas das empresas, uma vez que a autorregulação do setor raramente seria suficiente para garantir direitos dos titulares dos dados FUCHS (2021).

O Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor desde maio de 2018, é considerado um marco global de referência em proteção

de dados. Ele impõe regras estritas sobre como organizações devem coletar, processar e armazenar dados pessoais, reforçando princípios como transparência, minimização de dados e responsabilização (BÖYÜK, 2024).

Entre suas diretrizes centrais estão a exigência de um consentimento claro por parte do usuário para o processamento de seus dados, a definição clara das finalidades de uso das informações e a obrigação de disponibilizar aos indivíduos diversos direitos, tais como acesso aos dados coletados, retificação, portabilidade e eliminação (FUCHS, 2021).

O Regulamento Geral de Proteção de Dados da União Europeia (GDPR) também estabeleceu sanções severas em caso de violação, autoridades podem aplicar multas de até 20 milhões de euros ou 4% do faturamento global anual da empresa infratora, prevalecendo o maior valor (UNIÃO EUROPEIA, 2016). Essas penalidades expressivas refletem a intenção de tornar o cumprimento das normas de privacidade parte vinculado do modelo de negócios das empresas de tecnologia.

Além disso, o regulamento cria mecanismos de fiscalização por meio de autoridades nacionais de proteção de dados em cada país-membro da UE, fortalecendo a governança sobre fluxos informacionais. Como resultado, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) se tornou um padrão-ouro em privacidade digital, inspirando reformas legais em todo o mundo (BÖYÜK, 2024).

ZUBOFF (2019) reconhece que a adoção do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) foi um passo importante no enfrentamento das desigualdades no controle de informações, o definindo como “um bom começo” na construção de um novo padrão de controle sobre o capital de dados. Trata-se de uma iniciativa que propõe a reformulação dos modelos de negócio de grandes empresas de tecnologia, historicamente acostumadas a operar sob baixa regulação governamental, trazendo à discussão social a necessidade de impor limites aos excessos do mercado de dados (ZUBOFF 2019).

No rastro do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), empresas de redes sociais passaram a adequar suas políticas internas para demonstrar conformidade. De fato, após a implementação do regulamento europeu, observou-se um movimento setorial de revisão dos documentos de privacidade,

buscando apresentar termos mais claros quanto à coleta, uso de informações e opções de controle disponíveis ao usuário (BÖYÜK, 2024).

Como exemplo, o *Twitter* reforçou a transparência sobre os dados que coleta e incorporou ferramentas acessíveis de gerenciamento de privacidade, permitindo que o usuário personalize configurações e exerça escolhas sobre anúncios personalizados e compartilhamento de informações (BÖYÜK, 2024).

Essa mudança é destacada por FUCHS (2021) como um avanço positivo, pois oferece aos indivíduos maior agência sobre seus dados dentro da plataforma, um pequeno contraponto ao desequilíbrio típico em que apenas as empresas detinham o controle informacional. Do mesmo modo, o *YouTube* e outras plataformas passaram a declarar que qualquer compartilhamento de dados com terceiros ocorre apenas mediante consentimento do usuário e em conformidade com as exigências legais, evidenciando a preocupação em demonstrar conformidade regulatória de forma pública (FUCHS, 2021; BÖYÜK, 2024).

Em síntese, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) impulsionou mudanças significativas nas práticas de proteção de dados, tanto ao impor obrigações legais quanto ao reforçar a responsabilidade das empresas no tratamento de informações pessoais. Essa tendência influenciou a criação da Lei Geral de Proteção de Dados (LGPD) no Brasil, que, inspirada no GDPR, estabelece diretrizes para o processamento de dados, direitos dos titulares e deveres de controladores e operadores, consolidando um novo padrão jurídico de proteção da privacidade (BRASIL, 2018).

A Lei Geral de Proteção de Dados Pessoais (LGPD) criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por zelar pela aplicação da lei, editar normas complementares e fiscalizar eventuais infrações. Em relação a lei brasileira, ela prevê multas administrativas que podem chegar a 2% do faturamento da empresa no país, limitadas a 50 milhões de reais por infração, assim como outras penalidades, incluindo a comunicação pública da infração e o bloqueio ou remoção dos dados irregulares.

Assim como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a visão central da Lei Geral de Proteção de Dados Pessoais (LGPD) é redirecionar o controle sobre os dados na figura do usuário (titular), promovendo maior

transparência nas relações entre indivíduos e empresas e garantindo meios legais para coibir abusos no uso de informações pessoais. A adoção da Lei Geral de Proteção de Dados Pessoais (LGPD) representa parte de um movimento global no qual jurisdições buscam alinhar-se a um padrão internacional de privacidade, facilitando inclusive a interoperabilidade normativa (BRASIL, 2018).

De modo geral, tanto a Regulamento Geral de Proteção de Dados da União Europeia (GDPR) quanto a Lei Geral de Proteção de Dados (LGPD) visam garantir a privacidade e a autonomia dos indivíduos sobre seus dados pessoais, reconhecendo-os como direitos fundamentais.

Contudo, a literatura destaca desafios na efetividade prática dessas garantias, principalmente no que se refere ao consentimento informado e à transparência. Apesar da vigência do GDPR, muitas políticas de privacidade ainda são extensas, técnicas e de difícil compreensão para o usuário comum (BÖYÜK, 2024). BÖYÜK (2024) observou que, ao analisar as políticas das principais redes sociais, que embora formalmente as plataformas tenham ajustado seus termos para cumprir os requisitos legais, na prática um usuário comum não consegue entender plenamente o que está autorizando.

Assim, ainda que juridicamente os termos de uso sejam válidos (satisfazendo o modelo de “aviso e consentimento” previsto em lei), há uma lacuna entre a legalidade formal e a transparência substantiva (BÖYÜK, 2024). O resultado é que conceitos fundamentais dessas regulações, como o próprio consentimento livre e informado, podem ficar esvaziados no contexto real de uso, usuários continuam a entregar dados sem plena noção das consequências. FUCHS (2014) já chamava a atenção para a situação em que a assimetria de informação entre plataformas e usuários dificulta o pensamento crítico dos indivíduos apenas por via de consentimento, visto que o desequilíbrio estrutural de poder permanece (BÖYÜK, 2024; FUCHS, 2014).

Em concordância, ZUBOFF (2019) sustenta que mecanismos legais isolados enfrentam limitações diante da lógica expansiva do capitalismo de dados, as empresas tendem a contornar ou absorver as novas regras em seus modelos de negócio, o que exige não apenas fiscalização contínua, mas também estratégias educativas para dar o controle de seus próprios dados para os usuários, para que

estes produzam os efeitos desejados (FUCHS, 2021; ZUBOFF, 2019).

Ainda que possam ser insuficientes, as legislações antes mencionadas marcaram uma mudança regulatória necessária, estabelecendo balizas claras para a proteção de dados em escala internacional e nacional. Essa estrutura regulatória oferece um vocabulário jurídico para que violações sejam reconhecidas e punidas, por exemplo, vazamentos de dados passaram a ser notificados e considerados infrações graves, sujeitas a sanções administrativas e judiciais (BÖYÜK, 2024).

Diversos casos de violação de dados resultaram em multas históricas, evidenciando a tentativa dos reguladores de dar concretude às normas. Ao mesmo tempo, plataformas buscam equilibrar-se entre o cumprimento da lei e a manutenção de seus modelos de negócio baseados em dados, o que gera tensões contínuas. Neste sentido, autores argumentam que a simples existência das leis não basta, é preciso evoluir em mecanismos de aplicação e em formas de simplificar a comunicação com os usuários (FUCHS, 2021; BÖYÜK, 2024).

Portanto, a efetiva proteção de dados dependerá tanto da consistência desses parâmetros normativos quanto da capacidade de implementá-los de maneira transparente e acessível, garantindo que os direitos proclamados no papel sejam exercidos na prática cotidiana. A Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD), constituem pilares de um novo regime de governança da informação, que se encontra em construção contínua, são base para a responsabilização das plataformas e para a consciência dos usuários, mas demandam aprimoramentos e vigilância constante para acompanhar o rápido ritmo das inovações tecnológicas e das estratégias empresariais no ambiente digital (ZUBOFF, 2019; FUCHS, 2021).

Em conclusão, a fundamentação teórica evidencia que a criação dessas legislações representa um esforço direto de retomar o controle sobre os dados pessoais na sociedade da informação, acompanhando as advertências críticas da literatura acadêmica, todavia, seu sucesso em resgatar a autonomia e a privacidade do usuário ainda depende de como são efetivamente aplicadas e complementadas por outras iniciativas de regulação e educação digital.

Quadro x Resumo Teórico

Figura 2 – Quadro x Resumo Teórico

PRINCIPAIS ASPECTOS DO REFERENCIAL TEÓRICO	AUTORES
Capitalismo de vigilância e modificação comportamental	ZUBOFF, S.
Privacidade de dados nas redes sociais	BÖYÜK, M.
Políticas de privacidade e consentimento do usuário	CRANOR, L.F.; BÖYÜK, M.; SOLOVE, D.
Algoritmos de recomendação e manipulação de comportamento	ZUBOFF, S.; FUCHS, C.
Economia da atenção e dominação algorítmica	FUCHS, C.; ZUBOFF, S.
Vazamentos de dados e riscos digitais	BÖYÜK, M.; SÜZEN, A.A.; CEYLAN, O.
Legislação e regulamentações (GDPR e LGPD)	BÖYÜK, M.; FUCHS, C.; ZUBOFF, S.
Medidas técnicas de proteção de dados (criptografia, DLP, SIEM, etc.)	BÖYÜK, M.; IBSEC; CYERA
Engenharia social e riscos de segurança com terceiros	STEEL, A.; BÖYÜK, M.

Fonte: SILVA, Pedro (2025)

3. ANÁLISE DE DADOS

Este capítulo apresentará como as redes sociais utilizam as informações dos usuários, muitas vezes sem que eles percebam. Explica sobre o tempo gasto nas plataformas, vazamentos de dados, formas de influenciar o comportamento dos usuários e a dificuldade que muitos têm para entender os termos de uso. A análise se baseia em estudos que ajudam a entender esses problemas.

3.1. Tempo de uso dos usuários nas redes sociais e seu engajamento nessas plataformas.

Do ponto de vista quantitativo, todas as plataformas empregam algoritmos e designs com o objetivo claro de maximizar o tempo de uso e manter a atenção do usuário pelo maior período possível. Os dados de utilização confirmam a eficácia dessa estratégia, os usuários de redes sociais passam horas por dia engajados, em grande parte motivados por conteúdos recomendados algoritmicamente.

Figura 3 – Tempo médio diário de uso por plataforma (estimativas globais, 2022-2023)

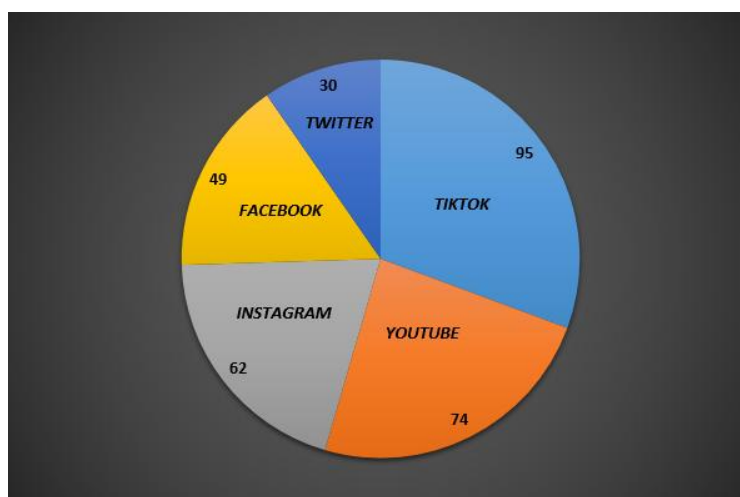
Plataforma	Tempo médio por usuário	Observações sobre engajamento
TikTok	95 minutos / dia	Feed "For You" algorítmico, vídeos curtos em rolagem infinita geram engajamento altamente viciante.
YouTube	74 minutos / dia	70% do conteúdo assistido é sugerido pelo algoritmo; reprodução automática mantém sessões > 60 minutos
Instagram	62 minutos / dia	Feed algorítmico personalizado e Stories/Reels em sequência contínua elevam o tempo na aplicação.
Facebook	49 minutos / dia	News Feed infinito com posts recomendados; embora menor que TikTok, ainda retém usuários por longos períodos.
Twitter (X)	30 minutos / dia	Timeline mista (seguidores e recomendações no "Para você"); uso mais breve, porém recargas frequentes (scroll contínuo).

Fonte: (DEIGHTON, KORNFELD, 2022; BACKLINKO, 2025)

Os números da figura 3 evidenciam a onipresença de uma interação impulsionada algorítmico. O destaque fica por conta do *TikTok*, cujos usuários ficam em média 1 hora e 35 minutos por dia no app liderando entre as redes sociais (DEIGHTON, KORNFELD, 2022). Esse tempo excede em muito plataformas tradicionais, na mesma métrica global, o *YouTube* mantém usuários por cerca de 74

minutos diários, e o *Instagram* por 62 minutos (BACKLINKO, 2025). Mesmo o *Facebook*, com público mais velho, ainda registra em torno de 45–50 minutos diários por usuário em média (DEIGHTON, KORNFELD, 2022).

Figura 3.1 – Tempo médio diário de uso por plataforma em formato de gráfico



Fonte: (DEIGHTON, KORNFELD, 2022; BACKLINKO, 2025)

Tais níveis de uso só são possíveis graças aos algoritmos de recomendação que alimentam um fluxo constante de conteúdo atraente, mantendo o usuário conectado. No *YouTube*, estima-se que 70% de todo o conteúdo assistido na plataforma é proveniente de recomendações automáticas, seja na página inicial ou na barra de vídeos sugeridos (RODRIGUEZ, 2018). Essas recomendações são muitas vezes personalizadas e calculadas pelo sistema de inteligência artificial do *Google*, de modo que um usuário quase sempre encontrará algo de interesse sem precisar sair procurando.

Consequentemente, sessões móveis no *YouTube* frequentemente ultrapassam 60 minutos ininterruptos graças a essa curadoria algorítmica (RODRIGUEZ, 2018). A função de reprodução automática para o próximo vídeo e a lista infinita de sugestões levam o usuário de um vídeo a outro, prolongando significativamente seu tempo de permanência. Essa mecânica de rolagem vertical interminável combinada com o aprendizado de máquina, que entende rapidamente as preferências do usuário, resulta em um ciclo do qual “é difícil sair” (DEIGHTON, KORNFELD, 2022). Estudos

apontam que essa experiência de recompensas frequentes gera uma reação comportamental semelhante à de vício, pequenos estímulos contínuos que prendem a atenção por muito mais tempo do que o intencionado (BURCH, 2025).

3.2. Vazamento de dados em redes sociais

Como apresentado anteriormente, nos últimos anos, as principais redes sociais, como *Facebook*, *Instagram*, *TikTok*, *Twitter (X)* e *YouTube*, registraram elevados índices de tempo de uso diário. Simultaneamente, essas plataformas também enfrentaram incidentes significativos de vazamento de dados de usuários.

Figura 4 – Vazamentos e exposições de dados em plataformas sociais

Plataforma	Incidente (ano)	Usuários afetados	Fonte
Facebook	Vazamento de dados (2019; revelado em 2021)	533 milhões	NORDVPN (2021)
Instagram	Scraping e venda de dados (nov. 2024)	489 milhões	CYBERPRESS (2024)
Instagram	Exposição de 17 milhões de contas (jan. 2025)	17 milhões	CYBERPRESS (2025)
Twitter (X)	Vazamento e divulgação em fórum (jan. 2023)	200 milhões	HINDUSTAN TIMES (2025)
TikTok	Scraping de perfis públicos (2020) e alegação negada (2022)	42 milhões (scraping) e 2 bilhões (alegação)	COMPARITECH (2020); WINDER (2022)
YouTube	Scraping de perfis públicos (2020)	4 milhões	COMPARITECH (2020)

Fonte: elaboração própria a partir de NORDVPN (2021), CYBERPRESS (2024; 2025), HINDUSTAN TIMES (2025), COMPARITECH (2020) e WINDER (2022).

Como apresentado na figura 4, as principais plataformas sociais registraram exposições de dados nos últimos anos. O *Facebook* sofreu um vazamento em 2019, revelado em 2021, com 533 milhões de perfis expostos, correspondendo a cerca de 20% da base global (NORDVPN, 2021). O *Instagram* teve 489 milhões de registros obtidos por *scraping* (raspagem de dados), que funciona a partir da extração automática de informações, em novembro de 2024, cerca de 25% dos usuários, seguido por novo vazamento de 17 milhões de contas em janeiro de 2025 (CYBERPRESS, 2024; 2025).

Em janeiro de 2023, o *Twitter* (atual *X*) viu a divulgação de uma base com 200 milhões de perfis, o que representa mais de metade de sua base ativa (HINDUSTAN

TIMES, 2025). O *TikTok* não teve nenhum vazamento interno confirmado, mas houve um *scraping* de 42 milhões de perfis em 2020 e uma alegação de 2 bilhões de registros em 2022, negada pela empresa (COMPARITECH, 2020; WINDER, 2022).

Por fim, o *YouTube* teve pouco menos de 4 milhões de perfis coletados por *scraping* em 2020, menos de 1% de seus mais de 2 bilhões de usuários (COMPARITECH, 2020).

3.3. Manipulação do comportamento de usuários em redes sociais

Embora a extensão do tempo de uso seja um dos resultados mais visíveis das estratégias algorítmicas, o impacto vai além, as plataformas moldam ativamente padrões de comportamento e decisão. O *TikTok*, *Instagram* e *YouTube* não apenas sugerem conteúdo, mas estruturam toda a experiência do usuário com o objetivo de condicionar hábitos e preferências de consumo. O Chief Product Officer (CPO) do *YouTube* revelou que aproximadamente 70% do tempo de exibição decorre de recomendações algorítmicas, evidenciando a centralidade do sistema de sugestões na experiência da plataforma (MOHAN, 2018).

No *Instagram*, a implementação do *feed* é baseado em inteligência artificial e aumentou em 24% do tempo total gasto, revelando a eficácia do design persuasivo (ETHERINGTON, 2023). Pequenas manipulações na apresentação do conteúdo, como o destaque para vídeos ou posts de alto apelo emocional, reforçam respostas impulsivas, desviando o comportamento do usuário para rotinas de consumo reiterativo (ZUBOFF, 2019).

Além disso, a prática de *microtargeting* alcançou novos níveis de precisão. Estudos recentes demonstram que mensagens personalizadas, ajustadas a características psicográficas específicas (como idade, valores pessoais ou inclinações políticas), podem ser até 70% mais eficazes na indução de ações do que mensagens genéricas (TAPPIN et al., 2023). Essa capacidade de segmentação minuciosa transforma as redes sociais em ambientes propícios à manipulação comportamental em larga escala, adaptando estímulos e persuasões a cada perfil individual.

Desse modo, não se trata apenas de manter o usuário conectado por mais tempo, mas de cultivar padrões habituais de interação, orientar preferências e

influenciar decisões, inserindo o comportamento individual dentro dos ciclos econômicos do capitalismo de vigilância (ZUBOFF, 2019). As redes sociais não apenas captam atenção, elas moldam o que as pessoas desejam, consomem e até mesmo pensam, em benefício dos interesses comerciais que dominam suas arquiteturas invisíveis de controle.

3.4. Compreensão dos termos de uso de redes sociais

Um levantamento do laboratório *Pew Research Center* revelou que 56% dos entrevistados frequentemente clicam em “concordo” sem ler o conteúdo dos contratos de privacidade (MCCLAIN et al., 2023). Essas estatísticas confirmam que os termos de serviço são longos e complexos, restringindo a verdadeira compreensão dos direitos cedidos pelos usuários.

Figura 5 - Métricas referente aos termos de serviço das redes sociais

Plataforma	Total de palavras	Páginas (aprox.)	Índice Flesch-Kincaid (grau escolar)	Tempo estimado de leitura
TikTok	7.412	25	15 (nível universitário)	30 minutos
Instagram	3.305	11	12 (nível superior médio)	13 minutos
Facebook	5.091	17	14 (nível universitário)	20 minutos
YouTube	3.801	13	12 (nível superior médio)	15 minutos

Fonte: (VPNOVERVIEW, 2023).

Conforme ilustrado na Figura 5, mesmo as políticas de privacidade mais concisas, como a do *Instagram*, com cerca de 11 páginas, podem demandar mais de dez minutos para leitura completa, enquanto a mais extensa, do *TikTok*, requer aproximadamente 30 minutos. Além da extensão, a complexidade linguística desses documentos é elevada, frequentemente exigindo um nível de compreensão equivalente ao universitário, o que dificulta sua leitura pelo público geral. Pesquisas indicam que apenas 9% dos adultos sempre leem os termos antes de aceitá-los, enquanto 36% admitem nunca os ler (AUXIER et al., 2019).

3.5. Critérios de seleção, análise e discussão dos artigos

Shoshana Zuboff, Christian Fuchs e Mustafa Böyük, foram os principais autores selecionados para o desenvolvimento desta monografia. Zuboff foi selecionada por conceituar o capitalismo de vigilância, destacando como grandes corporações transformam dados pessoais em matéria-prima valiosa. Fuchs, por sua vez, oferece uma análise marxista do trabalho digital, enfocando a exploração da atividade dos usuários (prosumidores) e dos trabalhadores de mídia digital. Böyük não trouxe nenhuma teoria própria para seu artigo, mas enfatizou o caráter lúdico e crítico das interações nas redes sociais. Eles foram escolhidos por abordarem dimensões complementares, Zuboff foca na extração de valor via dados, Fuchs no papel do trabalho e da teoria do valor, e Böyük na dimensão cultural e comunicacional das plataformas.

Na perspectiva de capitalismo de vigilância, ZUBOFF (2019) argumenta que vivemos um novo estágio do capitalismo informacional em que a tecnologia é usada para prever e modificar o comportamento humano com o objetivo de gerar lucro e controle de mercado. Em suas palavras, empresas como *Google* e *Facebook* “reivindicam unilateralmente a experiência humana como matéria-prima gratuita para tradução em dados comportamentais”. Estudos corroboram que essas empresas coletam massivamente dados dos usuários não apenas para melhorar serviços, mas principalmente para influenciar comportamentos. Assim, Zuboff destaca a lógica parasítica desse modelo como a “experiência humana” é expropriada em benefício das plataformas, constituindo uma ameaça à privacidade e à democracia.

Por outro lado, FUCHS (2014) analisa o trabalho digital sob uma ótica marxista. Para ele, os dados produzidos pelos usuários são efetivamente mercadorias vendidas a anunciantes, cujo valor excedente é criado tanto pelos funcionários das empresas quanto pela atividade gratuita dos próprios usuários. Fuchs enfatiza que os usuários são “infinitamente explorados” porque não recebem pagamento por suas contribuições. Em outras palavras, cada postagem, *like* ou compartilhamento constitui um trabalho imaterial não remunerado que sustenta a acumulação de capital nas plataformas.

Nesse sentido, existe um encontro com a teoria de Zuboff, ambos veem as plataformas digitais como máquinas de extração, Zuboff a partir dos dados comportamentais, Fuchs a partir do trabalho gratuito dos usuários e dos trabalhadores de mídia. Contudo, divergem na ênfase teórica, Zuboff destaca a dimensão novelística e institucional do fenômeno enquanto Fuchs fundamenta sua crítica na teoria de valor marxista, enfocando a exploração do trabalho e a geração de mais-valia pelos usuários.

A partir de análise de conteúdo em várias redes sociais, Böyük e Zuboff concluem que as mídias sociais se tornaram mais que meros canais de informação, assumindo um papel crucial de expressão cultural e interação social. Essa abordagem destaca a agência dos usuários como produtores de cultura digital, mas com foco nas dinâmicas simbólicas e não diretamente na extração econômica. Comparando as visões, nota-se convergência quanto ao diagnóstico de que as plataformas capturam valor dos usuários. Zuboff e Fuchs concordam que os usuários produzem recursos valiosos que sustentam o lucro das *Big Techs*.

Em contrapartida, divergem em alguns pontos, Zuboff conceitua tal processo como um novo estágio do capitalismo que exige regulação social ampla, enquanto Fuchs mantém o debate no âmbito teórico marxista clássico, enfatizando a crítica à mercadoria e ao trabalho não pago. Böyük complementa ao enfatizar que esse processo não é apenas econômico, mas também cultural, na qual o entretenimento e a crítica social convivem.

Os resultados empíricos deste trabalho apontam que as ideias de Zuboff e Fuchs se mostram consistentes com as evidências coletadas. Observou-se, por exemplo, que as políticas de dados das plataformas de fato permitem a coleta extensiva de informações pessoais, confirmando que “a experiência humana se torna matéria-prima mercantilizada” e que os usuários geram grande volume de conteúdo voluntário sem remuneração, alinhando-se à noção de exploração de trabalho gratuito. No entanto, o material empírico concentrou-se principalmente na dinâmica de poder e privacidade dos dados, conferindo mais peso às explicações de Zuboff e Fuchs.

Ao analisarmos os artigos entre si, é possível identificar que eles se complementam, Zuboff e Fuchs oferecem bases explicativas para os mecanismos de

extração de valor, enquanto Böyük ilumina como tais mecanismos se manifestam na cultura digital cotidiana. Assim, uma convergência emerge na crítica geral às desigualdades criadas pelas plataformas, mas cada autor focaliza aspectos distintos desse fenômeno.

Quanto aos pontos fortes, Zuboff fornece um quadro conceitual de grande abrangência, tornando acessível a ideia de uma “nova ordem econômica” e sinalizando a urgência de contramedidas democráticas. Sua narrativa sobre o “capitalismo de vigilância” popularizou o tema, mas também é criticada por alguns por não detalhar soluções práticas e por ter um caráter às vezes alarmista.

Fuchs, por outro lado, é elogiado pela riqueza teórica e pelo rigor marxista na análise do trabalho digital. Seu argumento de que os usuários são explorados de forma inédita é instigante, mas já foi questionado, críticos apontam que Fuchs apresenta certa inconsistência ao atribuir valor diretamente à atividade dos usuários, sem esclarecer se os dados eram mercadoria antes de seu processamento algorítmico. Essa complexidade teórica pode tornar sua abordagem pouco acessível a não-especialistas.

Böyük traz o ponto forte de destacar o papel cultural e comunitário das redes sociais, enfatizando sua função comunicacional e crítica. Sua análise qualitativa enriquece o debate com um olhar social, porém é limitada metodologicamente, portanto, não substitui estudos sobre poder corporativo ou impactos laborais.

Figura 6 – Quadro comparativo das abordagens teóricas de Zuboff, Fuchs e Böyük

Autor	Principais ideias/teorias	Pontos fortes	Limitações percebidas
Shoshana Zuboff	Capitalismo de vigilância, experiência humana como matéria-prima dos dados; monitoramento e modificação do comportamento para lucro.	Abordagem ampla e fundamentada; introduziu conceito-chave e estimulou debates públicos.	Visão macro e conceitual; críticas por amplo escopo (pouca especificidade sobre processos internos) e falta de propostas práticas detalhadas.
Christian Fuchs	Trabalho digital e marxismo, dados de usuários como mercadoria; exploração do trabalho não-remunerado dos prosumers.	Rigor teórico, fundamentado em Marx; explicita a dimensão laboral da economia digital.	Abordagem densa e abstrata; discussão sobre valor dos dados e natureza do trabalho digital é controversa; linguagem técnica.
Mustafa Böyük	Nenhuma teoria introduzida na fundamentação	Perspectiva original e cultural; destaca a agência dos usuários e dinâmicas de comunicação.	Foco limitado a aspectos culturais; análise centrada em exemplos específicos; não aborda diretamente a economia política ou privacidade dos dados.

Fonte: SILVA, Pedro (2025)

Em suma, a análise crítica revela que as ideias de Zuboff e Fuchs parecem mais centrais à dinâmica de poder observada nas plataformas digitais, especialmente no que concerne à captura de dados e à exploração do trabalho do usuário. A contribuição de Böyük, embora menos voltada à economia política, ajuda a contextualizar como essas dinâmicas afetam a cultura digital.

4. CONCLUSÃO

Os resultados mostram que, embora os termos de privacidade atendam formalmente às exigências da lei, eles continuam sendo complicados e difíceis de entender para a maioria das pessoas. Isso reforça a ideia de que o consentimento dado nesses casos é, muitas vezes, mais uma ilusão do que uma escolha real e consciente. Ou seja, os resultados corroboram para a hipótese de “ilusão de consentimento”.

Paralelamente, casos de vazamento de dados e análises de processos algorítmicos apontam para a fragilidade das medidas de proteção atualmente empregadas, evidenciando que a coleta e o uso excessivo dos dados não apenas comprometem a segurança das informações pessoais, mas também afetam o comportamento dos indivíduos de maneiras frequentemente sutis e imperceptíveis.

Assim, tais informações confirmam ambas as hipóteses propostas no início desta monografia, demonstrando que a coleta e o uso excessivo dos dados não apenas comprometem a segurança das informações pessoais, mas também influenciam o comportamento dos usuários em níveis muitas vezes imperceptíveis.

As ideias de autores como Zuboff, Fuchs e Böyük, trouxeram uma visão mais ampla e integrada, em que fatores econômicos, culturais e comportamentais se conectam de maneira orgânica na formação desse novo cenário digital.

Com base nestes resultados, propõe-se que futuras investigações aprofundem a análise dos efeitos dos algoritmos sobre graduações comportamentais em contextos diversificados, ampliando a amostra e explorando outras perspectivas sobre a interface entre tecnologia, legislação e consciência do usuário.

Este trabalho, ao contribuir para o debate sobre a proteção de dados e a transparência nas práticas digitais, sugere a necessidade de aprimoramento das políticas públicas e de soluções tecnológicas que promovam uma experiência digital mais ética e segura.

Em última análise, é esperado que as reflexões apresentadas nesta monografia inspirem tanto o setor acadêmico quanto os profissionais da área a repensarem e reformularem os mecanismos de proteção e de controle das informações no ambiente virtual, fortalecendo a cidadania digital e a autonomia dos usuários.

5. REFERÊNCIAS

AUXIER, Brooke; RAINIE, Lee; ANDERSON, Monica; PERRIN, Andrew; KUMAR, Madhu; TURNER, Erica. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Washington, D.C.: Pew Research Center, 15 nov. 2019. Disponível em: <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>. Acesso em: 28 abr. 2025.

BACKLINKO. TikTok Statistics You Need to Know in 2025. Disponível em: <https://backlinko.com/tiktok-users>. Acesso em: 28 abr. 2025.

BÖYÜK, Mustafa. User Data and Digital Privacy: Privacy Policies of Social Media Platforms. The Turkish Online Journal of Design, Art and Communication, v.15, n.1, p.225-239, dez. 2024.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BURCH, Sean. TikTok users spend twice as much time on the app as Instagram users spend on Instagram. TheWrap, 8 abr. 2025. Disponível em: <https://www.thewrap.com/tiktok-users-spend-twice-time-instagram>. Acesso em: 28 abr. 2025.

CARDOSO, Breno. Navegador do TikTok consegue rastrear comandos de teclado, revela pesquisa. MacMagazine, 19 ago. 2022. Disponível em: <https://macmagazine.com.br/post/2022/08/19/navegador-do-tiktok-consegue-rastrear-comandos-de-teclado-revela-pesquisa/>. Acesso em: 12 abr. 2025.

COMPARITECH. 235M Social Media Accounts From Instagram, TikTok and YouTube Exposed. Comparitech, 19 ago. 2020. Disponível em: <https://www.spiceworks.com/it-security/data-security/news/235m-social-media-accounts-from-instagram-tiktok-and-youtube-exposed/>. Acesso em: 10 abr. 2025.

CORASSA, Eugênio. A maior mentira da internet: “Li e aceito” e o papel dos termos de uso. Startups, 13 jun. 2024. Disponível em: <https://startups.com.br/coluna/a-maior-mentira-da-internet-li-e-aceito-e-o-papel-dos-termos-de-uso/>. Acesso em: 13 abr. 2025.

CYBERPRESS. Instagram Data Breach Sparks Global Privacy Concerns. CyberPress, 10 jan. 2025. Disponível em: <https://cyberpress.org/instagram-data-breach/>. Acesso em: 10 abr. 2025.

CYBERPRESS. Threat Actor Allegedly Claims Leak of 489 Million Lines of Instagram Data. CyberPress, 11 nov. 2024. Disponível em: <https://cyberpress.org/leak-of-489-million-instagram-data/>. Acesso em: 10 abr. 2025.

CYERA. Data Breach Mitigation: Seven Effective Strategies. 2023. Disponível em: <https://www.cyera.io/blog/data-breach-mitigation>. Acesso em: 13 abr. 2025.

DEIGHTON, John; KORNFIELD, Leora. Why TikTok is beating YouTube for eyeball time (It's not just the dance videos). Harvard Business School Working Knowledge, 15 nov. 2022. Disponível em: <https://www.library.hbs.edu/working-knowledge/why-tiktok-is-beating-youtube-for-eyeball-time>. Acesso em: 28 abr. 2025.

ETHERINGTON, Darrell. Instagram's AI-powered Reels Recommendations Are Boosting User Time Spent by 24%. TechCrunch, 2023. Disponível em: <https://techcrunch.com>. Acesso em: 28 abr. 2025.

FIRE, M. et al. Online Social Networks: Threats and Solutions. ACM Communications, 2014.

FUCHS, Christian. Social Media: A Critical Introduction. 2. ed. Londres: SAGE Publications, 2014.

FUCHS, Christian. Social Media: A Critical Introduction. 2. ed. Londres: SAGE Publications, 2021.

HINDUSTAN TIMES. Hacker claims over 200 million X users data leaked: Report. Hindustan Times, 23 jan. 2025. Disponível em: <https://www.hindustantimes.com/world-news/hacker-claims-over-200-million-x-users-data-leaked-report-101743592069973.html>. Acesso em: 10 abr. 2025.

IBSEC. 10 práticas para administrar senhas corporativas. IBSEC, 17 out. 2024. Disponível em: <https://ibsec.com.br/10-praticas-para-administrar-senhas-corporativas/>. Acesso em: 13 abr. 2025.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. Pittsburgh: Carnegie Mellon University, 2008. Disponível em: https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab06017.pdf. Acesso em: 13 abr. 2025.

MCCLAIN, C.; FAVERIO, M.; ANDERSON, M.; PARK, E. How Americans View Data Privacy: The Role of Technology Companies, AI and Regulation—Plus Personal Experiences with Data Breaches, Passwords, Cybersecurity and Privacy Policies. Washington, D.C.: Pew Research Center, 18 out. 2023. Disponível em: <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>. Acesso em: 28 abr. 2025.

MILNE, Stefan. Q&A: How TikTok's 'black box' algorithm and design shape user behavior. UW News, 24 abr. 2024. Disponível em: <https://www.washington.edu/news/2024/04/24/tiktok-black-box-algorithm-and-design-user-behavior-recommendation/>. Acesso em: 12 abr. 2025.

MOHAN, Neal. How YouTube's Algorithm Really Works. Wired, 2018.

Disponível em: <https://www.wired.com/story/how-youtube-algorithm-works/>. Acesso em: 28 abr. 2025.

NORDVPN. Facebook Data Breaches: Investigating Top Data Leaks. NordVPN Blog, 26 abr. 2021. Disponível em: <https://nordvpn.com/blog/facebook-data-breach/>. Acesso em: 10 abr. 2025.

PRIVACYTOOLS. Textos longos nas políticas de privacidade são um problema. PrivacyTools, 2 jun. 2022. Disponível em: <https://www.privacytools.com.br/texto-politicas/>. Acesso em: 13 abr. 2025.

REUTERS. Twitter urges all users to change passwords after glitch. 2018. Disponível em: <https://www.reuters.com/article/technology/twitter-urges-all-users-to-change-passwords-after-glitch-idUSKBN1I42JA/>. Acesso em: 13 abr. 2025.

SOLOVE, Daniel J. Understanding Privacy. Cambridge: Harvard University Press, 2009.

STEEL, Amber. Proteja sua empresa contra engenharia social com chaves de acesso. LastPass Blog, 31 out. 2023. Disponível em: <https://blog.lastpass.com/pt/posts/protecting-your-business-from-social-engineering-with-passkeys>. Acesso em: 13 abr. 2025.

TAPPIN, Ben M.; BLUMENTHAL-BARBY, Jennifer S.; ALBERY, Ian P. Personalized persuasive messaging is highly effective: evidence from a mega-study. Nature Human Behaviour, v. 7, p. 129–138, 2023.

THALER, Richard H.; SUNSTEIN, Cass R. Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven: Yale University Press, 2008.

THE GUARDIAN. YouTube fined \$170m for collecting children's personal data. 2019. Disponível em: <https://www.theguardian.com/technology/2019/sep/04/youtube-kids-fine-personal-data-collection-children>. Acesso em: 13 abr. 2025.

THE VERGE. TikTok will pay \$5.7 million over alleged children's privacy law violations. 2019. Disponível em: <https://www.theverge.com/2019/2/27/18243312>