



**Universidade de Brasília - UnB**  
Faculdade de Comunicação  
Curso de Comunicação Organizacional

Trabalho de Conclusão de Curso

**VIGILÂNCIA DE DADOS: A PERCEPÇÃO DO ESTUDANTE DE  
GRADUAÇÃO DA UNIVERSIDADE DE BRASÍLIA SOBRE A COLETA E  
VIGILÂNCIA DE DADOS NO APLICATIVO DE MENSAGENS WHATSAPP**

Luíza Ribeiro de Menezes Souza

17/0040577

Brasília

2022

LUÍZA RIBEIRO DE MENEZES SOUZA

**VIGILÂNCIA DE DADOS: A PERCEPÇÃO DO ESTUDANTE DE  
GRADUAÇÃO DA UNIVERSIDADE DE BRASÍLIA SOBRE A COLETA E  
VIGILÂNCIA DE DADOS NO APLICATIVO DE MENSAGENS WHATSAPP**

Monografia apresentada à Faculdade de Comunicação, da Universidade de Brasília, como requisito parcial para a obtenção do grau de Bacharel em Comunicação Social com habilitação em Comunicação Organizacional.

Orientadora: Elen Cristina Gerales

BRASÍLIA

2022

LUÍZA RIBEIRO DE MENEZES SOUZA

**VIGILÂNCIA DE DADOS: A PERCEPÇÃO DO ESTUDANTE DE  
GRADUAÇÃO DA UNIVERSIDADE DE BRASÍLIA SOBRE A COLETA E  
VIGILÂNCIA DE DADOS NO APLICATIVO DE MENSAGENS WHATSAPP**

Monografia apresentada à Faculdade de Comunicação, da  
Universidade de Brasília, como requisito parcial  
para a obtenção do grau de Bacharel em  
Comunicação Social com habilitação em  
Comunicação Organizacional.

Aprovada em \_\_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

**BANCA EXAMINADORA**

---

Profa. Elen Cristina Geraldês

**ORIENTADOR**

---

Prof. Marcos Urupá

**BANCA**

---

Profa. Janara Sousa

**BANCA**

---

Profa. Mariah Sampaio

**SUPLENTE**

## AGRADECIMENTOS

O desafio de fazer uma graduação é sempre dividido com várias pessoas, tive o privilégio de poder me encontrar em outra área de conhecimento e nada seria possível se não tivesse o apoio incondicional da minha família, em especial, minha mãe, que sempre fez absolutamente tudo para que eu pudesse colocar minhas energias no que realmente me faria feliz. Sempre foi minha fonte de determinação, me ensinou a ser doce e forte, a valorizar todo o aprendizado e a dar o meu melhor em tudo.

Aos amigos que eu conheci nessa caminhada, que por várias vezes foram essenciais para que não me sentisse sozinha em meio a tantas mudanças que passamos. Ao Lucas Fernandes e Lucas Neves, que dividiram esses últimos meses de faculdade comigo, que torceram e estavam sempre ali para dividir as dores e alegrias desse processo. À minha primeira amiga da UnB, Mila Oliveira, que sempre se mostrou presente e disponível mesmo estando em outro país! Às meninas do “*la noche mexicana*”, que por muitas vezes foram minha fonte de riso e alívio, é sempre bom saber que conseguimos construir amizades que vão além dessa fase. Aos meus amigos de voluntariado, em especial, o Pedro Azevedo, a única pessoa que acompanha o meu humor e segue qualquer piada que solto, obrigada por tudo, você é essencial na minha vida. Por fim, ao amigo João Victor Sampaio, que se doou e dedicou horas para me ajudar nesse trabalho, você foi incrível. Obrigada a todos.

Elen, a melhor orientadora que eu poderia escolher, obrigada por todo carinho que colocou em cada reunião e correção, por se fazer presente e nos dar a segurança de continuar. Seu trabalho me inspira e desejo que mais alunos possam ser tocados com o seu jeito tão humano de lidar com os desafios da graduação.

Também quero agradecer à Universidade de Brasília, que sempre foi um sonho até mesmo quando eu não sonhava em estar ali, foram anos de vivências que comprovaram a importância da universidade pública de qualidade para toda a sociedade. Obrigada a todos os professores que, mesmo com tantos desafios e descaso de um governo assombroso, continuam acreditando na educação.

## **Resumo**

As redes sociais já se tornaram uma extensão da vida em sociedade. Nesse cenário, as empresas encontraram um ambiente para a coleta e vigilância de dados a fim de construir perfis de consumo com potencial de modificar desejos e ações. Recentemente, o aplicativo de mensagens WhatsApp alterou sua política de privacidade para introduzir a versão *Business*, direcionada às empresas, e com essas modificações os riscos à violação de direitos e liberdades se tornaram mais evidentes. O trabalho, por meio de uma revisão bibliográfica e pesquisa quantitativa, buscou compreender a importância da proteção de dados e identificar qual o conhecimento de estudantes da Universidade de Brasília sobre o assunto. Os resultados demonstraram que mesmo os estudantes, que se constituem em perfil de usuários ativos e constantes da internet, ainda possuem conhecimento raso sobre o tema, além de certa resistência em aprofundá-lo.

**Palavras-chave:** proteção de dados pessoais; vigilância de dados; políticas de comunicação

**Abstract**

Social networks have already become an extension of life in society. In this scenario, companies found an environment for data collection and surveillance in order to build consumption profiles with the potential to modify desires and actions. Recently, the messaging application WhatsApp has changed its privacy policy to introduce the Business version, aimed at companies, and with these changes the risks of violating rights and freedoms have become more evident. The work, through a literature review and quantitative research, sought to understand the importance of data protection and identify the knowledge of students at the University of Brasília on the subject. The results showed that even students, who constitute a profile of active and constant users of the internet, still have shallow knowledge about the subject, in addition to some resistance to deepening it.

**Keywords: Personal data protection; data surveillance; communication policies**

# SUMÁRIO

<b>1. INTRODUÇÃO .....</b>	<b>8</b>
<b>CAPÍTULO 1: EM BUSCA DE ANTECEDENTES .....</b>	<b>12</b>
<b>CAPÍTULO 2: REVISÃO CONCEITUAL .....</b>	<b>19</b>
<b>2.1. O início e a evolução do WhatsApp .....</b>	<b>19</b>
2.1.1 Alterações da política de privacidade .....	20
<b>2.2. Vigilância digital .....</b>	<b>25</b>
2.2.1 O objeto da vigilância do WhatsApp: os metadados .....	27
<b>2.3. Direito à privacidade .....</b>	<b>30</b>
<b>CAPÍTULO 3 PESQUISA EMPÍRICA .....</b>	<b>33</b>
3.1 O questionário .....	33
3.2 Análise dos dados .....	34
<b>4. CONSIDERAÇÕES FINAIS .....</b>	<b>45</b>
<b>REFERÊNCIAS .....</b>	<b>48</b>
<b>APÊNDICE .....</b>	<b>54</b>

## 1. INTRODUÇÃO

A internet, que surgiu a partir de tentativas de avanços tecnológicos durante a guerra fria (CASTELLS, 2020), hoje é parte fundamental para a vivência de diversas funções na sociedade, desde facilitar o acesso a direitos a fazer com que os indivíduos sintam-se parte de um grupo. A rede mundial de computadores está cada vez mais onipresente no cotidiano das pessoas e, embora uma parte da população do planeta viva sem esses recursos, a conectividade online tornou-se tão necessária que é difícil imaginar uma realidade sem esses aportes tecnológicos, sobretudo entre a população jovem, urbana e de classe média.

Por anos, o crescimento da internet e os avanços tecnológicos foram encarados como inevitáveis. Curran (2016) explica que, com a entrada da internet no mercado, em meados de 1990, existia certo fascínio exótico pelo tema e os estudos que abordavam sobre suas funcionalidades pareciam comparar a ideia de “ciberespaço” a romances de ficção científica. As maravilhas da internet e a corrida por fazer parte desse momento histórico suscitaram visões amplamente acríicas sobre esse universo.

Uma grande parcela de trabalhadores e trabalhadoras tiveram que se adaptar às necessidades desse momento de mudanças e buscaram se posicionar no ambiente virtual o mais rápido possível. Três décadas depois, o Brasil tornou-se o terceiro país dentre os pesquisados que mais consome online. Em levantamento realizado pela Mastercard (2021), por exemplo, o crescimento de empresas que migraram para o ambiente virtual em 2020 ultrapassou os 200% em comparação ao ano anterior.

Esse movimento do offline para o online causa uma falsa impressão de que a população brasileira possui o mesmo nível de acesso ao ambiente virtual, sugerindo que a rede é um espaço mais democrático, mas a realidade do acesso à internet no Brasil é de atraso.

Em dados obtidos pela *Pesquisa Nacional por Amostra de Domicílio Contínua: Tecnologia da Informação e Comunicação*, divulgada pelo IBGE em 2019, ano anterior ao início da pandemia de covid-19, mais de 12 milhões de famílias ainda não possuíam acesso à internet. Além disso, 39,8 milhões de brasileiros com 10 anos ou mais não usavam a rede, sendo que nas classes C e D o percentual de desconectados alcança 59%. Se a análise for feita de acordo com as regiões do país, o Norte e Nordeste concentram 54,3% e 52,3%, respectivamente, de pessoas sem acesso à internet. (VIEIRA, 2021)

Esses dados indicam que, apesar das mudanças tão rápidas e avanços tecnológicos contínuos, a inclusão digital no Brasil ainda é um desafio que gera outras complicações para parte considerável dos brasileiros. Ao entregar tantas possibilidades sem permitir que seus

usuários tenham conhecimento e, principalmente, conscientização sobre as suas vantagens e riscos, abrem-se as portas para abusos por parte das grandes empresas de tecnologia.

Uma das mais recentes preocupações está na coleta e utilização dos dados pessoais retirados de interações na internet, que ganharam mais visibilidade após o início da vigência da Lei Geral de Proteção de Dados (Lei 13.709/2018), inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Para ser aprovada, a LGPD precisou de anos de elaboração, melhorias dos projetos de leis, várias tentativas de ser sancionada e finalmente entrou em vigor em 2021. Durante sua elaboração, o legislador não procurou inviabilizar negócios digitais que usam da personalização de seu conteúdo para chegar de maneira mais certa em seus consumidores, mas garantir a transparência e o cumprimento dos direitos de seus titulares.

O objetivo de regular a internet não tem relação com impedir ou inibir o seu potencial, é o que se constata a partir do Marco Civil da Internet; mas deixar claro aos cidadãos sobre os limites das ações das empresas no mundo digital, a necessidade da transparência nos termos de uso e, principalmente, que os termos utilizados para explicar o consentimento sejam acessíveis. Em fevereiro a proteção de dados recebeu ainda mais atenção, pois foi acrescentado ao rol de direitos e garantias fundamentais ao cidadão o direito à privacidade e à proteção dos seus dados pessoais, vistos como essencial para a vida plena e digna das pessoas.

Embora seja comum ouvir “se você não tem nada a esconder, você não tem nada a temer”, quando se questiona pessoas comuns sobre a importância da proteção de seus dados pessoais, esse posicionamento pode ser fundamentado em uma falta de conhecimento sobre o poder dessas “pequenas informações” que, talvez soltas, parecem não dizer muito sobre seu titular, mas quando conectadas podem ser ferramenta de vigilância que fere o direito de privacidade e induz a ações e manipulações das quais o usuário não possui controle.

Os dados pessoais são considerados atualmente o petróleo do século XXI (THE ECONOMIST, 2017), sua capitalização tornou-se o principal objeto de trabalho de diversas empresas que não exercem apenas o serviço que entregam ao seu consumidor final, mas se tornaram verdadeiras empresas de análise de dados e, talvez o mais preocupante, dominam a vida de uma parcela enorme de usuários. Nesse contexto, é possível se falar em uma colonização de dados, tal como o colonialismo histórico explorou terras e pessoas, a colonização de dados explora e monetiza a vida dos usuários (COULDRY; MEJIAS, 2019).

Trazendo esses fatos para o cenário atual, o isolamento de grande parte da população devido à pandemia de covid-19 e, conseqüentemente, o aumento de tempo gasto nas

plataformas online apenas colaboraram para a entrega e a concentração de mais dados pessoais em empresas que dominam o mercado. É o caso dos aplicativos da empresa-mãe *Meta Platforms, Inc.* (antiga Facebook), entre esses o WhatsApp.

Em janeiro de 2021, o WhatsApp notificou seus usuários sobre as atualizações em seu termo de uso. Algumas mudanças começaram logo após a compra do aplicativo pelo Facebook, mas a que mais chama atenção é a obrigatoriedade em compartilhar, entre todos os aplicativos da empresa Meta, as conversas realizadas com empresas que usam o WhatsApp Business e que contrataram o Facebook para gerenciar a comunicação entre elas e o usuário. Dessa forma, entra em suspeição a principal ferramenta para proteção dos dados dos usuários, a criptografia de ponta a ponta, garantindo que somente as pessoas que estão se comunicando podem ler ou ouvir as mensagens trocadas (WHATSAPP, 2021). Com as mudanças, tanto o Facebook quanto as empresas terceirizadas terão acesso a essas comunicações.

No Brasil, a preocupação ainda é maior devido ao domínio que a ferramenta tem no país. O WhatsApp está instalado em 99% dos *smartphones* e, entre as plataformas de redes sociais, é o aplicativo no qual o cidadão brasileiro mais passa tempo ao longo do dia (PAIVA, 2021). Isso significa que com as mudanças realizadas pela ferramenta, a empresa Meta terá acesso aos dados gerados por 99% dos 234 milhões de *smartphones* (EAESP, FGV, 2021) que estão em uso no país. Esses dados demonstram que essa nova imposição pode acarretar um consentimento forçado, já que retirar-se do aplicativo significa um risco de isolamento social, ele se tornou ferramenta de trabalho e, quando consideramos a utilização de dados móveis, é a única opção de vários cidadãos devido a prática de *zero-rating*<sup>1</sup>.

O presente estudo parte de duas premissas. A primeira é a necessidade de se pensar o crescimento da internet concomitantemente ao fortalecimento das leis de proteção de dados pessoais. A segunda é que o comportamento do usuário dentro das plataformas também deve ser ativo para resguardar seus direitos. Em consonância com esses pressupostos e tomando como partida as mudanças realizadas nos Termos de uso da rede de mensagens WhatsApp no início de 2021, a pesquisa busca avaliar, na perspectiva dos estudantes, se tais mudanças foram comunicadas de uma forma efetiva, se elas impactaram na conscientização dos usuários para a proteção dos seus dados e quais as barreiras que impedem os usuários de tomarem atitudes para se protegerem.

O primeiro capítulo conta com uma revisão bibliográfica de artigos e pesquisas realizadas na área de Comunicação Social e quais foram os avanços e questões abordadas até

---

<sup>1</sup> *Zero-rating* é a prática que algumas operadoras utilizam de oferecer aos seus clientes o acesso a determinados aplicativos e serviços sem custos financeiros.

o presente momento. No segundo capítulo é feita uma revisão conceitual abordando os três principais pontos para a pesquisa, o WhatsApp e as mudanças de modelo de negócio e das políticas de privacidade, a coleta e vigilância de dados e por fim o direito à privacidade e a proteção de dados. Finalizando o trabalho, é apresentado o questionário e os resultados da perspectiva dos estudantes da Universidade de Brasília.

## CAPÍTULO 1: EM BUSCA DE ANTECEDENTES

Antes mesmo de adentrar nas questões teóricas dessa pesquisa, é importante localizá-la no contexto acadêmico e identificar a importância do estudo para a sociedade. Apesar de ser um tema muito relevante, principalmente quando compreendemos que os desdobramentos dos avanços na conectividade já estão inseridos no dia a dia da população de modo irreversível, a vigilância de dados ainda não é um tema muito explorado na área da comunicação social; em contrapartida já se tornou assunto central de vários estudos realizados em outras áreas, como o direito.

Neste capítulo, fez-se o resgate de outros estudos já realizados sobre o tema, por meio de uma busca nos sites da Biblioteca Digital da Produção Intelectual Discente da Universidade de Brasília (BDM), da Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) e no Google Acadêmico, realizada entre os dias 01 e 15 de fevereiro de 2022. Foram utilizadas as palavras-chave “proteção de dados”, “vigilância de dados” e “WhatsApp”, abrangendo o período de 2015 a 2022, porque o foco do trabalho são as alterações na política de privacidade do aplicativo de mensagens Whatsapp, ocorridas nos últimos anos, que culminaram com a nova política em fevereiro de 2022 .

Como apontado anteriormente, a produção acadêmica sobre o assunto na área de comunicação ainda é recente e, por consequência, não é robusta. No entanto, durante a busca, alguns trabalhos relevantes com esse tema foram encontrados e é importante resgatar conclusões que já foram constatadas nessas pesquisas.

O Google Acadêmico foi o ponto de partida para a busca de artigos sobre o assunto e encontramos três artigos que, de certa maneira, abordam a temática do presente trabalho, são eles: *Vigilância e monitoramento na era da internet das coisas: um olhar sobre o “paradoxo da privacidade”*, *Privacidade e proteção de dados pessoais: perspectiva histórica e O capitalismo de vigilância e a política da desinformação*.

O primeiro artigo, *Vigilância e monitoramento na era da internet das coisas: um olhar sobre o “paradoxo da privacidade”* (2019), de Quezia Salles Cabral Viana e Guilherme Cavalcante Silva, foi publicado na Revista do EDICC da Unicamp e buscou compreender como a vigilância e o monitoramento na era da Internet das Coisas<sup>2</sup> estão impactando a vida e o comportamento dos estudantes universitários. Por meio de um questionário do tipo Likert<sup>3</sup>, o artigo identifica o nível de familiaridade dos estudantes com a internet e o mundo digital, se

---

<sup>2</sup> A Internet das Coisas é a interconexão digital de objetos físicos com a internet, tornando esses objetos um instrumento para reunir e transmitir dados.

<sup>3</sup> A escala Likert é normalmente usada em questionários de pesquisa de opinião. Ao responderem o questionário baseado nesta escala, os entrevistados expõem o nível de concordância que tem com uma afirmação.

a vigilância acontece de forma discreta a ponto de os estudantes não perceberem, se a troca de informações era considerada pelos estudantes algo vantajoso, até que ponto a vigilância interfere na liberdade dos universitários e com que frequência os alunos são expostos a publicidades impostas por algoritmos e como encaram essa situação.

Os resultados da pesquisa demonstraram que a maioria dos universitários utilizam a internet há pelo menos dez anos e 99,6% acessam a internet diariamente, sendo que a porcentagem de entrevistados que possuem algum tipo de conexão com a internet – seja por smartphones, computadores, tablets, etc – ultrapassa os 100% devido a respostas simultâneas. Essa contextualização demonstra o alto nível de conectividade dos estudantes com a internet há vários anos, mas esse fato não é sinônimo de usuários conscientes sobre a vigilância de seus dados (VIANA; SILVA, 2019).

O levantamento realizado por meio dos questionários demonstrou que há “uma discrepância entre o conhecimento por parte dos usuários da importância da proteção de seus dados e a efetiva tomada de ação com relação a isso.” (VIANA; SILVA, 2019, p. 255). Constatou-se que quando a vigilância não se apresenta de forma concreta, como câmeras de monitoramento, os estudantes não são capazes de identificar com tanta facilidade a vigilância de seus dados, por exemplo, não detectaram nenhum risco ao ceder seus dados em troca de benefícios como acessar *wi-fi* de locais públicos. Outra constatação indicada como preocupante pelos pesquisadores é que poucos alunos se incomodam, importam ou sequer reparam na produção de anúncios “personalizados” a partir de seus históricos de busca.

A pesquisa finaliza afirmando que há um paradoxo da privacidade mesmo em um público jovem e altamente conectado e, por consequência, permite admitir a existência desse fenômeno na sociedade como um todo, tornando o “capitalismo de vigilância”<sup>4</sup> algo ainda mais preocupante.

O segundo artigo, *Privacidade e proteção de dados pessoais: perspectiva histórica* (2021), foi realizado na área da Ciência da Informação pelas pesquisadoras Daniela Assis Alves Ferreira e Marta Macedo Kerr Pinheiro e pelo pesquisador Rodrigo Moreno Marques. O estudo discute, por meio de pesquisa bibliográfica e documental, a evolução histórica do conceito de privacidade e como ela é aplicada nos dispositivos normativos que definem o direito à privacidade e o direito à proteção de dados pessoais no Brasil e nos países que compõem a União Europeia. Existe dificuldade em conceituar o termo privacidade porque ela

---

<sup>4</sup> Popularizado pela pesquisadora Shoshana Zuboff, apresenta uma nova forma do capitalismo, em que os dados adquiridos pela vigilância são monetizados.

sofre variações de acordo com região, classe social, épocas e países, além da definição de público e privado, mas o trabalho adota o conceito de privacidade de Fortes (2017):

Conceber a privacidade na internet como um direito fundamental, em sentido amplo, capaz de recepcionar em seu bojo a proteção da vida privada, da intimidade, da imagem, da honra e dos direitos-base vinculados ao conceito de direitos de privacidade na internet, significa dizer que, na contemporaneidade, o direito de navegar na internet com privacidade, o direito de monitorar quem monitora, o direito de deletar dados pessoais e o direito de proteger a identidade online devem ser tutelados, explícita e expressamente, como um dos pilares de garantia da eficácia do direito fundamental à privacidade em sentido amplo (FORTES, 2017, p. 287).

A privacidade, que antes era limitada à família e ao lar, com o tempo passa a se referir ao que é pessoal, e na esfera pública tornou-se um conceito cada vez mais necessário de ser delimitado e protegido diante da vigilância dos indivíduos, feita tanto por empresas privadas quanto pelo Estado. Transformado pelos espíritos do capitalismo, o controle da privacidade do indivíduo eleva, então, o conceito de lar para um refúgio, modificando também o conceito de propriedade e tornando a vida privada passível de comercialização na sociedade globalizada por meio do uso das tecnologias de informação.

A internet transformou ainda mais esse cenário, uma vez que as tecnologias da comunicação e informação “colocam à disposição das próprias pessoas que não conhecem, uma espécie de impulso mórbido de se mostrar em público, por vaidade, por carência de atenção, por protagonismo banal, por celebridade fácil, ou para satisfazerem o exibicionismo” (CORREIA, 2014, p. 161).

Toda essa modificação de compreensão do que é privacidade e também da maneira como as pessoas se comportam para proteger a sua vida pessoal exigiu a formulação e implementação de políticas públicas e dispositivos legais para disciplinar o uso da internet. No Brasil, o Marco Civil da Internet (Lei nº 12.965, de 23 de abril 2014) foi um importante passo para deliberar sobre direitos, deveres e garantias para o uso da internet, mas ainda “deixou brechas em relação ao tratamento, utilização e comercialização dos dados pessoais dos usuários” (FERREIRA; PINEIRO; MARQUES, 2021, p. 168), além de ter sido necessária a aprovação de medida provisória pelo Senado para inserção da Autoridade Nacional de Proteção de Dados (ANPD), instância independente responsável por fiscalizar a aplicação da lei, pois a ANPD havia sido vetada pela Presidência da República.

O artigo conclui afirmando a necessidade de um olhar crítico com relação à privacidade e defendendo que toda agência reguladora possua participação efetiva “da

sociedade civil e comunidade acadêmica em seus órgãos deliberativos para fazer frente aos grandes interesses econômicos aí envolvidos, muitas vezes divergentes do interesse público” (FERREIRA; PINEIRO; MARQUES, 2021, p. 162). Os autores manifestam ainda a expectativa de que a pesquisa possa subsidiar futuros trabalhos sobre privacidade, proteção de dados pessoais, tais como vigilância e vigilância pública, mercado de dados, modelos de negócios digitais, Internet das Coisas e *Big Data*.

Por fim, o artigo *O capitalismo de vigilância e a política da desinformação* procura explicar como o capitalismo de vigilância, conceito abordado no primeiro artigo aqui apresentado, contribui para a desinformação da população. A partir de uma revisão literária e pesquisa documental, o artigo expõe casos recentes como a compra do software espião chamado *Remote Control System* (RCS) por países da América Latina, incluindo o Brasil, e a importância de serem elaboradas políticas públicas focadas na educação e na regulação do tema.

Esse novo modelo de capitalismo influencia e modifica o comportamento humano, no momento em que as grandes empresas de tecnologia vendem a certeza do sucesso de suas campanhas publicitárias e, para que esse objetivo seja alcançado, é necessário a obtenção da maior quantidade possível de dados por meio do “rastreamento infinito dos hábitos das pessoas” (FARIA; MAGALHÃES, 2021, p. 61). A extração e a refinação desses dados possibilita que as ações dos indivíduos sejam previstas, determinando o que deve ser mostrado para ele e manipulando seus hábitos de consumo, ou seja, “o produto vendido por essas empresas é a gradativa e imperceptível mudança no comportamento do cidadãos, para que eles vejam o mundo da forma que o anunciante queira.” (FARIA; MAGALHÃES, 2021, p. 61).

O capitalismo de vigilância usa a experiência humana como matéria-prima gratuita para suas práticas comerciais e se “retroalimenta indefinidamente” (FARIA; MAGALHÃES, 2021, p. 64). Dessa maneira, a economia movida a partir da extração dos dados está diretamente ligada ao aumento da vigilância.

A venda dessas informações coloca em risco não só a privacidade de cada usuário da internet, mas ameaça a democracia por ser facilitadora da desinformação e atacar direitos civis como igualdade e liberdade. Alguns países europeus surgiram com soluções que não alcançam o centro do problema, como banimento de memes da internet, proposta do partido governante da Espanha (FARIA; MAGALHÃES, 2021, p.75).

O artigo conclui que a regulação pública se torna imprescindível para que a questão da desinformação seja realmente solucionada. O estabelecimento de multas milionárias e

obrigações às empresas demonstra que a autorregulação não é um caminho suficiente e que o Estado democrático deve fazer sua parte,

(...) a sociedade civil deve acompanhar esses movimentos e, através de suas organizações públicas e privadas, os órgãos de comunicação social, os sistemas educacionais, as instituições representativas das diversas dimensões da sociedade, entre outros e outras, tomem os dados pessoais como algo tão importante a ser defendido como os demais direitos humanos. (FARIA; MAGALHÃES, 2021, p. 76).

Superando os artigos, a busca por trabalhos acadêmicos sobre a temática da vigilância de dados foi realizada nos sites da Biblioteca Digital da Produção Intelectual Discente da Universidade de Brasília (BDM) e da Biblioteca Digital Brasileira de Teses e Dissertações (BDTD). A pesquisa resultou em duas dissertações que colaboram com a pesquisa.

Com o título *Comunicação na internet e a violação do direito à privacidade: uma análise avaliativa das políticas e termos de uso na internet*, o primeiro trabalho, de autoria de Alessandra Lourenço Simões, avaliou os termos e condições de uso dos dez maiores aplicativos de redes sociais online, focando na coleta de dados pessoais e a forma como esses dados são utilizados. Por meio de revisão bibliográfica, a pesquisa apresenta conceitos básicos sobre privacidade, direito à comunicação e a vigilância na internet. Por fim, é feita a análise avaliativa sobre as políticas e/ou termos de uso dos aplicativos, mostrando “os aspectos em comum e as possíveis falhas no que diz respeito à comunicação com os usuários em relação ao uso dos seus dados e as possíveis violações ao direito à privacidade” (SIMÕES, 2017, s.p.).

A dissertação tem o objetivo de contribuir para o despertar dos usuários dessas redes sociais para uma maior conscientização quanto ao uso da internet, seus riscos e direitos, principalmente quando violados mediante autorizações que muitas vezes são realizadas de forma inconsciente. Apesar das redes sociais terem um papel importante para a evolução da comunicação, existe um outro lado que desperta preocupação, a possibilidade de monitoramento e vigilância dos usuários, e isso só se tornou possível a partir do momento em que a internet passa a ser comercializada em escala global e a informação passa a ser um bem valioso.

O interesse pela monitoração e vigilância dos cidadãos ganha força com a possibilidade de o usuário da internet ser também um possível consumidor, pois assuntos como marca, produto e compra, também passam a fazer parte do fluxo comunicacional do mundo digital. (SIMÕES, 2017, p.26)

Há uma variedade de ferramentas tecnológicas que podem auxiliar na vigilância digital e ela não se restringe a grandes empresas de tecnologia. Estão também “na nossa rotina nos grandes centros urbanos, em espaços públicos e privados, que aliados aos aplicativos de internet, monitoram a vida de seus usuários” (SIMÕES, 2017, p. 26), um exemplo são as câmeras de vigilância. Na internet, o monitoramento pode ser feito desde os cliques que são dados até mesmo o tempo gasto em cada página da web.

O estudo conclui que as políticas de segurança ou termos de uso, também conhecidos como contratos virtuais, não garantem que o usuário esteja ciente do uso de seus dados, principalmente porque não demonstrou ser um meio de comunicação efetivo. Os contratos virtuais são, em sua maioria, muito semelhantes e não deixam claro onde as informações serão armazenadas, por quanto tempo e quais as ações tomadas pelas empresas para que não sejam violadas. Durante a análise também foi detectada a possibilidade de compartilhamento de dados com empresas terceirizadas ou do governo sem a solicitação judicial.

São diversos os pretextos argumentados pelas empresas que controlam as principais mídias sociais digitais para que elas tenham acesso aos dados pessoais de seus usuários, cabendo ao governo ser ativo no monitoramento para prevenção e proteção dos cidadãos. A violação da privacidade dos usuários da internet, assim como os demais artigos aqui apresentados concluíram, tem potencial para violar direitos e interferir no exercício da democracia.

Por fim, a pesquisa realizada em 2013 com o título *Você tem WhatsApp? Um estudo sobre a apropriação do aplicativo de celular por jovens universitários de Brasília*, de autoria de Bruna Sthefany Souza dos Reis, analisou como os jovens de Brasília utilizam o aplicativo de mensagens WhatsApp, quais foram os reflexos desse novo meio de comunicação e como o aplicativo altera o elemento tempo. O trabalho utilizou da etnografia e netnografia para fundamentar sua metodologia, isto é, a pesquisadora se inseriu em um grupo de estudantes no WhatsApp e fez um estudo de observação e mapeou os perfis analisados a partir das práticas comunicacionais nas redes sociais.

O trabalho não fala diretamente sobre o papel do WhatsApp como ferramenta de vigilância digital, mas é interessante observar a evolução comportamental dos usuários do aplicativo e constatar as mudanças e as ações que ainda persistem. A pesquisa concluiu que o WhatsApp não criou algo novo, mas se tornou a “extensão das relações sociais dos jovens e é usado mais para compartilhar o cotidiano dos usuários do que informações midiáticas” (REIS, 2013, p. 53) – a frequência de mensagens sobre o cotidiano foi de 21%, contra 1% sobre informações midiáticas.

Apesar do aplicativo ainda ter esse papel de conexão entre colegas e troca de mensagens sobre o cotidiano, o cenário em que ele está inserido mudou radicalmente e é possível constatar de forma empírica que nos últimos anos a força de troca de mensagens midiáticas foi ampliada, além disso a pesquisa não apresenta nenhuma porcentagem de mensagens entre empresas e usuários, o que atualmente é comum e até estimulado pelo aplicativo.

Todas essas pesquisas demonstraram a importância do estudo das plataformas principalmente quando analisamos os impactos que elas causam não apenas na vida de cada usuário, mas na sociedade como um todo. É preciso que esse esforço também seja representativo na área de comunicação que tanto tem relação com as diferentes formas de troca de informações e com o comportamento de grandes empresas de tecnologia na coleta e análise de dados a partir dessa troca.

A revisão bibliográfica auxilia a pesquisa ao expor os avanços desse tema na área de comunicação e as abordagens propostas pelos pesquisadores. A maioria das pesquisas levam em consideração o comportamento dos usuários nas plataformas online e demonstram a importância de uma educação digital que apresente as consequências das trocas de dados com Estado e grandes empresas de tecnologia, também demonstram como a vigilância acarreta em riscos que ultrapassam a esfera particular de cada usuário.

A internet é, e deve continuar sendo, um ambiente infinito de novas possibilidades para a implantação da vigilância de dados, porém nenhum dos trabalhos observados aborda o motivo da hegemonia de alguns aplicativos no Brasil e, especificamente, o papel do aplicativo de mensagens mais utilizado em nosso país, o Whatsapp. Dessa maneira a pesquisa soma na busca por compreender as escolhas dos usuários por determinada plataforma online e como auxiliar na conscientização dos usuários sobre os riscos desse acesso ilimitado à sua vida privada.

## CAPÍTULO 2: REVISÃO CONTEXTUAL

Neste capítulo, iremos aprofundar os principais termos deste estudo, buscando visões complementares de diferentes autores sobre o WhatsApp, a vigilância de dados e o direito à privacidade.

### 2.1. O início e a evolução do WhatsApp

O aplicativo, que está instalado em 99% dos *smartphones* brasileiros, provocou grande impacto na diminuição do uso do SMS – funcionalidade que permite a troca de mensagens de texto – e permite até a realização de ligações telefônicas. Além da criação de comunidades e conexão entre as pessoas, o WhatsApp está se tornando uma forte presença nos negócios online, isso explica a atualização da política de privacidade e as novas possibilidades de interação entre as empresas e seus clientes.

Antes de avançar ao momento atual do aplicativo, é interessante observar a sua evolução e as mudanças em seu modelo de negócio. O WhatsApp foi lançado em 2009 por dois ex-funcionários do Yahoo, Jan Koum e Brian Acton, e surgiu como uma forma de compartilhar o status dos usuários com amigos e alguns meses depois do seu lançamento ele seguiu outro caminho, se tornando uma alternativa ao SMS.

Seus criadores tinham como princípios a frase "Sem anúncios! Sem jogos! Sem truques!" (PAHWA, 2021, tradução da autora) e nos primeiros anos não havia nenhum tipo de coleta de dados dos usuários, além do número de telefone cadastrado. Para manter os desenvolvedores e controlar o número de *downloads*, era cobrada uma anuidade no valor de U\$0,99 (PAHWA, 2021).

Em pouco tempo o WhatsApp alcançou a marca de 200 milhões de usuários, se tornando uma ameaça e uma oportunidade de capitalização para o grupo Facebook (atual Meta, Inc.) (WARZEL, 2018), um baú de tesouros a ser explorado pela maior empresa de anúncios da internet. Então, em fevereiro de 2014, o aplicativo foi adquirido pela gigante da tecnologia pelo valor de U\$19 bilhões. Logo após a aquisição, os fundadores do WhatsApp em entrevista afirmaram que o respeito pela privacidade estava codificado no DNA da ferramenta, já que o construíram com a preocupação de saber o menos possível sobre seus usuários (AGRELA, 2014).

Apesar da afirmativa feita pelos criadores, o modelo de negócio foi modificado para que pudesse conversar com as outras funções exercidas pelo conglomerado e, o que antes não era retido, como os status, imagens de exibição e frequência de uso do WhatsApp, começa a

ser compartilhado com a empresa-mãe e, posteriormente, novos recursos foram sendo adicionados para torná-lo ainda mais vantajoso aos negócios (PAHWA, 2021).

Todas essas alterações nos objetivos originais do aplicativo fizeram com que os fundadores deixassem a empresa Facebook. Brian Acton então constituiu, junto com o empreendedor norte americano, Moxie Marlinspike, a fundação sem fins lucrativos Signal Foundation, que tem como principal serviço o Signal Messenger, aplicativo de mensagens conhecido pelo seu alto nível de segurança (CARVALHO, 2021).

Entre as modificações realizadas pelo Facebook, um dos novos recursos é o WhatsApp Business API, que foi lançado em janeiro de 2018 no Brasil. Para alcançar os objetivos dessa nova versão, modificou termos da política de privacidade do aplicativo que, desde fevereiro de 2021, permite que os metadados dos usuários sejam compartilhados com as empresas do grupo Meta, Inc., ou seja, mesmo que você não tenha uma conta em nenhuma outra rede social do conglomerado, você estará alimentando o banco de dados delas. A atualização abriu as portas para o marketing do WhatsApp, com potencial de se tornar um dos canais com as maiores taxas de engajamento (PAHWA, 2021).

Manuel Castells, sociólogo e teórico da comunicação especialista em redes, colabora com essa linha de pensamento ao afirmar que:

O Facebook é uma rede social com o objetivo de obter lucros empresariais que dependem fundamentalmente do aumento de tráfego e da captação de dados que podem ser vendidos. Ou seja, como rede, trata-se de um sistema de comunicação. Como negócio, naturalmente, é comercial e seu negócio não é a comunicação, e sim o negócio de dados (CASTELLS, 2018).

### *2.1.1 Alterações da política de privacidade*

As mudanças realizadas dão continuidade ao compartilhamento de dados que já acontece desde 2016, mas as novidades alcançaram a política de privacidade do aplicativo, explicitando os objetivos da empresa de aumentar seu acesso aos dados dos usuários que serão compartilhados com a Meta, Inc., a empresa-mãe. As mudanças estão relacionadas diretamente às contas do WhatsApp Business, ou seja, os dados produzidos entre conversas de usuários comuns com empresas.

A política de privacidade é um documento jurídico e lista todas as ações que poderão ser realizadas pelo aplicativo com os dados gerados no seu sistema. Ela deve dar visibilidade ao tratamento de dados pessoais e atender os princípios da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), como garantir que o conteúdo seja de fácil acesso e

compreensão, orientar como os dados serão tratados, a finalidade do tratamento, se existe compartilhamento com terceiros ou não, o prazo de retenção dos dados, limitar o tratamento apenas ao necessário, identificar os agentes que farão esse tratamento, impossibilitar o tratamento com fins discriminatório e demonstrar medidas eficazes para o cumprimento das normas de proteção de dados pessoais (BRASIL, 2018).

Se faz necessário analisar as principais mudanças na política de privacidade do WhatsApp, principalmente para compreender o que causou maior preocupação das autoridades e organizações que estudam o tema da proteção de dados. Os textos comparados são da Política de Privacidade de 2020 (PP1) e a mais recente de 2021 (PP2). Ambas estão no site do WhatsApp<sup>5</sup>.

A PP2 inicia seu texto se diferenciando da PP1 ao explicar que os novos termos de política de privacidade apresentam informações adicionais para afirmar o compromisso da ferramenta com a privacidade, também introduzem a importância que o aplicativo tem para diversas empresas que o utilizam para se comunicar com seus clientes. Reafirmam ainda que o aplicativo faz parte das Empresas do Facebook e “colabora com o Facebook para fornecer experiências e integrações com a família de aplicativos e produtos do Facebook” (WHATSAPP, 2021, s.p.). Nesse primeiro momento, também determina que o fornecimento de alguns dados são necessários para que o usuário continue a utilizar o aplicativo.

O termo “informações” foi substituído, na PP2, por “dados” em todos os títulos. A primeira seção é denominada de “Dados que coletamos” (antigo “Informações que coletamos”), nesse tópico os dados de pagamentos passam a fazer parte do rol de dados que serão coletados, afirmando que irão tratar dados adicionais do usuário, como a conta para pagamento. Os dados sobre dispositivos de conexão também recebem novas informações, sendo elas o tempo, a frequência e a duração das atividades e interações. Nos dados de conexões e dispositivos foi incluído o nível de bateria do celular, a força do sinal, a versão do aplicativo que está sendo utilizado, a operadora do celular e o provedor da internet. A partir desse momento, o PP2 começa a introduzir os dados destinados aos “Produtos das Empresas do Facebook” e a informação de que para esses produtos existem identificadores exclusivos associados ao mesmo dispositivo ou conta.

Os dados de localização também foram modificados, incluindo a informação de que mesmo quando o usuário não utilizar os recursos de localização, o aplicativo usará o

---

<sup>5</sup> Acesse as políticas de privacidade nos links: <https://www.whatsapp.com/legal/privacy-policy> e <https://www.whatsapp.com/legal/privacy-policy/revisions/20200720>.

endereço de IP e outros dados – como código de área de número de telefone – para calcular a localização geral.

Na seção “Dados de terceiros”, um novo tópico é relacionado às Empresas no WhatsApp, quando o aplicativo explica que as empresas que utilizam o WhatsApp para contato com seus clientes podem fornecer dados sobre as interações delas com o usuário e, trabalhando com serviços terceirizados, esses dados podem sair da plataforma e, nesse momento, a empresa Meta, Inc. não mais garante a criptografia de ponta-a-ponta.

O próprio Facebook utiliza serviços de terceiros, mas antes o que era apresentado como uma maneira de “operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços” (WHATSAPP, 2020, s.p.) agora é apresentado também como meio para “processar pagamentos; entender como as pessoas usam nossos Serviços; comercializar nossos Serviços, ajudar você a se conectar com empresas usando nossos Serviços” (WHATSAPP, 2021, s.p.), além de afirmar que a empresa também garante a segurança, integridade e a possibilita oferecer ajuda ao cliente.

A seção “Como usamos os dados” e a personalização dos serviços é evidenciada quando o aplicativo afirma que esses dados são utilizados para “aprimorar, corrigir e personalizar nossos Serviços e conectá-los aos Produtos das Empresas do Facebook que você pode usar” (WHATSAPP, 2021, s.p.), além de iniciar a possibilidade de interações comerciais com o objetivo de permitir que as empresas consigam “enviar notificações de transação, consulta e envio, atualizações de serviços e produtos, e marketing” (WHATSAPP, 2021), apontando que as mensagens de marketing podem conter ofertas do interesse do usuário.

Levando em consideração que o WhatsApp mantém a não permissão de inclusão de banners digitais de publicidade dentro do aplicativo, os dados coletados nessas conversas poderão ser usados pelas empresas contratantes para direcionar anúncios nas plataformas da empresa-mãe (CARDOSO, 2020).

No tópico “Dados compartilhados por você e por nós”, é inserido o tema “Empresas no WhatsApp”, que afirma que existem serviços específicos, como as métricas relacionadas ao uso dos serviços por essas empresas. Por fim, o WhatsApp reafirma o compartilhamento de dados com as demais empresas do Facebook e, diferentemente da política de privacidade anterior, retira a afirmação de que “Na verdade, o Facebook não usará suas mensagens do WhatsApp por qualquer motivo que não seja nos auxiliar na operação e na execução dos Serviços”(WHATSAPP, 2021), abrindo a possibilidade de ter as mensagens também compartilhadas.

Apesar de defender que as alterações não comprometem a segurança dos dados de seus usuários, a política de privacidade que está vigendo no Brasil não é a mesma aplicada na União Europeia, Estados Unidos e Canadá, conhecidos por possuírem uma legislação forte em que já foram aplicadas multas ao Facebook<sup>6</sup>.

Todas essas alterações causaram reações dos órgãos responsáveis por fiscalizar a proteção de dados no Brasil. Os novos termos do WhatsApp foram avaliados pela Agência Nacional de Proteção de Dados (ANPD), Ministério Público Federal (MPF), Conselho Administrativo de Defesa Econômica (Cade) e Secretaria Nacional do Consumidor no Ministério da Justiça e Segurança Pública (Senacon), que expediram uma recomendação conjunta que adiou as alterações na Política de Privacidade para evitar possíveis danos aos usuários.

Além da recomendação, a ANPD instaurou um processo administrativo e avaliações técnicas que, a partir de seu texto, permitem compreender as principais alegações sobre a falta de transparência, sendo elas: informações não facilmente acessíveis aos usuários do Google; estrutura escolhida para fornecer a informação em desacordo com as regras gerais de proteção de dados; informações relevantes disponibilizadas ao usuário somente após diversos cliques; informações nem sempre claras ou compreensíveis; finalidade da extração de dados descrita de forma genérica e vaga; informações que não são claras o suficiente para que o usuário compreenda que a base legal para a personalização de anúncios é o consentimento e não o legítimo interesse da empresa<sup>7</sup>; e a inexistência de informação sobre o período de retenção de alguns tipos de dados.

A nota técnica também destaca algumas alterações já listadas anteriormente por esse trabalho e apresenta interpretações importantes a partir dessas mudanças. O primeiro apontamento está no fato de que a política de privacidade anterior permitia que, no prazo de 30 dias, os usuários poderiam escolher por não compartilhar seus dados para receber anúncios no Facebook. Muitos usuários nem mesmo se atentaram a essa possibilidade, mas a opção não consta mais na política atualizada, tornando impossível a revogação dessa permissão de tratamento dos dados.

---

<sup>6</sup> Em 2017, o Facebook foi multado pela Comissão Europeia (CE) em €110 milhões por combinar automaticamente os usuários do WhatsApp e do Facebook, enquanto na Itália recebeu multa de €3 milhões por impor o compartilhamento dos dados dos usuários com o Facebook. Em 2018, nova ocorrência, dessa vez de €600 mil por transferir e processar dados sem o consentimento de seus usuários.

<sup>7</sup> O legítimo interesse da empresa é interpretado como sendo o tratamento de dados pessoais para finalidades legítimas e específicas, considerado a partir de situações concretas, hipótese mais flexível de autorização legal para o tratamento de dados pessoais. O fundamento não deve ser utilizado como uma “carta coringa” e eximir as empresas de solicitar o consentimento dos titulares. A própria LGPD adiciona cuidados extras que devem ser tomados pelas empresas para essas situações.

Os identificadores exclusivos também foram pontos de preocupação da Agência, que afirmou que esse compartilhamento “pode dar grande poder analítico ao Facebook, o que pode representar possível impacto à privacidade do usuário” (ANPD, 2021, p. 10).

As informações de localização coletadas não estão detalhadas e, “apesar de a coleta de dados de localização em nível agregado ou geral não aparenta ser medida excessivamente invasiva” (ANPD, 2021, p.11), a não especificação do rol de informações que serão retiradas pode acarretar na captura da localização detalhada do usuário.

O fato de o Facebook ser dono do aplicativo como possível terceirizado das empresas que o utilizam acarreta em dupla coleta de informações, pois a empresa pode fornecer aos seus serviços terceirizados acesso às suas comunicações para ler, gerenciar e processar as informações.

Por fim, a agência também se preocupa com o fato de a Política de Privacidade deixar em aberto se o Facebook é capaz ou não de usar as mensagens do WhatsApp para quaisquer motivos, tendo em vista que se for possível esse acesso “para fins que não estão claros, pode haver um prejuízo à legítima expectativa dos titulares de dados pessoais, que acreditam que o conteúdo das mensagens nunca é acessado.” (ANPD, 2021, p.15).

Além da Política de Privacidade endereçada aos usuários comuns, o WhatsApp Business (WAB) também possui uma política com termos específicos para as empresas que passam a fazer parte do aplicativo. De acordo com a ANPD, essa ferramenta não deve ser vista apenas como “a ponta final de uma comunicação”, mas sim como uma aplicação servidora, uma vez que existem funcionalidades exclusivas de tratamento das mensagens trocadas, dessa forma:

(...)o uso do WAB permite que o conteúdo de mensagens e dados do usuário saiam do domínio do WhatsApp e entrem em domínio de terceiros (Seja a Empresa no WhatsApp, Empresas do Facebook, ou outras empresas que ofereçam serviços para ambas), com regras de negócio e políticas de tratamento de dados que devem ser conhecidas (ANPD, 2021, p. 20)

Todas essas alterações tornam questionável o poder do WhatsApp sobre seus usuários, apesar de o aplicativo afirmar que essas mudanças não são novidade, sob a alegação de que desde 2016 os dados começaram a ser compartilhados entre as empresas. No entanto, a quantidade de dados compartilhados sem dúvidas aumenta quando outros agentes, como lojas, iniciam interações dentro do aplicativo.

A reação dos usuários brasileiros do aplicativo a essas mudanças tornou-se motivo importante para uma pesquisa mais aprofundada, cujo intuito é responder alguns questionamentos atuais, como a falta de cultura de privacidade no Brasil e a importância da compreensão da plataforma WhatsApp diante desse fato.

## 2.2. Vigilância digital

A partir da análise das mudanças realizadas na política de privacidade do WhatsApp é possível iniciar um estudo sobre os motivos de tantas empresas se interessarem pela coleta de dados pessoais dos usuários da internet e como eles são utilizados na prática para beneficiar os negócios tanto online quanto offline por meio da vigilância digital.

A vigilância pode ser observada antes mesmo do advento da internet, em dispositivos adotados para controle dos cidadãos. Foucault tem extenso trabalho sobre o tema e classifica a vigilância como forma de poder disciplinar, argumentando que, com o objetivo de assegurar a dominação e a disciplina, são utilizados métodos como a observação hierárquica, permitindo que haja a vigilância. Esse modelo de dominação é característico da lógica do capitalismo (FUCHS, 2011), consequência do “liberalismo e da arte liberal do governo é a extensão dos procedimentos de controle, constrangimento e coerção” (FOUCAULT *apud* FUCHS, 2011, p.67), e todas as técnicas estão completamente ligadas umas às outras (FUCHS, 2011).

O filósofo também apresenta a vigilância do panóptico<sup>8</sup>, que se baseia na invisibilidade do poder de disciplina, em que “vê-se tudo, sem nunca ser visto”. Esse tipo de vigilância é exatamente o que encontramos atualmente nas plataformas online, modelo ao qual cabe o paralelo entre a vigilância do panóptico com a vigilância digital relatada ou seja, apesar de possuir todo um documento jurídico que determina o que será vigiado, não é muito claro e nem visível para os usuários dessas plataformas a existência desse sujeito vigilante. Foucault ainda corrobora com esse paralelo ao explicar que o que se é vigiado “é visto, mas não vê; objeto de uma informação, nunca sujeito numa comunicação” (FOUCAULT *apud* FUCHS, 2011, p.165). Atualmente já se fala na extrapolação do panóptico e se observa uma espécie de superpanóptico, pois essa observação vai além dos espaços físicos e alcança todo o ciberespaço, ampliando o número de vigilantes e de sujeitos afetados.

---

<sup>8</sup> A ideia do panóptico é colocar um princípio de vigilância no centro, que exerce poder soberano sobre todos os indivíduos que estão dentro da máquina de poder, é o sonho mais antigo dos soberanos, nenhum sujeito escapa e nenhuma ação é desconhecida. (Foucault, 2007, p. 93)

Fernanda Bruno (2021), doutora em Comunicação e Cultura pela Universidade Federal do Rio de Janeiro, elucida que os objetivos dos bancos de dados e perfis estão na antecipação de tendências, o que diferencia a vigilância digital do panóptico. Para a pesquisadora, “a vigilância digital põe em obra uma visibilidade que é sobretudo informacional e temporal, onde não basta tudo ver, mas principalmente prever, a ponto de preceder o evento” (BRUNO, 2021). Quer dizer que atualmente a vigilância deve ser capaz de prever ações e cenários futuros, o que não significa que as suas consequências serão vistas em outra linha de tempo, mas consistem em processos que permitem intervir nas escolhas desses usuários no presente para alterar ações possíveis no futuro. A vigilância que estamos inseridos atualmente:

(...) trata-se de uma vigilância que não mais isola e imobiliza indivíduos em espaços de confinamento, mas que se aproxima ou mesmo se confunde com o fluxo cotidiano de trocas informacionais e comunicacionais. Uma vigilância que se exerce menos com o olhar do que com sistemas de coleta, registro e classificação da informação; menos sobre corpos do que sobre dados e rastros deixados no ciberespaço; menos com o fim de corrigir e reformar do que com o fim de projetar tendências, preferências, interesses. (BRUNO, 2021, p. 153)

Além de Foucault, George Orwell também se debruçou nas questões sobre a vigilância e, no clássico “1984”, concebe uma distopia em que uma sociedade totalitária tem como autoridade o “Grande Irmão”, que tira de toda a população o seu direito à privacidade, monitorando todos por meio de câmeras e televisores. Mesmo sendo um cenário ficcional, a história se mostrou bastante coerente com o que vivemos na atualidade, com os diversos dispositivos, programas e aplicativos que monitoram o sujeito, naturalizando a troca de informações fornecidas diariamente pelos próprios usuários.

O que podemos apontar como diferença entre a ideia de vigilância do “Big Brother”, desenvolvida no livro de Orwell, e o que vivemos é o que Lace (2015) acredita ser o caminho que a sociedade está seguindo, de “pequenos irmãos”, e não mais de um sujeito central. Além do autor, Haggerty e Ericson também sustentam que a vigilância não é mais centralizada e homogênea, permitindo “controle” tanto de poderosos como de pessoas comuns (LYON, *apud*, HAGGERT e ERICSON, 2017).

O sociólogo David Lyon explica que “a vigilância está se tornando parte de todo um modo de vida” (LYON, 2017, p. 825, tradução da autora), por isso já é possível se falar em uma “cultura da vigilância”, algo que não está mais externo à existência das pessoas. Todos os dias o cidadão comum entrega, de forma voluntária ou não, seus dados e possibilita que organizações o vigie, sendo que nessa lógica descrita acima a tentativa por proteção da

privacidade passa a ser vista como algo negativo, pois o pensamento se inverte: se a pessoa se protege é porque ela deve ter algo a esconder.

Essa mudança de visão sobre a proteção dos dados pessoais contribui com a tentativa de se apresentar a vigilância dos usuários da internet como algo positivo e vantajoso para todas as partes, divulgando a ideia de que de um lado o consumidor, de forma gratuita, receberá serviços personalizados que atendem necessidades individuais e específicas e, do outro, as organizações investem em publicidades com retorno garantido.

A gratuidade nessa relação não é verdadeira, sabemos que existe uma moeda de troca e ela é a datificação dos usuários, ou seja, tornar diversos aspectos da vida dessas pessoas em dados que posteriormente podem virar informações<sup>9</sup>. As grandes empresas de tecnologia, principalmente as que vendem publicidade (caso do Facebook e Google, por exemplo), perceberam que com a coleta e vigilância dos dados é possível identificar antigos hábitos, incluir novos e, por meio da assimilação da rotina do usuário, o tornar mais vulnerável a fazer o que é induzido pelas diversas marcas que contratam o seu serviço e instigam o consumo.

As conclusões desses autores possibilitam compreender que sempre foi forjada uma estrutura de vigilância sobre os sujeitos e hoje, mais do que nunca, as novas tecnologias possibilitam que os que detêm as informações sejam cada vez mais poderosos. Em outras palavras, a vigilância é exercida de maneira sutil e sem causar alardes aos usuários, quer dizer que o diagnóstico feito por Foucault de que “a visibilidade é uma armadilha” permanece mais atual do que nunca.

### *2.2.1 O objeto da vigilância do WhatsApp: os metadados*

A vigilância pode ser exercida a partir da coleta de vários tipos de dados, como por exemplo imagens de câmeras de segurança; no caso do WhatsApp o principal objeto utilizado para a vigilância, e que se tornou fonte de renda do aplicativo, são os chamados metadados.

Os metadados passaram a ser mais conhecidos por pessoas fora da área de tecnologia após as revelações de Edward Snowden por meio do *Wikileaks*, que mostrou como a coleta de dados que não são classificados tão relevantes, como os dados sensíveis, “podem construir um perfil mais detalhado até mesmo do que ouvir conteúdo” (MACASKILL; DANCE, 2013, s.p.).

---

<sup>9</sup>É importante compreender que dados e informações não são sinônimos. Dados podem ser números, coordenadas geográficas, símbolos, datas, nem sempre específicos. Apenas quando tratados e analisados é possível transformar esses dados em informações, que nesse momento podem identificar os usuários.

Quando falamos em um aplicativo de mensagem, pode-se chegar a conclusão de que os dados que estão sendo reunidos são as informações produzidas durante as conversas entre os usuários. Apesar de ser uma preocupação do fim da criptografia de ponta a ponta nas conversas entre o usuário e empresas, os dados mais coletados ainda são os metadados, gerados sempre que há uma ação nos dispositivos digitais. Eles acrescentam aos dados mais informações sobre uma ação realizada, por exemplo, ao acessar um site o seu endereço de IP, o navegador utilizado e o número de cliques realizados se transformam em metadados daquela ação.

A pesquisadora Anne J. Gilliland, da Universidade da Califórnia, define os metadados como “a soma total do que se pode ser em um dado momento sobre qualquer objeto informacional em qualquer nível de agregação” (GILLILAND, 2005, s.p., tradução da autora), isso quer dizer, qualquer objeto digital, independente do seu formato, pode ser manipulado como um único objeto por um computador e qualquer ação digital pode contribuir para a descoberta de metadados significativos.

De acordo com a SaferNet, fundação que promove os direitos humanos na internet no Brasil, existe uma lista de metadados mais comuns como o número de telefone, endereço de e-mail, nome das pessoas que usam o serviço, dados de localização, data e hora de acessos, informação dos aparelhos utilizados, assuntos de e-mails, duração de ligações e números de série (SAFERNET, 2013, s.p.).

No caso específico dos metadados retirados das contas de usuários do WhatsApp, são eles: modelo do *smartphone*, sistema operacional, status da bateria, força do sinal da internet, endereço de IP, horário de uso do WhatsApp, pagamentos e transações, atualizações de status, idioma, fotos de perfil, contatos, empresas as quais o usuário interage, tempo gasto no aplicativo, provedores de serviço de terceiros, e informações da seção “sobre” (WHATSAPP, 2021).

Todas essas informações quando cruzadas se tornam um ativo importante que alimentam a máquina de anúncios do grupo Meta Inc.. Esses metadados permitem que a empresa compreenda melhor as ações e consequências de cada atitude praticada pelo usuário na internet, construa um perfil detalhado e, como exposto anteriormente, estimule novos comportamentos.

Jaron Lanier, no livro *Dez Argumentos Para Você Deletar Agora Suas Redes Sociais*, afirma que “agora somos todos animais de laboratório” (LANIER, 2018, p. 13) pela constância da manipulação do comportamento a partir do rastreamento e avaliação de inteligências artificiais. O autor ainda explica que o problema não está na mudança de hábitos

– que pode ser algo natural – mas hoje todos estão inseridos nas redes sociais e o que antes era apenas uma propaganda, agora deve ser “compreendida como uma modificação de comportamento permanente e em escala gigantesca.” (LANIER, 2018, p. 14).

No livro *A sociedade em rede*, Manuel Castells também colabora com a ideia das mudanças de comportamento a partir do entrelace entre online e offline. O autor afirma que

(...) computadores, sistemas de comunicação, decodificação e programação genética são todos amplificadores e extensões da mente humana. (...) A integração crescente entre mentes e máquinas, inclusive a máquina de DNA, está anulando o que Bruce Mazlish chama de a “quarta continuidade” (aquela entre seres humanos e máquinas), alterando fundamentalmente o modo pelo qual nascemos, vivemos, aprendemos, trabalhamos, produzimos, consumimos, sonhamos, lutamos ou morremos. (CASTELLS, 2020, p.89)

Castells, apesar de ser um grande entusiasta e esperançoso dos avanços da internet, admite que os algoritmos são um campo de poder da sociedade em rede (CASTELLS, 2015) que está nas mãos de grandes empresas tecnológicas. Fernanda Bruno também segue esse pensamento ao afirmar que “esse saber é, ao mesmo tempo, controle, pois antecipa o que cada um é, o que pode fazer e o que pode escolher” (BRUNO, 2021, p. 156).

Um exemplo de vigilância e busca por antecipação de uma empresa é o *case* de análise preditiva da Target, que ficou famoso no mundo ao revelar como a vigilância dos compradores do supermercado previu a gravidez de uma adolescente antes mesmo que ela contasse aos pais. Basicamente, por meio da análise dos dados de uma parcela de clientes grávidas que participaram de uma campanha do supermercado, a empresa estudou os hábitos de compras dessas gestantes e passou a monitorar itens tidos como essenciais, a partir desses dados conseguiram identificar quais consumidores estavam grávidas, mesmo que não informassem à empresa, e iniciavam o envio de promoções na frente dos concorrentes (DUHIGG, 2012).

A partir dessa estratégia de marketing, podemos constatar o que a pesquisadora Fernanda Bruno questiona sobre a ideia comum de que as ofertas são superindividualizadas, ou seja, que a vigilância entrega produtos e serviços específicos para cada usuário. Na realidade, a autora afirma que “essa individualização almejada pelo perfil é menos da ordem da verdade ou da representação do que da ordem da simulação, da performatividade e da proação” (BRUNO, 2021, p. 156). Isso quer dizer que não se busca expor a identidade individual de cada usuário, mas prever ações e uniformizar escolhas.

A busca por homogeneizar as escolhas de toda uma população em troca de conseguir impor um consumo de massa é também ponto de tensão quando estudamos as consequências da vigilância. A partir de dados que não aparentam entregar informações tão relevantes, é possível construir identidades simuladas que já preveem os próximos passos dos usuários e que sufoca inúmeras outras possibilidades. No livro *Os custos da conexão: como os dados estão colonizando a vida humana e se apropriando dela para o capitalismo* (tradução da autora), Nick Couldry e Ulises Mejias acreditam que essa tentativa recorrente de transformar a vida e as relações das pessoas em *inputs* para a geração de lucro demonstra como o capitalismo está evoluindo (COULDRY; MEJIAS, 2019).

Nessa sociedade capitalista, a preocupação por utilizar da vida de cada cidadão para busca por capital é algo que tem alto potencial em atingir direitos humanos que deveriam ser inviolados e protegidos.

### **2.3. Direito à privacidade**

A sociedade da informação, baseada na circulação de informações, nos faz questionar se o direito à privacidade não está sendo minimizado e apagado devido aos constantes avanços tecnológicos, por isso é essencial compreender onde surgiu a ideia de privacidade e as mudanças que a ideia já sofreu com o tempo.

Inicialmente a privacidade, ou ainda mais simples, a necessidade de solidão é encontrada em partes da Bíblia, em textos gregos e na China Antiga (DONEDA, 2012, p.2), mas apenas com o surgimento do homem burguês e do conceito de propriedade privada que se inicia a busca por limitar o acesso tanto do Estado como de outras pessoas à vida íntima.

A primeira vez que se tem registrado o termo “direito à privacidade” foi em artigo de título homônimo, de Samuel Warren e Louis Brandeis, em 1890 (DONEDA, 2012, p. 60). Nele, o conceito aparece como o direito ao isolamento, a se destacar da sociedade. Danilo Doneda afirma que “o direito à privacidade não se apresentava exatamente como uma realização de exigências naturais do homem, mas sim de uma classe”, portanto, a privacidade foi marcada por elitismo (DONEDA, 2012, p. 61). A associação só foi afastada com o desenvolvimento tecnológico, quando parcela significativa da população, mesmo a menos abastada, se torna sujeita a ter sua privacidade ofendida (DONEDA, 2012).

A corrida tecnológica teve papel importante para redefinir os limites do direito à privacidade, o ser humano não era mais o único detentor da ação de processar informações e não era só o Estado que coletava informações para o controle social, as máquinas estavam

cada vez mais inteligentes e o desenvolvimento do mercado com os avanços nas áreas de marketing, comunicação e plataformas online exibiam novas ameaças.

Dessa forma, o direito civil de propriedade encontrou a urgência de ser ampliado a partir do momento em que foi reconhecida a natureza espiritual, do intelecto e dos sentimentos do homem, e a propriedade física não era mais suficiente para abarcar tudo o que o ser humano carregava. Assim, “o próprio direito teve que ser estendido para dar conta da nova esfera de vida que clamava por reconhecimento” (THIBES, 2017, p. 322).

A privacidade se torna o direito de proteger seus bens materiais e sua personalidade. Ela é afirmada no momento em que o indivíduo tem controle das suas informações e sabe quem possui acesso a elas e como elas são utilizadas, sendo que essa consciência significa, de forma concreta, ter poder sobre si mesmo. Não cabe mais limitar a privacidade ao “direito a ser deixado só”. Todas as mudanças que vivemos e continuaremos a viver exige ampliação progressiva da esfera do privado e análise mais abstrata do que deve ser resguardado.

Apesar de se tornar cada vez mais um direito que busca bases filosóficas, o ministro do Supremo Tribunal Federal (STF), Gilmar Mendes, pondera que

não basta, assim, que um direito encontre bons motivos filosóficos, aceitos no momento, para ser positivado; é indispensável, ainda, o concurso de condições sociais e históricas favoráveis para que se incorpore aos estatutos vinculantes. (MENDES; BRANCO, 2016, p. 138).

Por isso, o momento histórico e cultural também tem papel importante na fixação de um direito.

O grande número de dados que circulam atualmente deve ser objeto de proteção e não pode ser negligenciado. Na estrutura contemporânea de sociedade, a definição de privacidade tem de ser funcional e, principalmente, necessita fazer referência à possibilidade do detentor do direito de conhecer, controlar, endereçar e interromper o fluxo de informações a ele relacionadas (MACHADO, 2014).

Na legislação brasileira, o direito à privacidade está no rol dos direitos fundamentais da Constituição Federal no artigo 5º, incisos X, XI, XIV e, mais recentemente, no LXXIX. Eles determinam, respectivamente, que:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;  
LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (BRASIL, 1988)

A inclusão do inciso LXXIX demonstra a busca por atualizar os objetos que devem ser protegidos. Com isso, já é possível afirmar que os dados pessoais são elementos essenciais da personalidade e da cidadania e, o que antes era uma parte menos desenvolvida da privacidade, toma seu lugar de importância e também auxilia na criação de uma cultura nacional de proteção de dados pessoais (COALIZÃO NA REDE, 2021).

A pesquisadora Joana Machado, da Universidade Federal do Piauí, afirma que “há muito tempo se vem reconhecendo que a informação é um bem jurídico de valor extraordinário” (MACHADO, 2014, p. 354). Assim sendo, é natural que o direito se posicione e determine novas medidas de proteção para o assunto, o Marco Civil da Internet (Lei 12.965/14) e a Lei Geral de Proteção de Dados (Lei 13.709/18) também demonstram isso.

Mesmo antes da inclusão da proteção de dados na Constituição Federal como um direito fundamental, o Supremo Tribunal Federal já havia reconhecido a importância da proteção dos dados como uma afirmação do direito fundamental à privacidade, uma interpretação ampliada do direito à intimidade, da vida privada, da honra e da imagem das pessoas, na liminar da Ação Direta de Inconstitucionalidade n. 6.387, sustentando que:

A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.(ADI, 2020, p. 20)

Estamos vivendo, como Bauman (2016) afirma, um momento interregno em que as velhas instituições estão morrendo e as novas ainda não nasceram, e esse processo de transição é profundo e acelerado por causa da tecnologia, o que antes na história eram mudanças lineares, hoje são transformações aceleradas. Novos paradigmas apareceram e é preciso que todas as áreas estejam preparadas para novas teorias, comportamentos e, no tópico em específico, legislações.

## CAPÍTULO 3 PESQUISA EMPÍRICA

### 3.1 O questionário

Os capítulos anteriores nos permitiram compreender quais foram as atualizações realizadas pela empresa Meta, Inc. no WhatsApp e porque estudiosos da proteção de dados demonstraram preocupação com as consequências dessas mudanças, bem como apontamentos sobre o que é a vigilância de dados e quais suas ferramentas utilizadas e, por fim, o motivo da proteção dos dados pessoais se tornarem um direito fundamental.

Neste capítulo, iremos descrever as técnicas e as etapas de pesquisa que permitem responder às questões-problema central deste estudo: se os e as estudantes da Universidade de Brasília possuem conhecimento das alterações realizadas pelo WhatsApp, se a comunicação sobre as alterações realizadas pelo aplicativo foram feitas de maneira eficiente, se os/as estudantes compreendem a importância do documento legal que é a política de privacidade e quais ações praticam para proteger seus dados pessoais e, por consequência, exercer seu direito à privacidade.

A escolha de estudantes da Universidade de Brasília deve-se a dois motivos: são próximos/as do universo da autora do estudo, facilitando o contato e a exequibilidade do trabalho, e, por serem universitários, teoricamente deveriam ter mais conhecimento e informação sobre o tema e, portanto, valorizá-lo. Levando em consideração as limitações de tempo e recursos, foi escolhida a elaboração de uma pesquisa quantitativa-descritiva com 200 universitários por meio de um questionário *survey*.

O pesquisador Antonio Carlos Gil explica que a pesquisa descritiva “tem por objetivo levantar as opiniões, atitudes e crenças de uma população” (GIL, 2002) e será possível recolher essas informações por meio de pesquisa *survey*. Já Pinsonneault e Kraener (1993) classificam esse tipo de pesquisa quanto ao seu propósito, no caso da descritiva ela

busca identificar quais situações, eventos, atitudes ou opiniões estão manifestos em uma população; descreve a distribuição de algum fenômeno na população ou, ainda, faz uma comparação entre essas distribuições. Neste tipo de *survey* a hipótese não é causal, mas tem o propósito de verificar se a percepção dos fatos está ou não de acordo com a realidade. (GIL *apud* PINSONNEAULT e KRAENER, 1993, p.106)

O questionário foi realizado pelo *Google Forms* e disparado em grupos de alunos da UnB e redes sociais. Devido ao curto prazo, foi delimitado 10 dias para a aplicação, entre os dias 23 de março e 04 de abril de 2022, e ao todo possuía 20 perguntas, entre elas 7 traçaram o perfil dos entrevistados, questionando idade, gênero e curso universitário e as demais

abordaram pontos pertinentes para o tema da pesquisa, se o estudante tinha conhecimento sobre as mudanças realizadas e o comportamento dos estudantes na internet<sup>10</sup>.

### *3.2 Análise dos dados*

O questionário ficou aberto no período de uma semana, entre os dias 28 de maio ao dia 04 de abril e teve o objetivo de coletar informações sobre o grau de conhecimento dos estudantes de graduação da Universidade de Brasília sobre as mudanças ocorridas na política de privacidade do aplicativo de mensagens WhatsApp e também se há certa compreensão com relação aos termos “vigilância de dados” e “coleta de dados”.

Dos estudantes que responderam o questionário, 91,5% estão na faixa etária de 18 a 25 anos, 4,5% entre os 26 e 30 anos, 2,5% com 31 anos ou mais e apenas 1,5% com 17 anos ou menos. O gênero predominante foi o feminino, com 62%, logo após o masculino, com 36%. A opção “outros” foi assinalada por 1,5% e, por fim, 0,5% se declararam não-binários.

O questionário alcançou as três áreas macros dos cursos de graduação, mas teve um número expressivo de estudantes da área de ciências humanas, com 63,5% das respostas, seguido de ciências biológicas (22%) e, por fim, cursos de ciências exatas (14,5%). Com relação ao grau de formação dos alunos, 56% estão nos quatro primeiros semestres da graduação, 19,5% estão entre o 5º e o 6º semestres e 21% estão nos últimos semestres de seu respectivo curso.

A maioria (75%) dos alunos possui acesso à internet há mais de 10 anos, sendo que 22,5% passaram a entrar na rede mundial de computadores entre 6 e 10 anos atrás e apenas 2,5% assinalaram que têm menos de 5 anos de uso da tecnologia. Cem por cento dos alunos sinalizaram que acessam a internet todos os dias. Esses dados qualificam os estudantes da Universidade de Brasília como usuários assíduos e familiarizados com o ambiente da internet.

Ao questionar qual o principal aplicativo de mensagem utilizado pelos estudantes, 96,5% afirmaram que acessam com mais frequência o WhatsApp e o restante utiliza dois outros aplicativos, 3% estão no Telegram e 0,5% no Instagram Messenger. A partir dessa pergunta, a segunda parte do questionário dividiu os estudantes entre os que utilizavam o WhatsApp como principal aplicativo de mensagens, totalizando 193 estudantes, e os que escolheram outro, apenas sete estudantes.

Iniciando a análise pelas respostas dos estudantes que usam o WhatsApp, foi questionado primeiramente o principal motivo para que o aplicativo fosse o mais acessado. A

---

<sup>10</sup> As perguntas do questionário estão localizadas na íntegra, no apêndice do trabalho.

resposta mais comum (97,4%) é o fato de a maioria dos amigos e familiares estarem no aplicativo, seguida das funcionalidades do aplicativo (31,6%), como as chamadas de voz e vídeo e em terceiro lugar por não consumir os planos de dados dos estudantes (31,1%).

Esse levantamento reforça a premissa de que o WhatsApp se tornou uma extensão do ambiente social dos usuários, sendo mais um motivo que impede que as pessoas sejam mais críticas com relação à ferramenta e busquem outras opções mais seguras, já que não fazer parte do aplicativo é um risco de exclusão social.

A questão seguinte inicia a temática da nova política de privacidade do aplicativo, a primeira pergunta questiona se os estudantes tiveram conhecimento das alterações realizadas e 71,5% não sabiam que houve mudanças, contra apenas 28,5% que tinham ciência. Mesmo que em torno de 28% dos estudantes saibam das mudanças realizadas pelo aplicativo, apenas 7,3% de fato leram a nova política de privacidade.

Aos estudantes que leram as novas políticas, foi questionado se houve total compreensão das alterações e 50% afirmaram que a comunicação não foi efetiva e por isso não compreenderam todas as mudanças realizadas. Além dessa parcela dos estudantes, 7,1% afirmam que houve compreensão das mudanças, mas apenas após olhar com atenção os novos termos, pois não houve comunicação muito clara. Por fim, 42,9% afirmaram que compreenderam a comunicação e que ela foi feita de forma clara.

Com relação aos estudantes que não leram os novos termos, a maioria (65,9%) afirmou que não teve interesse em ler, enquanto 25,7% não sabiam das alterações que ocorreram. Nas respostas abertas, os estudantes responderam que não leram por preguiça, por não terem interesse, porque a leitura é densa e demorada, por terem a possibilidade de ler alguns resumos na internet e também por saberem que independentemente das mudanças realizadas pelo aplicativo não existe a possibilidade de negociação ou mudança e que o aplicativo já se tornou indispensável na vida deles e delas.

As respostas reforçam que não existe ainda uma preocupação sobre o que o aplicativo pode ou não fazer com os dados que são produzidos nele e, por outro lado, se aceitou a falta de liberdade de escolha, pois ter acesso ou não à política de privacidade não determina as ações realizadas pelos usuários, ou seja, não importa compreender todas as mudanças realizadas já que não há espaço para modificações. Além desses pontos, pondera-se que o conteúdo da política de privacidade e a divulgação realizada para os usuários não respeitam os princípios da Lei Geral de Proteção de Dados Pessoais, que determina a garantia de que os usuários tenham fácil acesso e compreensão do documento.

Ao questionar especificamente sobre o WhatsApp Business, a aplicação que gerou as mudanças da política de privacidade do aplicativo, um número alto de estudantes já conhece a funcionalidade, 78,8% contra 21,2% que não sabiam dessa nova versão do aplicativo. Quando questionados se alguma empresa já entrou em contato com os respondentes pelo WhatsApp, a porcentagem aumenta para 88,6%. O resultado demonstra que as empresas estão ativas e utilizando as novas funcionalidades, mas uma parcela dos estudantes, cerca de 11%, que já foram contactados não sabem quais são as possíveis consequências desse contato direto.

A partir desse momento do questionário, foram formuladas algumas perguntas abertas, com a intenção de deixar os estudantes aprofundarem sobre o que era questionado de acordo com a própria perspectiva.

A primeira, com o seguinte enunciado: *Você acha interessante receber publicidades personalizadas a partir das suas buscas na internet?*, teve o objetivo de compreender se esse tipo de publicidade, que pode se intensificar devido o acesso ainda maior das empresas às informações produzidas a partir do WhatsApp Business, é vista como positiva ou não pelos estudantes e como eles interpretam essa personalização.

De acordo com as respostas, 45% dos estudantes não gostam de receber esse tipo de publicidade. Nos comentários, os estudantes explicam que com essa personalização sentem que a sua privacidade está sendo invadida, que estão sendo vigiados, perseguidos por pesquisas que fizeram anteriormente; reclamam que a personalização dos anúncios impedem que vejam outros conteúdos ou até mesmo que encontrem produtos e serviços de empresas menores; também surgiu a preocupação com um consumismo que não seria necessário se esse tipo de publicidade não existisse.

Os estudantes que responderam que gostam desse tipo de publicidade mais direcionada fundamentam que a personalização economiza tempo de pesquisa do produto que procuram e que gostam de receber produtos pelos quais realmente se interessam. Um estudante acredita que a personalização diminuiu a quantidade de publicidade que aparece, enquanto três estudantes afirmaram que mesmo sentindo vigiados ainda acham pertinente a personalização.

O questionário também recebeu respostas de estudantes que ainda não tinham certeza sobre o que acham desse tipo de publicidade (10,8%). Nesse grupo, a questão da privacidade também é abordada, um estudante afirma que é incômodo ver sua privacidade tão exposta e outro declara que às vezes é assustador. Novamente a questão sobre o consumismo desnecessário foi abordado, um estudante afirma que assim como é funcional, às vezes a

publicidade direcionada também o restringe, outro estudante pondera que pode ser interessante receber publicidades mais certeiras, mas chega a ser cansativo.

As respostas demonstram um equilíbrio entre os estudantes que acham vantajoso o alcance das publicidades personalizadas e os que se sentem incomodados por elas, mas até mesmo os que afirmam se interessar por esse tipo de publicidade admitem que existe um sentimento de vigilância. Os que ainda não formaram uma opinião clara sobre o assunto também abordam questões sobre falta de privacidade. Dessa forma, é possível constatar o início de uma conscientização sobre o meio em que se é adquirido as informações para o direcionamento da publicidade online.

As duas questões seguintes abordam sobre a segurança ao utilizar os serviços do WhatsApp. A primeira pergunta é sobre a segurança com relação às conversas realizadas dentro do aplicativo: 58,2% dos estudantes afirmam que acreditam que suas conversas estão seguras, enquanto 35,2% declaram que as mensagens não estão seguras e 6,2% não sabem dizer. Quando questionados se seus dados, como número de telefone, foto de perfil, status e localização, estão seguros, o resultado se inverte, 61,6% acreditam que esses dados não estão seguros, 34,7% afirmam segurança e 3,6% não sabem dizer.

Esse resultado demonstra que parcela considerável dos estudantes possui certa desconfiança sobre o compartilhamento dos dados pelo aplicativo mesmo que não tenham total conhecimento sobre o documento de política de privacidade. No entanto, as respostas às perguntas seguintes podem demonstrar que, mesmo sabendo da possibilidade desse compartilhamento, ainda não há uma compreensão muito clara sobre a vigilância de dados e a falta desse conhecimento pode acarretar em aceites com consequências ignoradas.

As últimas perguntas têm o objetivo de saber qual o nível de conhecimento dos estudantes sobre o termo vigilância de dados e o que vem em mente quando eles se deparam com essas expressões. A palavra “segurança” apareceu em 44 respostas, nelas os estudantes explicam que acreditam que o termo esteja relacionado a manter os dados seguros. Nessa mesma linha, a palavra “proteção” apareceu em 17 respostas, as quais sinalizam que a vigilância seja uma maneira de proteção dos dados; outras respostas interpretam a expressão “vigilância de dados” como um monitoramento para evitar o vazamento de dados.

Os estudantes que abordaram a vigilância dos dados como uma forma de controle, não indicaram que ele seria sobre os titulares dos dados, mas apenas um controle das informações coletadas. Isso pode demonstrar que os estudantes se afastam dos dados que produzem na internet, como se os dados não falassem sobre eles mesmos e não pudessem ter consequências em sua vida offline.

Apenas um estudante conectou a pergunta com o livro *1984*, de Orwell, e outro com o panóptico de Michel Foucault, tipo de vigilância que abordamos anteriormente e que possui conexão direta ao termo. A construção de um perfil detalhado e o rastreamento de comportamento foi abordado por dois estudantes, que compreendem a vigilância de dados como o caminho para obter dados e produzir informações mais específicas dos usuários.

Por fim, as duas últimas perguntas questionam sobre ações concretas que os estudantes costumam adotar para proteger seus dados pessoais. A primeira pergunta tinha o seguinte enunciado: *Você toma algum cuidado para proteger seus dados pessoais na internet? Quais cuidados?*. Com relação a internet no geral, 54 estudantes, 27,9% da amostra, afirmaram não adotar nenhum tipo de ação para proteger seus dados. Uma das respostas ilustra a ideia trazida pelo sociólogo David Lyon (2017), de que os usuários acreditam que, por não terem nada a esconder, não é preciso se preocupar com seus dados pessoais: “Não me atendo tanto a isso, pois não me sinto tão coagida, já que não pesquiso coisas absurdas ou falo coisas esquisitas”, traz uma declaração. Outras duas respostas exemplificam a sensação de que não há nada que se possa fazer para se proteger: “Honestamente nem tanto. Sinto que como já estou inserida em redes sociais, uso aplicativos, e-mail e outras ferramentas, os dados já estão expostos de certa maneira, logo a privacidade ou anonimato completo não é possível. Evito ao máximo cruzar a mesma conta em diferentes aplicativos (exemplo de fazer login com conta do google), porém é mais uma precaução caso seja roubada a conta ou aconteça algo”. Complementa a ideia da afirmação: “sinto que não adianta nada, que já vou estar exposto por possíveis vazamentos etc”.

Os demais estudantes incluíram em suas respostas vários cuidados que afirmaram ter, como a exclusão de histórico de buscas, navegação em abas anônimas, elaboração de senhas não convencionais, bem como evitam aceitar cookies de sites, mantêm antivírus atualizados e acessam a internet por meio de redes virtuais privadas.

Por último, a pergunta *No aplicativo de mensagens WhatsApp, você toma algum cuidado para proteger seus dados pessoais? Quais cuidados?* especifica ações dentro do aplicativo de mensagem e indicam que as maneiras de proteção respondidas pelos estudantes já se tornam mais reduzidas; 96 estudantes afirmaram não adotar nenhum tipo de cuidado, os demais se restringiram às ações disponibilizadas pelo próprio aplicativo, como a verificação em duas etapas, criptografia de ponta a ponta, inclusão de senhas, limitação para visualizar foto de perfil e privar status.

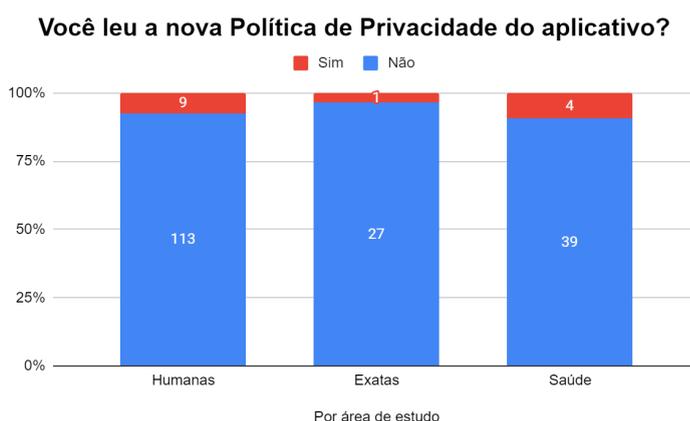
Quando se questiona ações de proteção dentro do aplicativo, fica claro que existe uma limitação pela própria ferramenta de se fazer algo com relação a isso, como demonstrado

durante a pesquisa, a única opção dada pelo aplicativo para recusar a nova política de privacidade ficou ativa por apenas 30 dias, durante esse período o usuário poderia recusar as modificações e se retirar do WhatsApp, após o prazo todos que permanecessem estariam aceitando as novas diretrizes. Além da falta de opções de agir para proteger seus dados, fazer algo também não parece ser uma atividade óbvia, não é claro aos usuários que, enquanto estão no aplicativo, estão entregando dados para a plataforma.

Dos 200 estudantes que responderam ao questionário, apenas sete afirmaram não utilizar o WhatsApp como principal rede de troca de mensagens. Quando questionados sobre o motivo, quatro estudantes justificaram que o Telegram possui mais funcionalidades e é uma verdadeira rede social, não se limitando apenas à troca de mensagens e status, como no WhatsApp. Os demais respondentes disseram não utilizar o WhatsApp por conta da quantidade limitada de grupos, por trabalhar mais no Telegram e por ter a possibilidade de conectar dois celulares simultaneamente, com a mesma conta, além de utilizar mais o aparelho que possui outro aplicativo.

Após a análise em separado de cada resposta, é viável cruzar alguns dados e identificar se as áreas de formação dos estudantes e o semestre podem alterar a percepção quanto às principais questões do trabalho. Quando analisamos os resultados de cada área macro de graduação sobre a leitura da nova política de privacidade do WhatsApp, constata-se que em todas as áreas mais de 90% dos estudantes não acessaram as diretrizes.

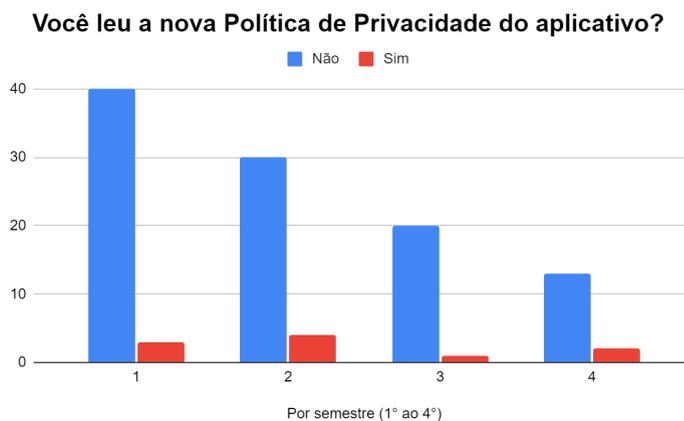
**Gráfico 1:** Estudantes que acessaram a nova política de privacidade do WhatsApp.



Fonte: Elaboração própria.

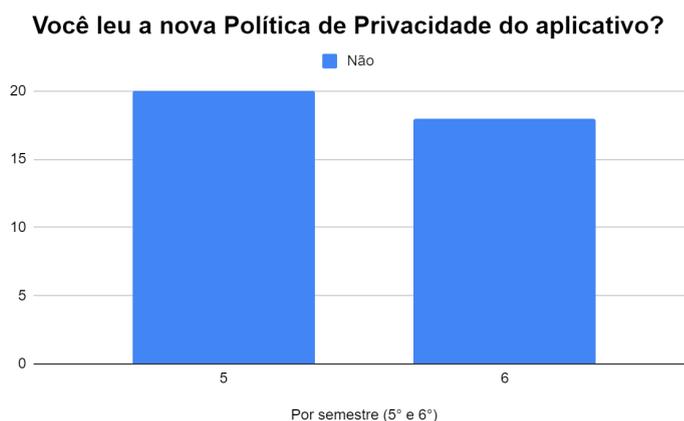
Analisando a mesma questão, mas com foco nas respostas de estudantes na divisão por período de curso, dos 14 semestres presentes na pesquisa, apenas em 7 alguns alunos chegaram a ler os novos termos.

**Gráfico 2:** Estudantes dos primeiros semestres de faculdade que leram a nova política de privacidade do WhatsApp.



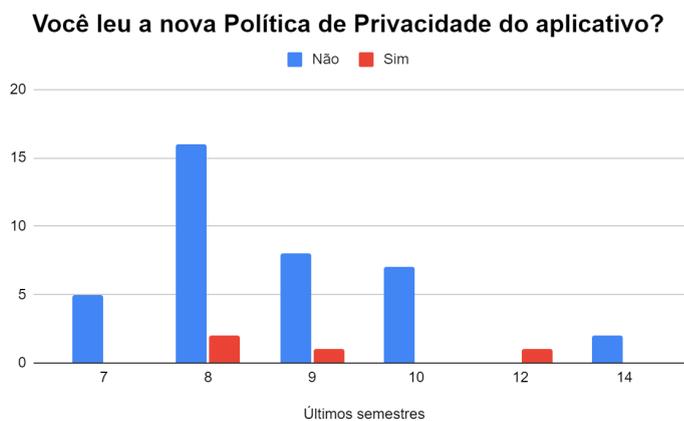
Fonte: Elaboração própria.

**Gráfico 3:** Estudantes do quinto e sexto semestre de faculdade que leram a nova política de privacidade do WhatsApp.



Fonte: Elaboração própria.

**Gráfico 4:** Estudantes dos últimos semestres de faculdade que leram a nova política de privacidade do WhatsApp.

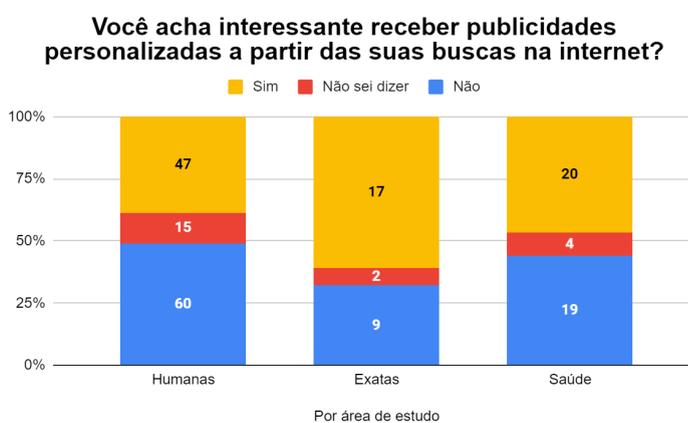


Fonte: Elaboração própria.

Esse cenário mostra que, ao contrário da expectativa de que estudantes com mais tempo de curso pudessem ter postura mais cautelosa em relação às políticas de privacidade, o recorte por período de graduação revela que não há interferência do critério quanto à questão perguntada, independentemente do grau de maturidade de cada um.

Sobre a questão relacionada ao interesse em receber propagandas personalizadas, as respostas apresentaram maior variação. Os estudantes de humanas se mostraram mais insatisfeitos com esse tipo de publicidade quando comparado com os estudantes das outras áreas.

**Gráfico 5:** Estudantes que se interessam por publicidade personalizada.



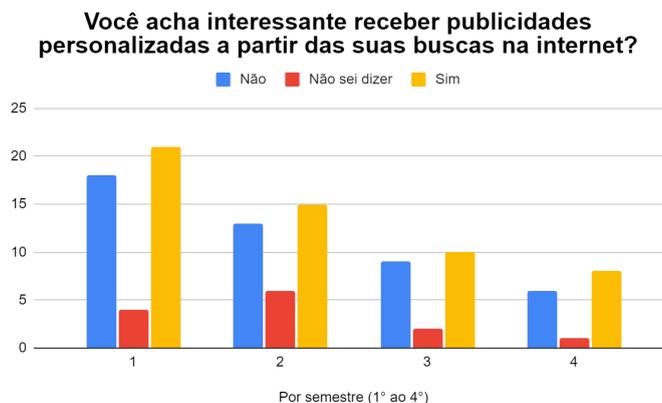
Fonte: Elaboração própria.

Apresentando o resultado em porcentagem, 49% dos estudantes de humanas não acham vantajoso o recebimento de publicidade personalizada, enquanto 44% dos estudantes de saúde e 32% dos estudantes de exatas também não se interessam por esse tipo de propaganda. Os números de estudantes que ainda não possuem opinião formada sobre o assunto também demonstra que os alunos de humanas possuem mais dúvida do que os das outras áreas, enquanto 12% da área de humanas não sabem opinar sobre o assunto, apenas 7% da área de exatas e 9% da área de humanas declara o mesmo.

Novamente, agregando as respostas de acordo com o semestre de cada estudante, os primeiros semestres – do primeiro ao quarto – a maioria dos alunos confirmaram gostar desse tipo de prática de publicidade. Os estudantes do quinto ao oitavo semestres possuem uma opinião contrária, não se sentindo confortáveis com publicidade personalizada, por fim, os estudantes do nono e décimo semestres seguem a mesma linha dos primeiros semestres, e os

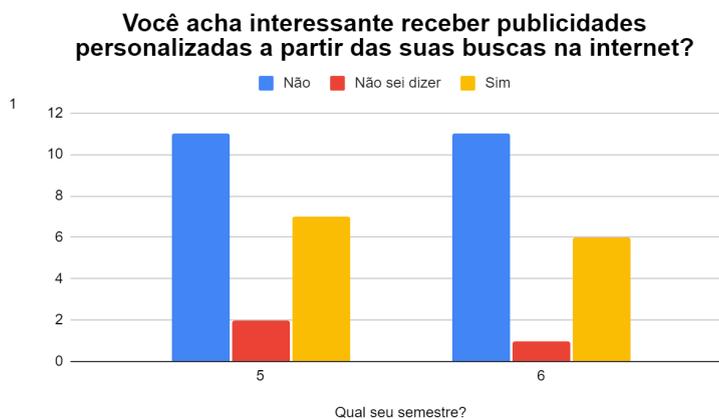
do décimo segundo e décimo quarto semestres não se interessam ou não sabem dizer, lembrando que a quantidade de estudantes respondentes destes últimos grupos é menor quando comparada aos demais.

**Gráfico 6:** Estudantes dos primeiros semestres que se interessam por publicidade personalizada.



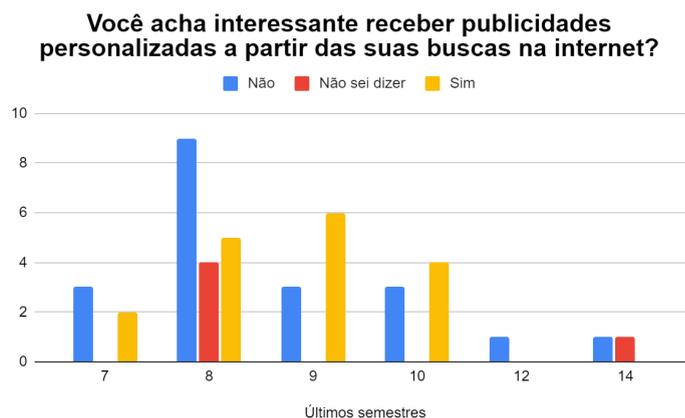
Fonte: Elaboração própria.

**Gráfico 7:** Estudantes do quinto e sexto semestre que se interessam por publicidade personalizada.



Fonte: Elaboração própria.

**Gráfico 8:** Estudantes dos últimos semestres que se interessam por publicidade personalizada.

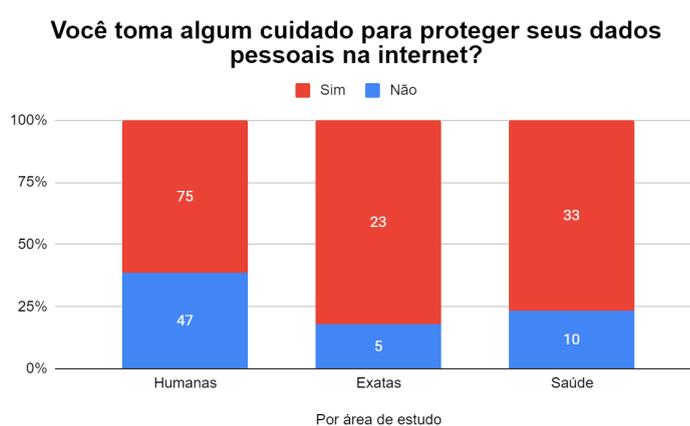


Fonte: Elaboração própria.

Por último, ao cruzarmos os dados dos estudantes que responderam sobre a adoção de algum cuidado para proteger seus dados pessoais na internet, é possível constatar uma informação curiosa: os estudantes que menos agem para proteger seus dados na internet são os da área de humanas – os mesmos que mais se colocaram contra a publicidade personalizada – e os estudantes de exatas são os que mais investem em proteger seus dados no ambiente online.

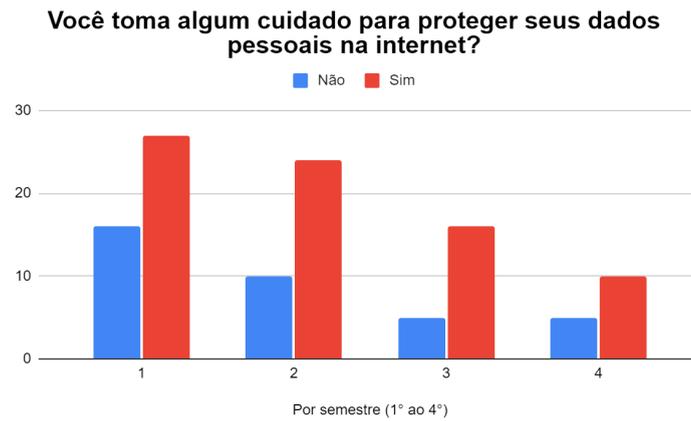
Ao analisar esses mesmos dados na distribuição por semestre cursado, em todos os segmentos, a maioria dos estudantes está atenta e busca proteger seus dados de alguma forma.

**Gráfico 9:** Estudantes dos primeiros semestres que tomam algum cuidado para proteger seus dados pessoais na internet.



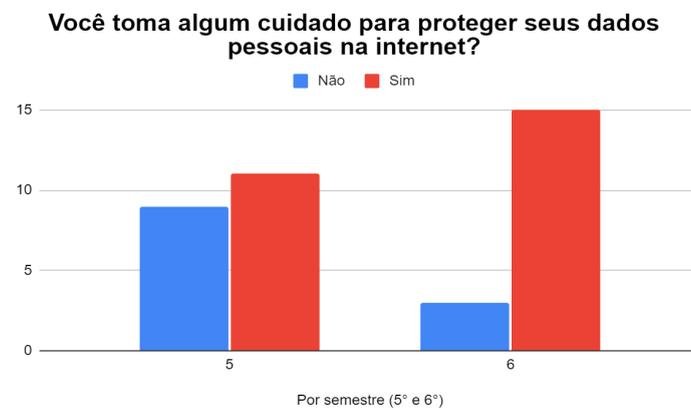
Fonte: Elaboração própria.

**Gráfico 10:** Estudantes dos primeiros semestres que tomam algum cuidado para proteger seus dados pessoais na internet.



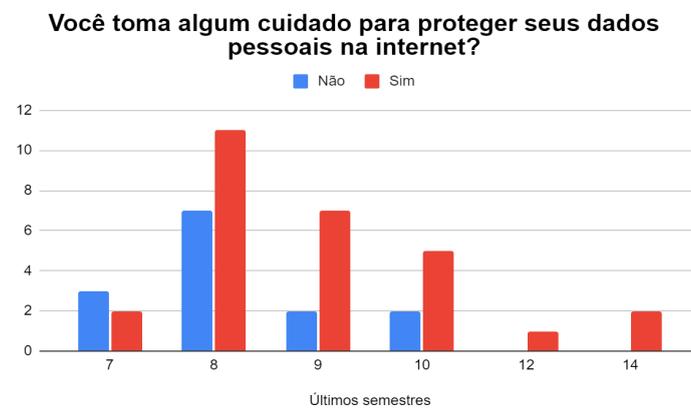
Fonte: Elaboração própria.

**Gráfico 11:** Estudantes do quinto e sexto semestre que tomam algum cuidado para proteger seus dados pessoais na internet.



Fonte: Elaboração própria.

**Gráfico 12:** Estudantes dos últimos semestres que tomam algum cuidado para proteger seus dados pessoais na internet.



Fonte: Elaboração própria.

As respostas ao questionário comprovam a necessidade de uma educação mais ativa sobre as várias temáticas que envolvem a internet. Mesmo que os estudantes da Universidade

de Brasília sejam usuários extremamente presentes e ativos na rede, nota-se que esse perfil não é sinônimo de usuários conscientes sobre as consequências que a falta de cuidado com seus dados pessoais podem acarretar.

O Estado deve se posicionar como ator principal na divulgação e conscientização sobre a Lei Geral de Proteção de Dados e na elaboração de mecanismos de educação digital. Não por acaso a proteção de dados se tornou direito fundamental e deve ser protegido, ainda mais por se tratar de direito que pode ser facilmente violado, tendo em vista que a sua coleta, sobretudo pelas grandes empresas de tecnologia, na maioria das vezes é feita sem grandes obstáculos.

#### 4. CONSIDERAÇÕES FINAIS

A internet sempre contou com defensores otimistas, que se empenham em argumentar a favor de seus mecanismos, acreditando que a tecnologia é caminho de libertação; e que os usuários são capazes de avaliar, por conta própria, as consequências das suas ações no ambiente online, ignorando os riscos e externalidades que caminham junto com a conectividade. Por outro lado, existem teóricos que analisam com muito receio e cautela todos os avanços da internet em um cenário que já demonstrou a falta de maturidade necessária dos usuários para se protegerem no ambiente online, as questões estruturais do capitalismo de vigilância que entrega as empresas o poder de definir as regras, dinâmicas e lógicas de funcionamento e a relação “imposta” aos cidadãos para que possam fazer parte desse ambiente.

O presente trabalho reconhece que a internet é um marco importante para os avanços tecnológicos que vivemos e que, em si, não é o grande problema; propor uma análise crítica do modelo que estamos inseridos não tem a pretensão de convencer que todas as vantagens advindas da conectividade não devam ser usufruídas, mas reconhecer que o cenário atual não é o ideal para proteção do lado mais fraco da relação, os usuários, e procurar por mais consciência e soluções é responsabilidade da academia.

O questionário aplicado foi direcionado aos estudantes da Universidade de Brasília que possuem um perfil de usuários assíduos da internet, com acesso a educação de qualidade, em um grande centro urbano, e que passaram por processos seletivos rigorosos. Se comparada aos estudantes das demais universidades federais, a UnB tem um dos menores percentuais de discentes que vivem com renda familiar mensal abaixo de um salário mínimo e meio (CAMPUS, 2019), refletindo diretamente na facilidade de acesso à informação e conhecimento.

Mesmo com todas essas características, a pesquisa demonstrou que ainda existe dificuldade em conscientizar e educar esse público sobre os riscos e a importância da proteção de dados. Pode-se levantar a hipótese de que, se em uma parcela da sociedade que possui todos os meios para se capacitar sobre o assunto ainda há resistência à adoção de cuidados básicos, a faixa socioeconômica menos privilegiada pode apresentar resultados ainda mais desafiadores.

Vivemos em um momento de transição no modelo comercial da internet. Se no início ele não era muito claro, hoje passa a ser melhor compreendido e os efeitos colaterais desse modelo começam a surgir; a quantidade de dados que nunca estiveram tão disponíveis antes, passam a ser o caminho utilizado por grandes empresas para ativar gatilhos de

comportamento e influenciar ações. Nesse momento, ter leis e um Estado que se posicione como agente ativo de fiscalização da utilização desses dados é essencial para conseguir administrar a complexidade desses novos avanços, é preciso que haja a implementação de políticas públicas e normativos legais regulatórios do ambiente online, pois já está demonstrado que a autorregulação não é um caminho que oferece segurança aos usuários.

Além disso, as organizações públicas e privadas, o terceiro setor e, novamente, o Estado precisam se apresentar como parceiros dos usuários da internet que não possuem conhecimento necessário sobre os efeitos de sua exposição no ambiente online. Esse apoio pode se dar por meio da intensificação da divulgação das leis que asseguram o direito de proteção dos dados, a simplificação dos vocabulário da internet para alcançar mais pessoas e a promoção de eventos educacionais sobre o assunto, de forma a tornar o usuário mais crítico e habilitado a opinar e decidir de forma consciente sobre o destino de seus dados. Mesmo com essas soluções, é preciso ter em mente que toda a maneira de educação também deve sofrer modificações, pois estamos lidando com uma realidade completamente nova que ainda experimenta os caminhos a serem seguidos.

Enquanto os usuários não passarem a ser os protagonistas das decisões sobre seus dados, as empresas continuarão os utilizando como mercadoria e, por ainda não termos condições de identificar a longo prazo as consequências dessa quantidade crescente de dados na mão de grandes empresas, as liberdades individuais permanecem em risco.

A pesquisa não tinha a pretensão de abordar todos os pontos importantes do debate sobre o tema, seja devido a questão da limitação do tempo para a finalização do trabalho e porque o tema pode levar a diversos caminhos e abordagens, por isso, ainda há muito o que se aprofundar sobre o assunto. Quais os próximos passos das empresas que se beneficiam desse modelo econômico; como respondem a usuários mais conscientes dos riscos; quais as dificuldades dos usuários que se encontram em realidades diferentes daquela apresentada pelos estudantes universitários, mas que, assim como eles, estão cada vez mais inseridos no mundo virtual; e como comunicar de forma mais eficiente sobre o assunto são questões que ainda precisam de respostas.

Por fim, a proteção dos dados estará cada vez mais no centro dos debates sobre a vida em sociedade, por isso, é preciso compreender o quanto as pessoas estão dispostas a abrir mão da sua segurança para ter mais conectividade ou o quanto estão dispostas a abrir mão da sua conectividade para ter mais segurança. Zygmunt Bauman, em entrevista, afirmou que nunca encontraremos uma solução perfeita para o dilema entre a segurança e a liberdade, pois

sempre haverá muito de um e pouco de outro. No entanto, nunca devemos parar de buscar essa mina de ouro (BAUMAN, 2013).

## REFERÊNCIAS

AGRELA, Lucas. **'Respeito pela sua privacidade está codificado em nosso DNA', diz CEO do WhatsApp**: aplicativo armazena apenas número de telefone e quais contatos do usuário também usam o serviço. Aplicativo armazena apenas número de telefone e quais contatos do usuário também usam o serviço. 2014. Disponível em: <<https://www.google.com/url?q=https://exame.com/tecnologia/respeito-pela-sua-privacidade-esta-codificado-em-nosso-dna-diz-ceo-do-whatsapp/&sa=D&source=docs&ust=1650163153094779&usg=AOvVaw0m4k9QnMI7ukpHD03Xw6jr>>. Acesso em: 17 mar 2022

ANPD. Nota Técnica n 2/2021 de 22 mar de 2021. **Atualização da Política de Privacidade do WhatsApp**. Disponível em: <<https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf>>. Acesso em: 01 mar 2022.

BAUMAN, Zygmunt. **IDEIAS DO MILÊNIO: "Estamos num estado de interregno. Vivemos na modernidade líquida"**. GloboNews. Marcelo Lins, Milênio. Disponível em: <<https://www.conjur.com.br/2016-jan-01/zygmunt-bauman-neste-seculo-estamos-num-estado-interregno>>. Acesso em: 10 abr. 2022

BAUMAN, Zygmunt. **Segurança e liberdade: uma dicotomia?**. Youtube, 09 jul. 2013. Disponível em: <<https://www.youtube.com/watch?v=Q3TdhIjBW5Q>>. Acesso em: 14 abr 2022

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União: seção 1, Brasília, DF, ano 130, 14 ago. 2018. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm)>. Acesso em: 23 mar. 2022.

BRASIL. **Supremo Tribunal Federal**. ADI no. 6.387 MC/DF. Relatora: Ministra Rosa Weber.

BRUNO, Fernanda. **Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas**. Disponível em:

<<http://revistas.unisinos.br/index.php/fronteiras/article/view/6129>> Acesso em: 08 março 2022.

CARVALHO, Lucas. **Para criador do Signal, luta contra WhatsApp mira "fim da internet utópica"**. 2021. Disponível em: <<https://www.uol.com.br/tilt/noticias/redacao/2021/04/29/quem-e-o-criador-do-signal-app-que-quer-substituir-o-whatsapp.htm>>. Acesso em: 18 mar. 2022.

CARDOZO, Nate. **Making It Easier to Manage Business Conversations on WhatsApp**. 2020. Disponível em: <<https://about.fb.com/news/2020/10/privacy-matters-whatsapp-business-conversations/>>. Acesso em: 13 mar. 2022

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 2020.

CASTELLS, M. **O poder da comunicação**. São Paulo: Paz e Terra, 2015.

CASTELLS, Manuel. **A democracia está se autodestraindo pela corrupção**. Entrevista concedida a Luís Antônio Giron. ISTOÉ, 13 jul. 2018. Disponível em: <<https://istoe.com.br/a-democracia-esta-se-autodestraindo-pela-corrupcao/>> . Acesso em: 10 mar. 2022.

COALIZÃO DIREITO NAS REDES. PEC 17/2019: **Autonomia para a ANPD e proteção de dados como direito fundamental**. Brasília, 2021. Disponível em: <<https://direitosnarede.org.br/2021/05/24/pec-17-2019-autonomia-para-a-anpd-e-protecao-de-dados-como-direito-fundamental/>>. Acesso em: 24 mar. 2022

COULDRY, Nick; MEJIAS, Ulises A. **The cost of connection: how data is colonizing human life and appropriating it for capitalism**. California: Stanford University Press, 2019.

CURRAN, James and Des Freedman. **Misunderstanding the Internet**, edited by James Curran, and Des Freedman, Taylor and Francis. ProQuest Ebook Central, 2016.

DONEDA, Danilo. **Considerações Iniciais sobre os bancos de dados**. Rio de Janeiro. 2012. Disponível em: <<https://pt.scribd.com/document/106501611/Consideracoes-iniciais-sobre-os-bancos-de-dados-Danilo-Doneda>>. Acesso em: 08 mar. 2022

DUHIGG, Charles. **How Companies Learn Your Secrets**. The New York Times, 2012. Disponível em: <[https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&\\_r=1&hp](https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp)>. Acesso em: 10 fev. 2022

EAESP, FGV. **31ª Pesquisa Anual do FGVcia da FGV/EAESP**. Uso da TI – Tecnologia de Informação nas Empresas. 2020. Disponível em: <[https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti\\_resultados\\_0.pdf](https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti_resultados_0.pdf)>. Acesso em 07 de maio de 2021.p. 64.

FARIA, Julian Affonso de; MAGALHÃES, Cláudio Márcio. **O Capitalismo de Vigilância e a Política da Desinformação**. Interações: Sociedade e as novas modernidades, [S.L.], n. 40, p. 60-79, 30 jun. 2021. Instituto Superior Miguel Torga. <http://dx.doi.org/10.31211/interacoes.n40.2021.a3>. Disponível em: <<https://www.interacoes-ismt.com/index.php/revista/article/view/493>>. Acesso em: 07 mar. 2022.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. **Privacidade e proteção de dados pessoais: perspectiva histórica**. Incid: Revista de Ciência da Informação e Documentação, [S.L.], v. 12, n. 2, p. 151-172, 30 nov. 2021. Universidade de São Paulo, Agência USP de Gestão da Informação Acadêmica (AGUIA). <http://dx.doi.org/10.11606/issn.2178-2075.v12i2p151-172>. Disponível em: <https://brapci.inf.br/index.php/res/v/168517>. Acesso em: 07 mar. 2022.

FUCHS, Christian. **How to define surveillance?** Matrizes, [S.L.], v. 5, n. 1, p. 116, 15 dez. 2011. Universidade de São Paulo, Agência USP de Gestão da Informação Acadêmica (AGUIA). Disponível em: <<https://www.revistas.usp.br/matrizes/article/view/38311>>. Acesso em: 20 mar. 2022.

GILLILAND-SWETLAND, A. J. **Introduction to metadata: Setting the stage**. 2000. Disponível em: <<http://www.slis.kent.edu/~mzeng/metadata/Gilland.pdf>>. Acesso em: Acesso em: 17 mar. 2022.

LYON, David. **Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity**. Disponível em: <<https://ijoc.org/index.php/ijoc/article/viewFile/5527/1933>>. Acesso em: 07 março 2022 p. 825 “It is no longer merely something external that impinges on our lives.”

LANIER, J. **Dez argumentos para você deletar agora suas redes sociais**, Rio de Janeiro: Editora Intrínseca Ltda, 2018.

MACASKILL, Ewen; DANCE, Gabriel. **What the revelations mean for you**. Londres: The Guardian, 2013. Disponível em: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>. Acesso em: 10 jan. 2022.

MACHADO, Joana de Moraes Souza. **A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados**. Disponível em: <<http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/view/206>>. Acesso em: 09 março 2022.

MASTERCARD. **Small Businesses - Big Challenges, Big Opportunities**. 2021. Disponível em: <https://www.mastercardservices.com/en/recovery-insights/small-business-reset/challenges-and-opportunities-around-globe>. Acesso em: 11 mar. 2022.

MENDES, Ferreira Gilmar e BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2014.

**PEC 17/2019: Autonomia para a ANPD e proteção de dados como direito fundamental**. Coalizão Direito nas Redes, 2021. Disponível em:

<<https://direitosnarede.org.br/2021/05/24/pec-17-2019-autonomia-para-a-anpd-e-protecao-de-dados-como-direito-fundamental/>>. Acesso em: 11 mar. 2022.

PAHWA, Aashish. **The History Of WhatsApp**. 2021. Disponível em: <https://www.feedough.com/history-of-whatsapp/>. Acesso em: 23 fev. 2022.

PAHWA, Aashish. **WhatsApp Marketing – An Actionable Guide**. 2021. Disponível em: <<https://www.feedough.com/whatsapp-marketing/>>. Acesso em: 23 jan. 2022.

PAIVA, Fernando (Org.). **Panorama Mobile Time/Opinion Box: Mensageria no Brasil**. 2020. Disponível em: <<https://www.mobiletime.com.br/pesquisas/mensageria-no-brasil-fevereiro-de-2020/>>. Acesso em: 29 abril 2022

**Pesquisa realizada pela ANDIFES indica que mais da metade dos alunos das universidades federais é de baixa renda. Campus online**, 2019. Disponível em: <<https://campus.fac.unb.br/materias/2019-05-20-pesquisa-realizada-pela-andifes-indica-que-mais-da-metade-dos-alunos-das-universidades-federais-e-de-baixa-renda/>>. Acesso em: 15 mar 2022.

REIS, Bruna Sthefany Souza dos. **Você tem WhatsApp?: um estudo sobre a apropriação do aplicativo de celular por jovens universitários de Brasília**. 2013. 83 f., il. Monografia (Bacharelado em Comunicação Organizacional)—Universidade de Brasília, Brasília, 2013.

SIMÕES, Alessandra Lourenço. **Comunicação na internet e a violação do direito à privacidade: uma análise avaliativa das políticas e termos de uso na internet**. 2017. 213 folhas. Dissertação( Comunicação Social) - Universidade Metodista de São Paulo, São Bernardo Campo. Disponível em: <<http://tede.metodista.br/jspui/bitstream/tede/1715/2/Alessandra.pdf>>. Acesso em: 07 mar 2022.

THIBES, Mariana Zanata. **As formas de manifestação da privacidade nos três espíritos do capitalismo: da intimidade burguesa ao exibicionismo de si nas redes sociais**. Sociologias, [S.L.], v. 19, n. 46, p. 316-343, dez. 2017. FapUNIFESP (SciELO).

**The world's most valuable resource is no longer oil, but data. The data economy demands a new approach to antitrust rules.** The Economist, 2017. Disponível em: <<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>>. Acesso em: 13 fev. 2022.

VIANA, Quézia Salles Cabral; SILVA, Guilherme Cavalcante. **Vigilância e monitoramento na era da internet das coisas: um olhar sobre o “paradoxo da privacidade”**. Revista do Edicc, São Paulo, v. 6, n. 1, p. 247-257, 05 jun. 2019. Disponível em: <<https://revistas.iel.unicamp.br/index.php/edicc/issue/view/353>>. Acesso em: 20 fev. 2022.

VIEIRA, Maria Lucia França Pontes. **Pesquisa Nacional por Amostra de Domicílios Contínua**. Rio de Janeiro: IBGE, 2021. 116 p. Disponível em: [https://biblioteca.ibge.gov.br/visualizacao/livros/liv101733\\_notas\\_tecnicas.pdf](https://biblioteca.ibge.gov.br/visualizacao/livros/liv101733_notas_tecnicas.pdf). Acesso em: 11 mar. 2022.

WARZEL, Charlie; MAC, Ryan. **These Confidential Charts Show Why Facebook Bought WhatsApp**: the company was obsessively tracking whatsapp and saw not just a rising competitor but a potential facebook killer.. The company was obsessively tracking WhatsApp and saw not just a rising competitor but a potential Facebook killer.. 2018. Disponível em: <<https://www.buzzfeednews.com/article/charliwarzel/why-facebook-bought-whatsapp>>. Acesso em: 23 fev. 2022.

WHATSAPP. **Sobre a criptografia de ponta a ponta**. 2021. Disponível em: <[https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt\\_br](https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br)>. Acesso em: 13 fev. 2022.

WHATSAPP. **Política de Privacidade do WhatsApp**. 2021. Disponível em: <<https://www.whatsapp.com/legal/privacy-policy>>. Acesso em: 28 fev. 2022.

## APÊNDICE

### Questionário *survey* aplicado pelo estudo

#### 1. Qual a sua faixa etária?

17 ou menos

18 a 25 anos

26 a 30 anos

31 anos ou mais

**2. Qual o seu gênero?**

homem

mulher

não-binário

outro

**3. Qual seu curso universitário?**

**4. Qual seu semestre?**

**5. Há quanto tempo tem acesso à internet?**

menos de 1 ano

2 a 5 anos

6 a 10 anos

mais de 10 anos

**6. Qual a frequência que você acessa à internet?**

todos os dias

5 vezes por semana

2 a 3 vezes por semana

1 vez por mês

Outro:

**7. Você utiliza algum aplicativo de troca de mensagens, assinale o que utiliza com mais frequência:**

- WhatsApp
- Messenger
- Telegram
- Signal
- Instagram Messenger
- Não utilizo aplicativos de mensagem

**Fim para os que não utilizam o WhatsApp como principal – questão “por que você não utiliza o WhatsApp como aplicativo principal para troca de mensagens?”**

**8. Por que você optou por utilizar o WhatsApp? Pode ser selecionada mais de uma opção.**

Não consome meu plano de dados

Maioria dos amigos e familiares utilizam

Não conheço outros aplicativos

Exigência do trabalho

Pelas funcionalidades

Outro:

**9. O aplicativo lançou em 2021 uma nova política de privacidade do aplicativo. Você teve conhecimento dessas alterações?**

Sim

Não

**10. Você leu a nova política de privacidade do aplicativo?**

Sim

Não

**11. Caso tenha lido, você teve total compreensão das alterações feitas pelo aplicativo?**

sim, a comunicação foi clara e compreendi as mudanças realizadas

não, a comunicação não foi efetiva, não compreendi todas as mudanças realizadas

Outro:

**12. Caso não tenha lido, o que te impediu de ler as novas políticas de privacidade?**

não soube que houve alterações

não tive interesse em ler

não sei onde encontrar a política de privacidade do aplicativo

Outro:

**13. Você conhece a função WhatsApp Business?**

Sim

Não

**14. Alguma empresa já contactou você pelo WhatsApp?**

Sim

Não

**15. Você acha interessante receber publicidades personalizadas a partir das suas buscas na internet?**

Sim

Não

Outro

**16. Ao utilizar o WhatsApp, você sente que suas conversas estão seguras?**

Sim

Não

Outro:

**17. Ao utilizar o WhatsApp, você sente que seus dados (número de telefone, foto de perfil, status, localização) estão seguros?**

Sim

Não

Outro

**18. Você tem familiaridade com o termo “vigilância de dados”?**

**19. Você toma algum cuidado para proteger seus dados pessoais na internet? Quais cuidados seriam?**

**20. No aplicativo de mensagens WhatsApp, você toma algum cuidado para proteger seus dados pessoais? Quais cuidados são?**