

**UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS**  
**UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS DA COMUNICAÇÃO**  
**NÍVEL DOUTORADO**

**ROBERTA FLECK SAIBRO KRAUSE**

**SENTIDOS DE *TECNOSEGURANÇA* PELA AMBIÊNCIA FACEBOOK**

**São Leopoldo**

**2022**

ROBERTA FLECK SAIBRO KRAUSE

**SENTIDOS DE *TECNOSEGURANÇA* PELA AMBIÊNCIA FACEBOOK**

Tese apresentada como requisito parcial para obtenção do título de Doutora em Comunicação, pelo Programa de Pós-Graduação em Ciências Comunicação da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientadores: Profa. Dra. Sonia Estela Montaña La Cruz  
Prof. Dr. Tiago Ricciardi Correa Lopes

São Leopoldo

2022

K91s Krause, Roberta Fleck Saibro.

Sentidos de tecnosegurança pela ambiência facebook /  
Roberta Fleck Saibro Krause. – 2022.

229 f. : il. ; 30 cm.

Tese (doutorado) – Universidade do Vale do Rio dos Sinos,  
Programa de Pós-Graduação em Ciências Comunicação, 2022.

“Orientadores: Profa. Dra. Sonia Estela Montañó La  
Cruz Prof. Dr. Tiago Ricciardi Correa Lopes.”

1. Tecnosegurança. 2. Interface. 3. Facebook. 4. Segurança.  
5. Tecnocultura. 6. Imagem. I. Título.

CDU 659.3:004

Dados Internacionais de Catalogação na Publicação (CIP)

(Bibliotecária: Amanda Schuster – CRB 10/2517)

**ROBERTA FLECK SAIBRO KRAUSE FERNANDES**  
**SENTIDOS DE TECNOSEGURANÇA PELA AMBIÊNCIA FACEBOOK**

Tese apresentada como requisito parcial para obtenção do título de Doutor, pelo Programa de Pós-Graduação em Ciências da Comunicação da Universidade do Vale do Rio dos Sinos - UNISINOS.

**APROVADA EM 21 DE OUTUBRO de 2022.**

**BANCA EXAMINADORA**

**PROF. DR. JOÃO LADEIRA - UFPR**  
**(PARTICIPAÇÃO POR WEBCONFERÊNCIA)**

**PROFA. DRA. SARA FEITOSA - UNIPAMPA**  
**(PARTICIPAÇÃO POR WEBCONFERÊNCIA)**

**PROF. DR. GUSTAVO FISCHER - UNISINOS**  
**(PARTICIPAÇÃO POR WEBCONFERÊNCIA)**

**PROF. DR. RONALDO HENN - UNISINOS**  
**(PARTICIPAÇÃO POR WEBCONFERÊNCIA)**

**PROF. DR. TIAGO RICCIARDI CORREA LOPES – ORIENTADORA**  
**(PARTICIPAÇÃO POR WEBCONFERÊNCIA)**



---



## **AGRADECIMENTOS À CAPES**

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

*Para o amor da minha vida, minha filha Valentina.*

## AGRADECIMENTOS

Aos meus pais, Sandra e Paulo, pela vida, pelo amor, carinho, educação e pelas constantes palavras de apoio desde os momentos mais angustiantes às celebrações em minha vida.

Ao meu marido, Otávio, pelo companheirismo, gigantesca paciência, suporte, bom-humor e estímulo ao meu desenvolvimento como pesquisadora e professora. Agora, volto para nossa família com todo o meu tempo e saudades!

À minha irmã, que sempre apoiou minha formação, auxiliou nos momentos difíceis, escutou, muitas vezes, meus anseios e festejou minhas conquistas.

À minha filha Valentina, que se faz presente em absolutamente todas as páginas dessa tese. Sua gestação foi paralela ao ingresso no doutorado, e, na semana que estou encerrando a tese, com uma alegria que mal cabe em mim, celebro o seu aniversário de 4 anos!

À minha madrinha, Ana Luiza, que apoiou nas leituras, nas produções textuais, nos custos envolvidos nessa entrega final, e no suporte emocional que o doutoramento exige.

Aos colegas da UNISINOS, Camila de Ávila, Aline Corso, Guto Bozetti, Christian Gonzatti, Anaís Bertoni, Marlon Santa Maria e João Damasio. Aos egressos do TCAv que me ajudaram nos momentos mais tensos de encerramento, Daniel Petry e Rafael Tourinho Raymundo.

À orientadora Profa. Dra. Sonia Montañó, que sempre acreditou na minha capacidade, acompanhou e auxiliou na construção dessa tese até sua qualificação.

Ao Prof. Dr. Tiago Lopes, orientador dessa tese, que foi absolutamente essencial, pela disponibilidade e desafio de orientar uma pesquisa em andamento, me acompanhando e conduzindo às reflexões necessárias para que eu pudesse chegar no encerramento do trabalho, sempre com uma forte postura de estímulo, acreditando nas loucuras que proponho nessa investigação.

Ao Prof. Dr. Ronaldo Henn, pela atenta leitura e sugestões encaminhadas na qualificação, visando a melhoria da pesquisa.

Ao Prof. Dr. Gustavo Fischer, pelo apoio em diversos momentos ao longo do curso, tanto em questões profissionais quanto encaminhamentos específicos para o trabalho, desde o seminário de tese até a qualificação, sempre estimulando melhoria constante em meu desenvolvimento como pesquisadora do TCAv.

À Escola Superior de Propaganda e Marketing, e aos meus amigos e gestores, Rene Goellner e Alessandro Souza, pelo apoio e crença na pesquisa, envolvendo diversos aspectos associados ao doutoramento e compreensão em relação às demandas dessa tese.

À CAPES, pela bolsa e oportunidade, ao PPGCC e à UNISINOS.

Por fim, reforço, imensamente, o agradecimento à minha família. Sou bolsista, professora e pesquisadora e saliento que essa tese só foi possível de ser realizada paralelamente à maternidade por eu ter o privilégio de contar com uma **excelente** rede de apoio familiar do meu marido, minha mãe, meu pai e minha irmã, que amo imensamente.

### **Nota**

Saliento que essa pesquisa de doutorado, assim como minha dissertação foram financiadas pela CAPES, que me concedeu a bolsa PROEX, viabilizando a realização de um sonho pessoal para minha formação científica e, conseqüentemente, atuação profissional atual como professora de ensino superior no Brasil. Reforço que essa pesquisa foi desenvolvida durante a pandemia de Covid-19.

*Aqui, na comunidade, podemos relaxar – estamos seguros, não há perigos ocultos em cantos escuros (com certeza, dificilmente um “canto” aqui é “escuro”)*  
(BAUMAN, 2003, p. 7).

## RESUMO

Nossa tese tem como objetivo compreender como são construídos sentidos durante de *tecnosegurança* pela ambiência Facebook. No intento de complementar a construção do problema de pesquisa, se determinam como objetivos específicos articular discussões relacionadas à privacidade e segurança na cultura digital à perspectiva das audiovisualidades da tecnocultura; formular o conceito de “*tecnosegurança*” enquanto sintoma da *tecnocultura* contemporânea, que se espalha através e para além das mídias, produzindo ambiência; e, por fim, autenticar sentidos de segurança e de privacidade enunciados pelas interfaces do Facebook. Nossa abordagem utiliza um itinerário metodológico que trata de um contágio de iniciativas, como intuição, cartografia e metodologia das molduras e, como desdobramento, tivemos como inspiração o movimento do *flâneur*, dando a ver sete coleções criadas a partir de afinidades eletivas que emergem de nossa observação, indicando que o objeto assume duas ordens: a da materialidade, referente ao percurso pela plataforma e interfaces paralelas, e da ordem das virtualidades, ou as *ethicidades* e imaginários que emergem dos emolduramentos agenciados. Autenticamos algumas *ethicidades* que se atualizam em molduras e moldurações de significação associadas aos imaginários que comunicam sentidos de vigilância, segurança, infância, cuidado, medo, proteção, confiança, judicialização e anonimato. Conforme demonstra nossa investigação, a fotografia da galáxia da *tecnosegurança* pela ambiência FB é formada por três constelações: Confiança Programada, Usuário Vulnerável e Ambiência da *Tecnosegurança* Contemporânea. Entendemos, como parte da contribuição dessa pesquisa, a identificação da construção de um perfil multifacetado do usuário que percorre essa ambiência conforme a *ethicidade* circunstanciada pela interface. Compreendemos que o FB é um complexo objeto de molduras, *ethicidades* e moldurações que carregam sentidos, dando a ver imaginários do próprio FB, não apenas restritos a ele, mas como sintoma da cultura digital contemporânea, a qual o próprio FB integra e retroalimenta para permanecer operando, alicerçado em sentidos identitários próprios da *tecnosegurança*. São nesses construtos que se atualizam em virtualidades, que compõem uma complexa arquitetura, que o FB reconvoca constantemente memórias, a partir das imagens de interface, criteriosamente desenvolvidas para construir confiança por meio de uma promessa dicotômica entre liberdade e controle.

**Palavras-chave:** *tecnosegurança*; interface; Facebook; segurança; *tecnocultura*; imagem.

## ABSTRACT

This thesis aims to understand how meanings are constructed during *technosecurity* by the Facebook environment. In an attempt to complement the construction of the research problem, specific objectives are determined to articulate discussions related to privacy and security in digital culture from the perspective of technoculture audiovisualities; to formulate the concept of “*technosecurity*” as a symptom of contemporary technoculture, which spreads through and beyond the media, producing an ambience; and finally, to authenticate meanings of security and privacy enunciated by Facebook's interfaces. Our approach uses a methodological itinerary that deals with a contagion of initiatives, with the unfolding of cartography we were inspired by the movement of the *flâneur*, showing seven collections created from elective affinities that emerge from our observation, indicating that the object assumes two orders: that of materiality, referring to the path through the platform and parallel interfaces, and the order of virtualities, or the *ethicities* and imaginaries that emerge from the framed agencies. We authenticate some *ethicities* that are updated in frames and frames of meaning associated with imaginaries that communicate meanings of surveillance, security, childhood, care, fear, protection, trust, judicialization and anonymity. As our investigation demonstrates, the photograph of the *technosecurity* galaxy by the FB environment is formed by three constellations: Programmed Trust, Vulnerable User and Contemporary *Technosecurity* Ambience. We understand as part of the research contribution an identification of the construction of a multifaceted profile of the user that runs through this environment according to the ethics circumstantiated by the interface. We understand that FB would be a complex object of frames, *ethicities* and framings that carry meanings, revealing imaginaries of FB itself, but not just restricted to it, but as a symptom of contemporary digital culture, in which it is a constituent part and feeds back to remain operating based on the identity senses typical of *technosecurity*. It is in these constructs that they are updated in virtualities that make up a complex architecture, constantly recalling memories from the interface images carefully developed to build trust through a dichotomous promise between freedom and control.

**Key-words:** *technosecurity*; interface; Facebook; security; *technoculture*; image.

## LISTA DE FIGURAS

Figura 1 - Captura de tela Facebook Polices (ago. 2020).....	21
Figura 2 - Captura de excerto de tela do Facebook para privacidade da conta (out. 2020) .....	22
Figura 3 - Segurança de acesso à conta no Facebook (out. 2020).....	23
Figura 4 - Revisão da configuração de privacidade no Twitter (abr. 2020).....	24
Figura 5 - Central de privacidade do Twitter (jun. 2022).....	24
Figura 6 - Captura de tela do Estadão - uso de <i>cookies</i> .....	25
Figura 7 - Captura de tela do Google Meet - segurança nas reuniões por videochamada.....	25
Figura 8 - Captura de tela ( <i>notebook</i> pessoal) - mensagem de proteção do antivírus McAfee	26
Figura 9 - Captura de tela ( <i>notebook</i> pessoal) - mensagem do antivírus McAfee informando uma possível ameaça .....	27
Figura 10 - Captura de tela ( <i>notebook</i> pessoal) com mensagem do antivírus .....	27
Figura 11 - Excerto de tela da apresentação do novo <i>design</i> de interface do FB .....	30
Figura 12 - Captura de tela da seção Conta, no Google, e a preocupação com segurança e proteção .....	32
Figura 13 - Arranjo de capturas de telas com manifestações sobre proteção da conta no Google e do recurso Captcha.....	33
Figura 14 - Charge do cartunista Peter Steiner.....	37
Figura 15 - Postagem no Instagram do Data Privacy Brasil.....	38
Figura 16 - <i>Black Mirror</i> - Netflix 2016 .....	39
Figura 17 - Arranjo de imagens capturadas nas câmeras de vigilância pessoal .....	43
Figura 18 - Arranjo de capturas de telas provenientes de sistemas de reconhecimento facial.	44
Figura 19 - Excerto do YouTube com o comercial Itaú - Privacidade - Informação .....	45
Figura 20 - Captura de tela do último <i>frame</i> do comercial Itaú - Privacidade - Informação ...	45
Figura 21 - Excerto da tela da página da campanha institucional banco Itaú - Privacidade ....	46
Figura 22 - Captura de tela do comercial do WhatsApp com o tema privacidade .....	47
Figura 23 - Captura de tela do segundo filme publicitário do WhatsApp da campanha “Criptografia de ponta a ponta” .....	48
Figura 24 - Captura de tela da campanha publicitária do WhatsApp (out. 2021) .....	49
Figura 25 - Captura de tela da segunda peça da mesma campanha publicitária do WhatsApp (dez. 2021).....	49
Figura 26 - Excerto de tela do Gmail sobre verificação de segurança da conta.....	51
Figura 27 - Meme circulando no FB sobre proteção de <i>login</i> no Gmail .....	52



Figura 28 - Contágio do itinerário metodológico .....	104
Figura 29 - Exemplo do exercício de recolher interfaces para análise do <i>player</i> de vídeos do FB - LAR (maio 2019) .....	105
Figura 30 - Tentativa de inventariar as capturas de telas e compreender a arquitetura da interface (jul. 2019) .....	106
Figura 31 - Captura de tela da primeira versão do <i>site</i> The Facebook (publicada em 12 fev. 2004).....	108
Figura 32 - Captura de tela da página inicial do The Facebook aberto para as demais comunidades acadêmicas (16 jul. 2004).....	109
Figura 33 - Excerto de tela da página inicial do FB quando restrito ao uso da comunidade escolar (19 abr. 2006).....	110
Figura 34 - Excertos de capturas de telas da <i>newsfeed</i> para versão <i>desktop</i> (jul. 2021/set. 2020).....	111
Figura 35 - Excerto de tela - <i>newsfeed</i> - personalização a partir do usuário .....	113
Figura 36 - Excerto de tela - <i>timeline</i> do usuário .....	114
Figura 37 - Barra de busca do FB e suas categorias de indexação de resultados.....	115
Figura 38 - Página dentro do The Facebook dedicada a conteúdo publicitário - <i>Announcements</i> (ago. 2005).....	116
Figura 39 - Detalhamento da operação publicitária dentro do Facebook - sob nova nomenclatura (nov. 2005).....	117
Figura 40 - Evolução da opção <i>Announcements</i> para Facebook Flyers (fev. 2007) .....	118
Figura 41 - Excerto de tela sinalizando na <i>newsfeed</i> os produtos destinados aos usuários do FB .....	120
Figura 42 - Galáxia das constelações .....	128
Figura 43 - Montagem comparação de <i>layout</i> para a presença da <i>ethicidade</i> infância na página de <i>login</i> da primeira versão da plataforma The Facebook em 2004 <i>versus</i> versão 2022 .....	130
Figura 44 - Armazenamento das interfaces no Google Drive .....	131
Figura 45 - Armazenamento das interfaces no Microsoft Power Point.....	132
Figura 46 - Coleção Infância .....	134
Figura 47 - Código QR para acessar imagens das interfaces que compõem a coleção Infância.....	135
Figura 48 - Indicação da dissecação da interface <i>newsfeed</i> - coleção Infância.....	136
Figura 49 - Dissecação da coleção Infância - <i>newsfeed</i> .....	137
Figura 50 - Dissecação da coleção Infância - <i>timeline</i> .....	138

Figura 51 - Indicação da seção Privacidade na <i>newsfeed</i> do FB (abr. 2021) .....	140
Figura 52 - Captura da seção Privacidade dentro do FB .....	141
Figura 53 - Termos e Políticas do Facebook .....	142
Figura 54 - Dissecção da coleção Infância - Termos e Políticas do Facebook.....	143
Figura 55 - Dissecção da <i>ethicidade</i> infância - Central de Segurança no Facebook .....	146
Figura 56 - Indicação da coleção Infância na reprodução da interface gráfica, versão aplicativo do FB .....	147
Figura 57 - Fotografia do <i>datacenter</i> do FB na Carolina do Norte .....	148
Figura 58 - Arranjo de interfaces da coleção Guardião de Memórias.....	149
Figura 59 - Código QR para acessar imagens das interfaces que compõem a coleção Guardião de Memórias .....	150
Figura 60 - Dissecção da <i>ethicidade</i> - Guardião de Memórias.....	150
Figura 61 - Dissecção da coleção Guardião de Memórias.....	153
Figura 62 - Dissecção da coleção Guardião de Memórias - <i>newsfeed</i> .....	154
Figura 63 - Dissecção da coleção Guardião de Memórias.....	155
Figura 64 - Dissecção da coleção Guardião de Memórias.....	156
Figura 65 - Coleção Sujeito Inseguro e Lógica Suspeita.....	159
Figura 66 - Código QR para acessar a coleção Usuário Inseguro e Lógica Suspeita.....	159
Figura 67 - Dissecção da coleção Sujeito Inseguro e Lógica Suspeita.....	160
Figura 68 - Dissecção da coleção Sujeito Inseguro e Lógica Suspeita.....	162
Figura 69 - Dissecção da coleção Sujeito Inseguro e Lógica Suspeita.....	165
Figura 70 - Dissecção da coleção Sujeito Inseguro e Lógica Suspeita.....	166
Figura 71 - Coleção <i>Tecnoinsegurança</i> .....	169
Figura 72 - Código QR para visualização da coleção <i>Tecnoinsegurança</i> .....	169
Figura 73 - Dissecção da coleção <i>Tecnoinsegurança</i> .....	170
Figura 74 - Dissecção da coleção <i>Tecnoinsegurança</i> .....	172
Figura 75 - Dissecção da coleção <i>Tecnoinsegurança</i> .....	174
Figura 76 - Arranjo de interfaces da coleção Políticas de Pergaminho.....	176
Figura 77 - Código QR para visualização da coleção Políticas de Pergaminho .....	177
Figura 78 - Coleção Território do FB - excerto de tela da seção Privacidade de 2004 no The Facebook.....	178
Figura 79 - Captura de tela da sinalização de mudança de nome da empresa Facebook Inc. para Meta (1 nov. 2021) .....	180
Figura 80 - Dissecção da coleção Políticas de Pergaminho.....	181

Figura 81 - Dissecação da coleção Políticas de Pergaminho.....	183
Figura 82 - Dissecação da coleção Políticas de Pergaminho para compararmos leitura aproximada e captura da página completa.....	184
Figura 83 - Captura das 3 imagens que compõem a seção completa das Políticas de Privacidade do FB .....	185
Figura 84 - Excerto de tela da seção Políticas de Privacidade, na versão anterior à atualização da Meta (jul. 2022) .....	186
Figura 85 - Dissecação da coleção Políticas de Pergaminho em áreas dispersas ao FB .....	187
Figura 86 - Arranjo das interfaces que compõem a coleção Medo e Vigilância.....	189
Figura 87 - Código QR para visualização da coleção Medo e Vigilância.....	190
Figura 88 - Dissecação da coleção Ambiência da Tecnosegurança Contemporânea.....	191
Figura 89 - Dissecação da coleção Medo e Vigilância.....	193
Figura 90 - Coleção Medo e Vigilância.....	194
Figura 91 - Dissecação da coleção Medo e Vigilância.....	196
Figura 92 - Coleção Serviços Autenticadores .....	197
Figura 93 - Código QR para visualização da Coleção Serviços Autenticadores.....	197
Figura 94 - Dissecação dos Serviços Autenticadores .....	198
Figura 95 - Tentativa de mapear a seção Privacidade da conta do Google .....	200
Figura 96 - Dissecação coleção Serviços Autenticadores dos jornais <i>ZH</i> e <i>Folha de São Paulo</i> e do Miro .....	201
Figura 97 - Dissecação da coleção Serviços Autenticadores com biometria, reconhecimento facial e <i>login</i> social .....	202
Figura 98 - Dissecação da coleção Serviços Autenticadores do filme <i>Outter and inner space</i> e da campanha publicitária da Samsung.....	204
Figura 99 - Perfis do usuário multifacetado percebidos no mapeamento das constelações ...	206

## LISTA DE SIGLAS

CPF	Cadastro de Pessoa Física
CAPTCHA	<i>Completely Automated Public Turing test to tell Computers and Humans Apart</i>
CIA	<i>Central Intelligence Agency</i>
CIBERIDEA	Núcleo de Pesquisa em Tecnologias da Comunicação, Cultura e Subjetividade
CNPQ	Conselho Nacional de Desenvolvimento Tecnológico
DPB	Data Privacy Brasil
FB	Facebook
FGTS	Fundo de Garantia por Tempo de Serviço
GDPR	<i>Global Data Protection Regulation</i>
GUIs	<i>Graphical User Interfaces</i> (Interface Gráfica do Usuário)
HCI	Interface Humano Computador
IA	Inteligência Artificial
INTERCOM	Sociedade Brasileira de Estudos Interdisciplinares da Comunicação
IoT	<i>Internet of Things</i>
LabMem	Laboratório de Memória das/nas Mídias Online
LAR	Laboratório do Audiovisual em Rede
LGPD	Lei Geral de Proteção de Dados
MIT	Massachusetts Institute of Technology
NSA	<i>National Security Agency</i>
NYU	Universidade de Nova Iorque
OOH	<i>Out-Of-Home</i>
PET	Tecnologias de Aumento da Privacidade
Rede Lavits	Rede Latino-Americana de Estudo sobre Vigilância, Tecnologia e Sociedade
RFID	<i>Radio Frequency Identification</i>
SRS	Sites de Redes Sociais
TAR	Teoria Ator-Rede
TCAv	Audiovisualidades, <i>Tecnocultura</i> , Comunicação, Memória e Design
UCI	University of California Irvine
UPI	<i>User Profile Information</i>

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>16</b>
<b>1.1 Problema e objetivos de pesquisa.....</b>	<b>28</b>
<b>1.2 Sentidos de <i>tecnosegurança</i> nas mídias.....</b>	<b>36</b>
<b>1.3 Estado da arte .....</b>	<b>53</b>
<b>2 (TECNO)SEGURANÇA CONTEMPORÂNEA .....</b>	<b>66</b>
<b>2.1 Construtos tecnoculturais de segurança e privacidade.....</b>	<b>66</b>
<b>2.2 <i>Tecnosegurança</i> .....</b>	<b>76</b>
<b>3 METODOLOGIA.....</b>	<b>92</b>
<b>3.1 Itinerário metodológico .....</b>	<b>92</b>
<b>3.2 Recolhendo e situando o <i>corpus</i> pela <i>tecnosegurança</i> .....</b>	<b>105</b>
<b>4 CONSTELAÇÕES .....</b>	<b>127</b>
<b>4.1 <i>Flâneur</i> e colecionadora .....</b>	<b>129</b>
<b>4.2 Primeira constelação - Confiança Programada.....</b>	<b>133</b>
4.2.1 Coleção Infância .....	133
4.2.2 Coleção Guardião de Memórias .....	147
<b>4.3 Segunda constelação - Usuário Vulnerável .....</b>	<b>157</b>
4.3.1 Coleção Sujeito Inseguro e Lógica Suspeita .....	158
4.3.2 Coleção <i>Tecnoinsegurança</i> .....	168
4.3.3 Coleção Políticas de Pergaminho .....	176
<b>4.4 Terceira constelação - <i>Ambiência da Tecnosegurança Contemporânea</i> .....</b>	<b>188</b>
4.4.1 Coleção Medo e Vigilância .....	189
4.4.2 Coleção Serviços Autenticadores .....	196
<b>5 CONSIDERAÇÕES FINAIS.....</b>	<b>208</b>
<b>REFERÊNCIAS .....</b>	<b>214</b>

## 1 INTRODUÇÃO

“Sorria, você está sendo filmado” se tornou uma sinalização tão comum na atualidade, que parece passar despercebida – talvez porque já estamos acostumados a estar diante de tantas situações cuja captação de nossa imagem é utilizada pela justificativa do monitoramento e vigilância, pregando um controle para maior segurança. Mas, o que significa estar seguro? Estar protegido e longe de perigo, na *tecnocultura* que vivemos hoje, pode ser inferido como ter o direito do controle sobre a própria privacidade, da liberdade e de confiar que alguém ou algo está zelando pela nossa proteção?

Com o intuito de situar o(a) leitor(a) nessa tese, e nas discussões que irei levantar ao longo da introdução, já adianto, logo neste segundo parágrafo, que essa pesquisa busca investigar os sentidos durante de *tecnosegurança* pela ambiência Facebook, produzidos hoje, na *tecnocultura* contemporânea. O trabalho se situa numa série de articulações que circundam aspectos como segurança, privacidade e proteção, que se dispersam na cultura digital, nas mídias e pelas mídias, caracterizando uma ambiência própria, definida pela *tecnosegurança*.

Contudo, para desenvolver o tensionamento e o nível de reflexão que demanda uma tese, posso dizer que este foi o momento que mais me senti insegura ao longo dos 37 anos de vida. Mas, arrisco a dizer que essa mesma sensação que me acompanha ao longo da pesquisa, que teve início em 2018, ao ingressar no doutorado, também se faz presente na grande maioria da população em tempos tão difíceis, na busca pela segurança. Acredito, inclusive, que a pesquisa é uma manifestação metafórica de algo que provoca, questiona e promove um desconforto na autora durante todo o seu processo. Portanto, sentir-se seguro, conforme traz o dicionário brasileiro, significa estar “livre de perigo ou de risco. Que não hesita; firme. Certo, convicto. Constante, leal. Indubitável, certo. Preso, fixo. Avarento. Contrato pelo qual uma das partes se obriga a indenizar outra dum perigo, ou prejuízo eventual” (FERREIRA, 1993, p. 498). Portanto, absolutamente não me sinto segura em ter desenvolvido essa tese em tempos tão incertos, mas justamente a busca por “estar fora de perigo” talvez seja o que me moveu ao longo do doutoramento, questionar, buscar e refletir sobre a segurança, hoje, é o grande catalizador de meu processo acadêmico e profissional.

Mas, chegar nesse tema da segurança foi um processo que refletiu numa série de contágios, como, por exemplo, meu interesse pessoal sobre o assunto e manifestações que vieram à tona nos últimos anos auxiliaram a chegar na problematização. Como o próprio título da pesquisa já dá pistas do tema que me cerca, ou o que “nos olha”, nas palavras de Didi-Huberman (1998), no objeto escolhido, a *tecnosegurança* contemporânea, me apropri

da fala do professor, Dr. Gustavo Daudt Fischer (Unisinos), em uma orientação, ainda durante o mestrado, que verbalizou: “pesquisa é processo”; desta forma, entendo que todas as etapas no desenvolvimento do doutoramento são importantes a partir da proposta de encará-las como aprendizado, desvio e (re)construção.

Assim, o objeto foi se mostrando, aos poucos, durante todo o curso do doutorado, e ficando cada vez mais evidente com base nas diversas manifestações que me cercavam, desde questões pessoais, sociais e culturais. Me apoio nas palavras de André Lemos (2009, p. 622), no artigo publicado há 13 anos, ao afirmar que entramos na era da mobilidade informacional, quando era possível “[...] aliar, pela primeira vez, localização, vigilância, e mobilidades física e informacional (capacidade de consumir, produzir e distribuir informação)”. Nesse sentido, como usuária das redes sociais, professora e pesquisadora em Comunicação, meu olhar para determinadas interfaces sempre foi pelo viés da *tecnocultura* e das audiovisualidades, buscando perceber a memória das e nas imagens, quais sentidos e imaginários eram atualizados nas materialidades que manuseava a partir dos meus notebook e *smartphone*. E, com a aceleração do uso de dispositivos e *softwares*, devido ao isolamento social, causado pela pandemia de COVID-19<sup>1</sup>, estar na *web* ou fazer uso de aplicativos em celular se tornou algo não só comum como necessário para as demandas de trabalho que aceleravam durante a realização de atividades remotamente e que marcaram o ano de 2020.

Um dos ambientes que justamente me fez exercitar esse tipo de “visão”, com base nas audiovisualidades, foi o Facebook; e minha relação com a plataforma teve início concomitantemente ao ingresso, em 2014, no mestrado em Ciências da Comunicação do Programa de Pós-Graduação (PPGCC), da Universidade do Vale do Rio dos Sinos (UNISINOS), já fazendo parte da mesma linha de pesquisa que integro hoje, *Mídias e Processos Audiovisuais*. À época, minha visão sobre história e memória eram baseadas naquelas versões tidas como evolucionistas, a partir da perspectiva linear e cronológica do tempo e das coisas. E, minha pretensão, ao entrar no mestrado, era compreender um pouco mais sobre a história da publicidade audiovisual brasileira, refletir sobre a sociedade e a cultura consumidora de produtos e serviços anunciados na mídia televisiva “de antigamente”<sup>2</sup>.

---

<sup>1</sup> Diante da propagação da COVID-19, doença causada pelo novo coronavírus, a Organização Mundial da Saúde (OMS) decretou pandemia mundial no dia 11/03/20. Segundo a OMS, uma pandemia é a disseminação mundial de uma nova doença. Com início na China, o coronavírus se espalhou rapidamente por todos os continentes, contaminando milhares pessoas e levando diversos governantes a tomarem medidas drásticas para a contenção da doença. A dinâmica da transmissão de doenças infecciosas e, em particular, da COVID-19, deve ser compreendida para que os governos e cidadãos possam tomar as melhores decisões (BVS, 2020).

<sup>2</sup> Uso as aspas para referenciar esses termos relacionados à cronologia do tempo pois configuram-se como visões diferentes da perspectiva de tempo que adoto tanto na dissertação quanto nesta tese (ao longo do texto essa escolha ficará mais clara ao leitor).

Mas nem sempre foi assim, pois acredito que o ambiente molda o pesquisador e vice-versa, e, na minha dissertação, que materializa parte das reflexões e atualizações da pesquisadora em construção, desenvolvi, sob orientação do Prof. Dr. Gustavo Daudt Fischer, um trabalho que tangibiliza uma série de mudanças na minha maneira de encarar a história e, conseqüentemente, a relação entre passado, presente e memória. Essa perspectiva que está centrada na maneira de pensar o tempo, foi crucial para compreender os objetos de pesquisa em Comunicação, e, principalmente, as imagens como parte central dessa construção cultural, ou melhor, *tecnocultural*. Esse olhar só foi possível ser realizado porque, desde o ingresso ao mestrado, participo como membro do Grupo de Pesquisa Audiovisualidades da *Tecnocultura*, Comunicação, Memória e Design (TCAv)<sup>3</sup>, vinculado ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ), espaço de intensa provocação reflexiva e metodológica para tensionar objetos comunicacionais dentro da linha de pesquisa *Mídias e Processos Audiovisuais*.

Além do envolvimento com o TCAv, concomitantemente às disciplinas cursadas ao longo dos dois anos de mestrado e demais atividades acadêmicas da formação, fui sendo “contagiada” pela lente das audiovisualidades da *tecnocultura*, e iniciei um movimento de tentar compreender diversas manifestações de catalogação e arquivamento de materiais publicitários “antigos” na *web*.

Ao olhar para o conteúdo audiovisual publicitário frente à característica de memorialização da publicidade, fomos contagiados pelo debate que tensiona as audiovisualidades e a *tecnocultura*. Deixamos de encarar a memória como a fonte “redentora do passado”, e passamos a pensar a história através dos anacronismos, posicionando a imagem como central no pensamento sobre o tempo, o que caracteriza as imagens como portadoras de memória (KRAUSE, 2016, p. 12).

A minha dissertação, sob o título *Zelando o ouro produzido no passado: escavando construtos de memória da publicidade audiovisual a partir do site Propagandas Históricas* (KRAUSE, 2016)<sup>4</sup>, buscou verificar como os construtos de memória da publicidade audiovisual se atualizam a partir do *site* Propagandas Históricas, onde busquei, em suas zonas adjacentes, dissecar as interfaces e escavar as camadas (ou tempos) que coalescem no objeto, criando constelações que foram mapeadas com base em um agir arqueológico<sup>5</sup>. Esse

---

<sup>3</sup> Meu desenvolvimento como pesquisadora, e, atualmente, como professora, está extremamente alicerçado no caráter reflexivo e laboratorial que o TCAv proporciona. Minha passagem pelo grupo de pesquisa iniciou de maneira bastante tímida, mas, aos poucos, a partir das provocações realizadas em nossos encontros, desde 2014, fui buscando um lugar mais ativo entre os alunos integrantes, passando pela coordenação discente, algumas vezes, grupo de mídias e pela coordenação da publicação da *newsletter* mensal do TCAv.

<sup>4</sup> O trabalho pode ser consultado no endereço <http://www.repositorio.jesuita.org.br/handle/UNISINOS/5184>.

<sup>5</sup> A proposta de Fischer (2012a) será aprofundada ao longo do texto.



movimento tem como forte pano de fundo a proposta da arqueologia da mídia, vertente relativamente recente que provoca refletir sobre as descontinuidades e rupturas das mídias como alternativas igualmente relevantes para a cultura<sup>6</sup>.

Mas, ao encerrar o ciclo do mestrado em 2016, recebi da banca examinadora como sugestão para futuros encaminhamentos da pesquisa, uma possível apropriação para submissão de projeto de tese, para seleção de doutoramento, indicando explorar outras possibilidades audiovisuais na *web* a partir de sua interface. Ou seja, desenvolvi uma proposta com o objetivo de avançar na perspectiva das audiovisualidades para formatos que ultrapassavam a minha preocupação com os construtos de memória da publicidade audiovisual, ao investigar as diversas camadas de temporalidades das imagens, através de sua atualização na *web*, ou mais precisamente, do *player* de vídeos do FB, encarando as imagens como um audiovisual de interface inspirado em Montañó (2015). Ao dar continuidade nas inquietações sobre o ambiente da *web*, e em uma das zonas adjacentes cartografadas na dissertação, a rede social Facebook (FB), começou a ter um protagonismo no meu interesse na pesquisa.

Nesse sentido, a proposta de avançar sobre o objeto empírico FB me fez pensar sobre o que, de fato, me inquietava tanto sobre aquela coleção de interfaces capturadas, exercício que tive o hábito de fazer desde quando ingressei no PPGCC. Entre diversas idas e vindas, comecei a refletir sobre algo positivo que me provocava ao olhar (e me deixar ser olhada) pelas imagens coletadas, uma espécie de sentimento positivo, alegre e feliz que me envolvia toda vez que revolia as imagens da coleção capturada. Algo me remetia a uma espécie de escapismo do “mundo real” e pandêmico, de fora das interfaces, e me mantinha segura ali dentro dessa comunidade criada entre amigos (que já não encontrava desde o início do isolamento social) e conteúdos festivos e coloridos. Paralelo ao exercício de revisão da coleção, o FB realizou uma atualização no seu *design*, enquanto eu flanava por sua interface, estimulando a reflexão sobre certos sentidos de segurança que, provavelmente, estavam sendo construídos ali dentro, mas, relacionados ao uso de informação ou dados coletados justificados pela personalização da minha experiência na conta e da privacidade concedida às informações cadastradas.

Dessa forma, ainda incerta sobre o tema a ser abordado na pesquisa, mas indo em direção a aspectos como privacidade de conta no FB e segurança das informações, realizei o

---

<sup>6</sup> Essa maneira de encarar os objetos comunicacionais me acompanha desde então, e, ao longo de toda a tese, a arqueologia da mídia e sua visão de tempo estarão presentes na maneira como tensiono o objeto, fundamentado na visão de autores como Michel Foucault (1969), Marshall McLuhan (1964), Gustavo Daudt Fischer (2012a), Friedrich Kittler (2019) e Erkki Huhtamo (2011).

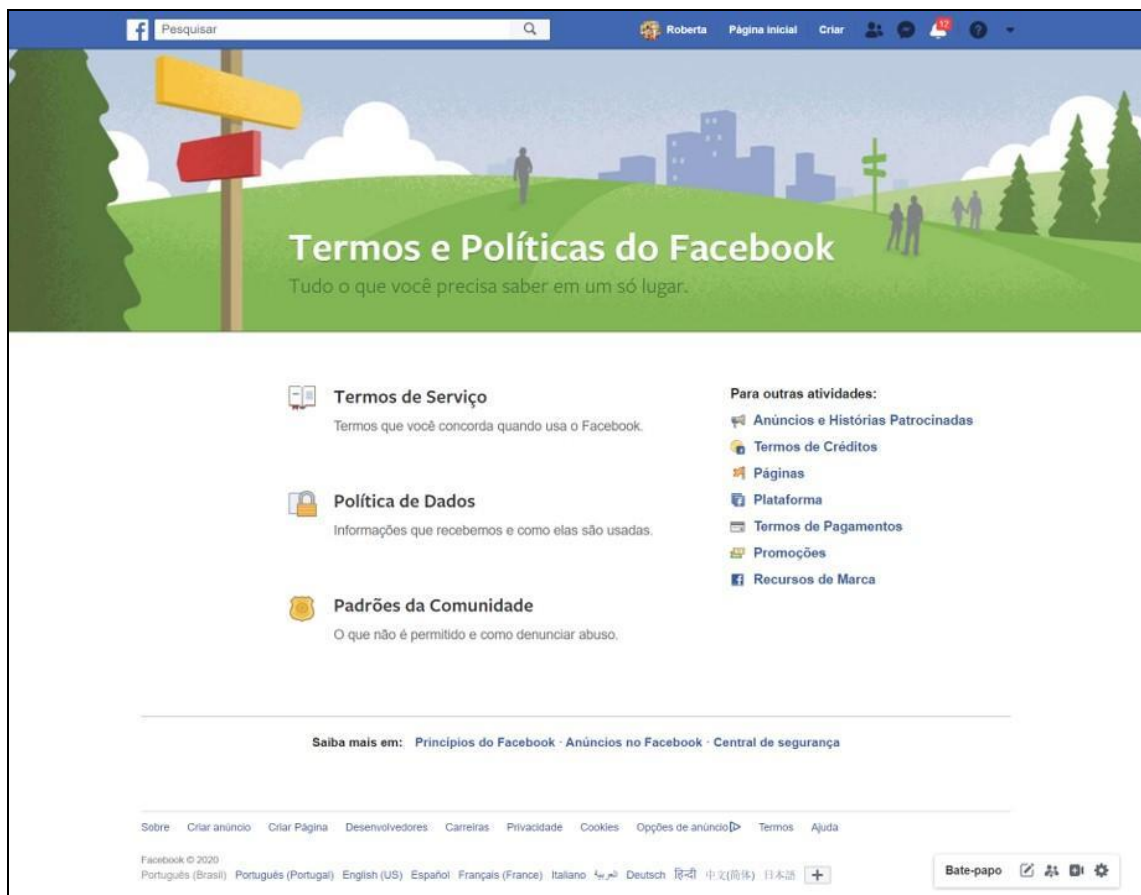
exercício em busca do estado da arte do objeto, e encontrei pesquisas associando segurança e FB, a partir da perspectiva da vigilância, da privacidade e do uso de dados. Paralelamente, foi chamando minha atenção diversas manifestações que orbitam o tema da segurança na *tecno cultura*, como privacidade, controle de informações, uso de dados, verificação de senhas, câmeras de vigilância e monitoramento.

Ao encontro dessas temáticas, que foram emergindo, percebi que alguns desses aspectos já haviam sido pautados em escândalos largamente debatidos nas mídias mundiais, como o caso do analista Edward Snowden, que, conforme matéria publicada no jornal *The Guardian* (2013), declarou, em 2013, haver um sistema de vigilância e monitoramento sem precedentes não somente de cidadãos norte-americanos, mas de líderes mundiais através da National Security Agency (NSA), órgão da Central Intelligence Agency (CIA), que culminou em um dos maiores vazamentos de informação sigilosa da história dos Estados Unidos, utilizando empresas como o FB. Antecedendo a Snowden, outro grande escândalo de vazamento de informações foi promovido em 2010, pelo ativista Julian Paul Hawking, mais conhecido como Julian Assange, fundador do *site* Wikileaks (2006), quando seu *site* publicou documentos sigilosos do governo norte-americano revelando dados sobre os combates ao Iraque e Afeganistão pelos Estados Unidos. E, ainda, o caso relatado por uma diretora da empresa de gestão de dados, Cambridge Analytica, Brittany Kaiser, afirmando o mau uso de informações coletadas de usuários da rede social FB que foram utilizadas para moldar perfis de eleitores, com a intenção de favorecer o resultado das eleições norte-americanas, que elegeram Donald Trump como presidente, em 2016, e o impacto sobre o referendo do Brexit no mesmo ano. Esse acontecimento ficou conhecido como o maior escândalo envolvendo o FB, exigindo que seu fundador, Mark Zuckerberg, fosse interrogado pelo senado americano no ano de 2018, dando explicações sobre como sua empresa permitiu “vazar” informações de aproximadamente 87 milhões de usuários sem sua autorização prévia, auxiliando a moldar e forjar conteúdos com intenção política, econômica e religiosa.

Concomitantemente, passei a refletir sobre como o tema da segurança vem ganhando centralidade atualmente, em que se pode verificar, a partir de um processo de audiovisualização da cultura, com o uso de câmeras para controle de circulação, vigilância urbana, governamental, reconhecimento facial e tantas outras iniciativas, inclusive midiáticas, manifestadas por meio de campanhas publicitárias, produções de entretenimento audiovisuais e dispositivos tecnológicos. Aliado ao tema da segurança na *tecno cultura* atual, outros aspectos acompanham essa preocupação criando um eixo relacionando diretamente à pauta de privacidade, confiança, vigilância, monitoramento e anonimato.

Foi possível perceber essas relações a partir de um exercício que realizei, solicitado pela orientadora Dra. Sônia Montañó (2015), inspirado na figura do trapeiro, como sujeito que coleta vestígios ao longo do caminho, e passei a colecionar centenas de capturas de telas no meu dispositivo móvel e, também, no meu *notebook*, juntando uma espécie de “sucata”, ou manifestações associadas à segurança e privacidade de usuários e seus dados e que não pareciam ter a pretensão de ser centrais à atenção na interface do FB, onde fui intencionalmente buscar como a rede social diz que utiliza os meus dados e os armazena, e, possivelmente, onde poderia visualizar o que já foi coletado a meu respeito, conforme as imagens, a seguir, demonstram:

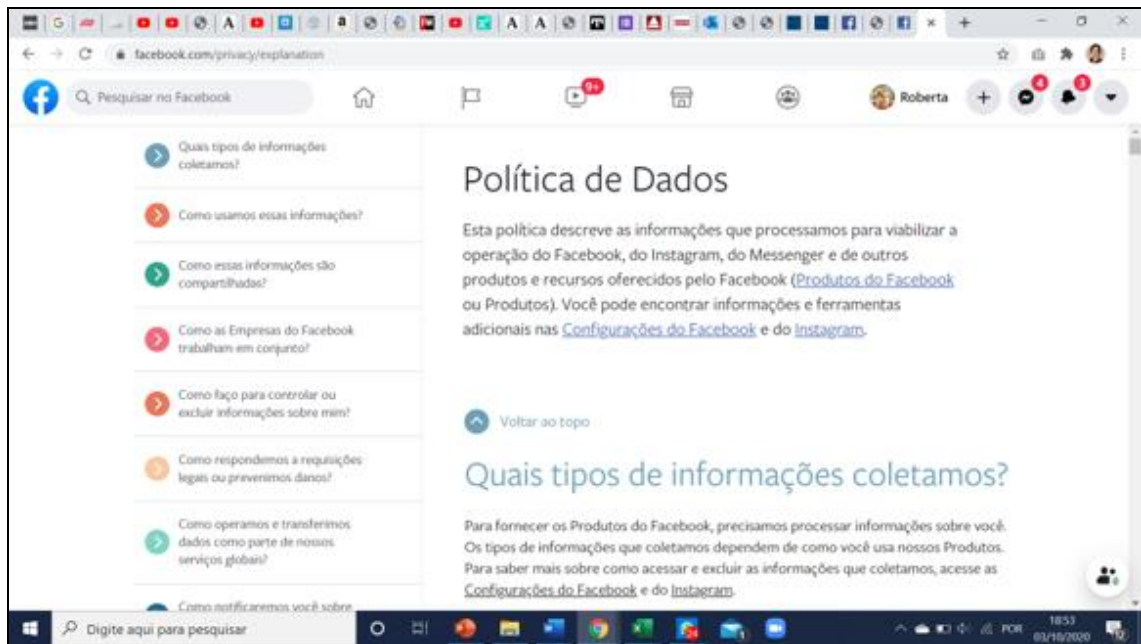
Figura 1 - Captura de tela Facebook Policies (ago. 2020)



Fonte: Facebook (2020).<sup>7</sup>

<sup>7</sup> Maiores informações em <https://www.facebook.com/policies>.

Figura 2 - Captura de excerto de tela do Facebook para privacidade da conta (out. 2020)

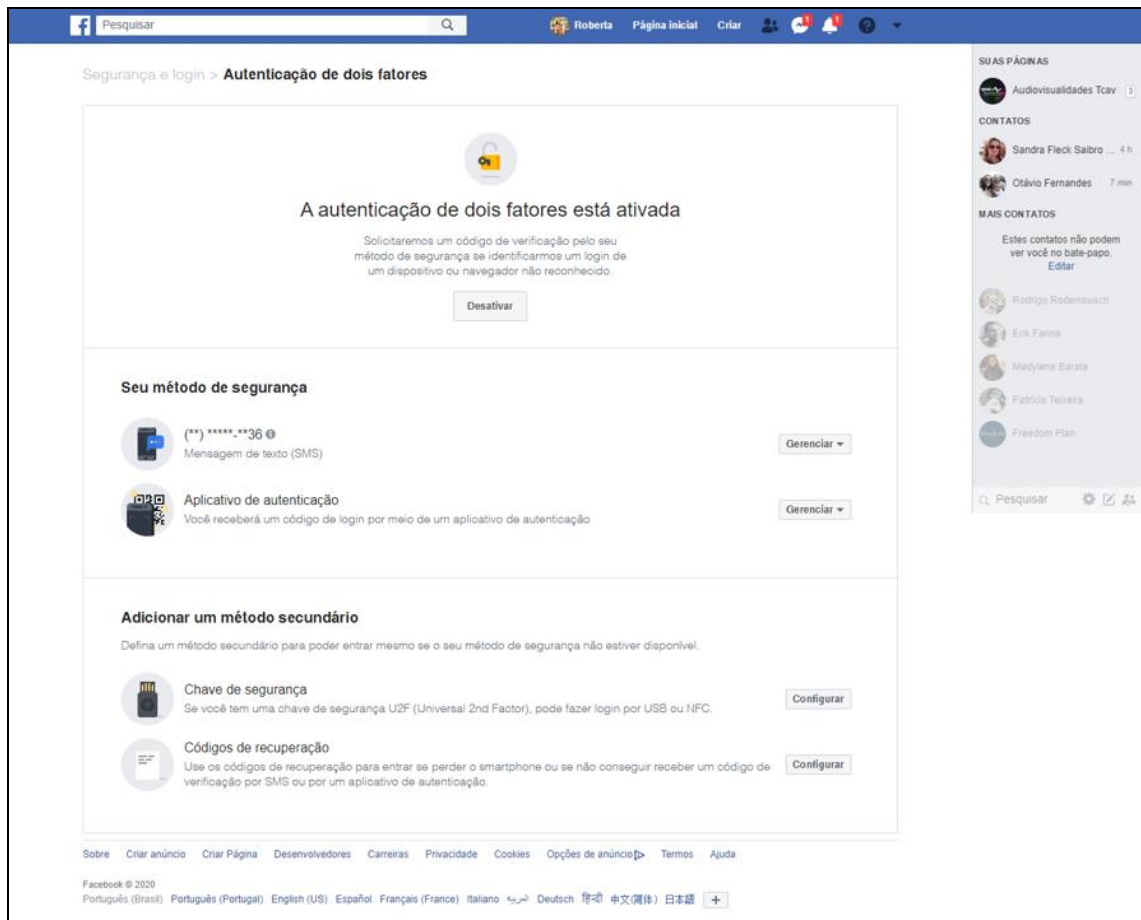


Fonte: Facebook (2020).<sup>8</sup>

Outros aspectos associados à segurança da conta estavam agrupados em políticas de acesso, senha e proteção para entrar na conta pessoal cadastrada no FB. Há a possibilidade de utilizar a verificação por dois fatores, cadastrando outro *e-mail*, dispositivo ou código SMS ou, ainda, código QR para confirmar se é o mesmo usuário que está acessando determinado *login*, conforme mostra captura a seguir:

<sup>8</sup> Maiores informações em <https://www.facebook.com/policies/cookies>.

Figura 3 - Segurança de acesso à conta no Facebook (out. 2020)

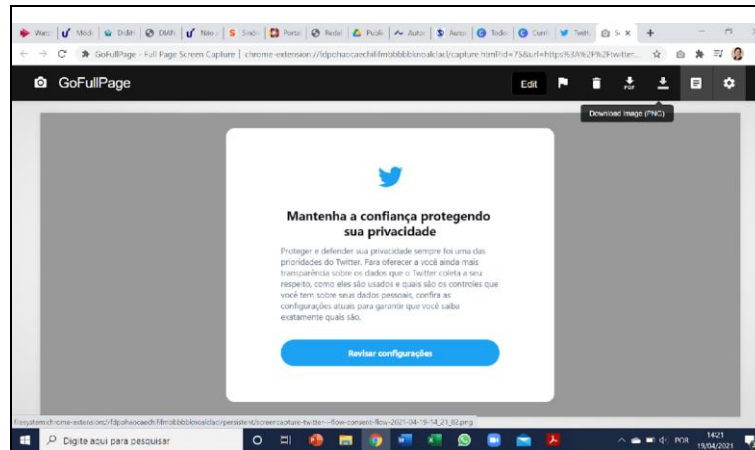


Fonte: Facebook (2020).<sup>9</sup>

Paralelamente ao movimento de coleta das interfaces do FB, fui guardando outras manifestações em diversos outros ambientes, na *web*, que demonstraram preocupação com uma espécie de proteção, como a captura abaixo realizada na minha conta, na rede social Twitter em 2021, quando este me “ofereceu” para fazer a revisão das configurações de privacidade:

<sup>9</sup> Maiores informações em <https://www.facebook.com/policies/cookies>.

Figura 4 - Revisão da configuração de privacidade no Twitter (abr. 2020)



Fonte: <https://privacy.twitter.com/pt> (2021).

Figura 5 - Central de privacidade do Twitter (jun. 2022)



Fonte: Twitter (2022).<sup>10</sup>

Junto ao exercício de coleta das interfaces, realizado desde 2018, foi sancionada a Lei nº 13.709, em 14 de agosto do mesmo ano, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil, que resumidamente comenta no seu art. 1º:

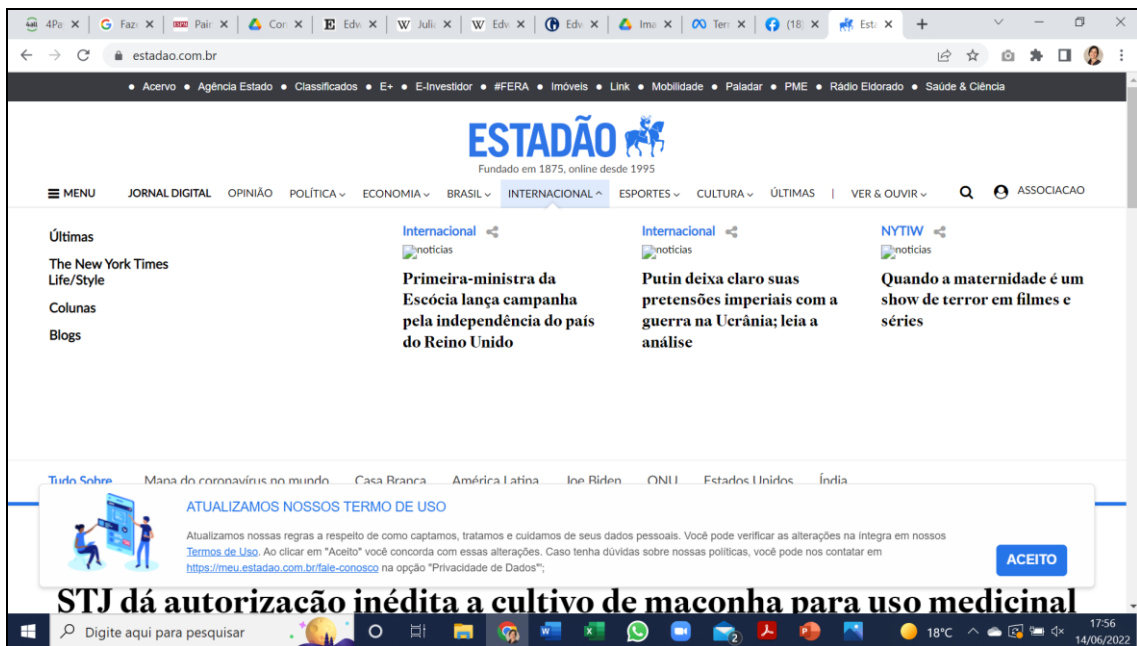
Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A criação da LGPD, dentre diversas iniciativas que visam proteger os dados dos cidadãos, exige que todos os *publishers* ou produtores de conteúdo e *sites* da internet, que coletam informações de usuários em território nacional, deveriam de adequar-se à regulamentação, informando e questionando se o visitante aceita a prática de coleta de dados,

<sup>10</sup> Maiores informações em <https://privacy.twitter.com/pt>.

a partir da inserção de *cookies* em suas páginas publicadas na internet. Ao entrar em vigor a regulamentação, os *publishers* passaram a inserir o questionamento em suas interfaces desde o primeiro contato com o usuário, como o exemplo na parte inferior da interface, a seguir, demonstra:

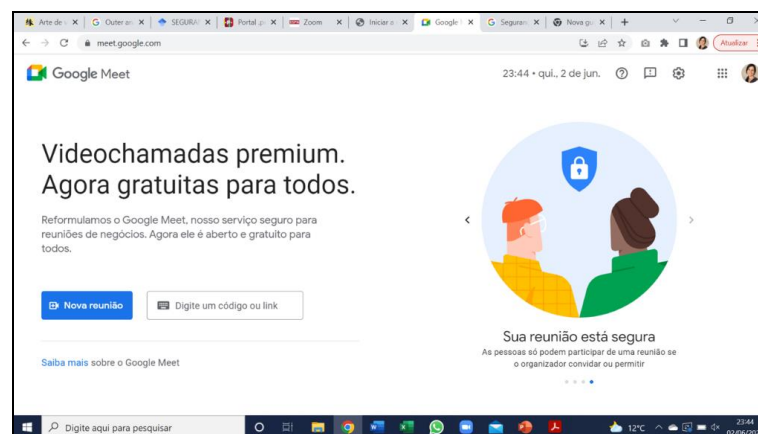
Figura 6 - Captura de tela do Estadão - uso de *cookies*



Fonte: Estadão (2022).

A captura de tela, abaixo, demonstra a preocupação com a segurança do conteúdo da reunião através da ferramenta de videochamadas Google Meet. O texto que acompanha a ilustração afirma que “sua reunião está segura”, concedendo ao usuário o controle de quem pode participar da reunião e, conseqüentemente, ter acesso ao conteúdo restrito:

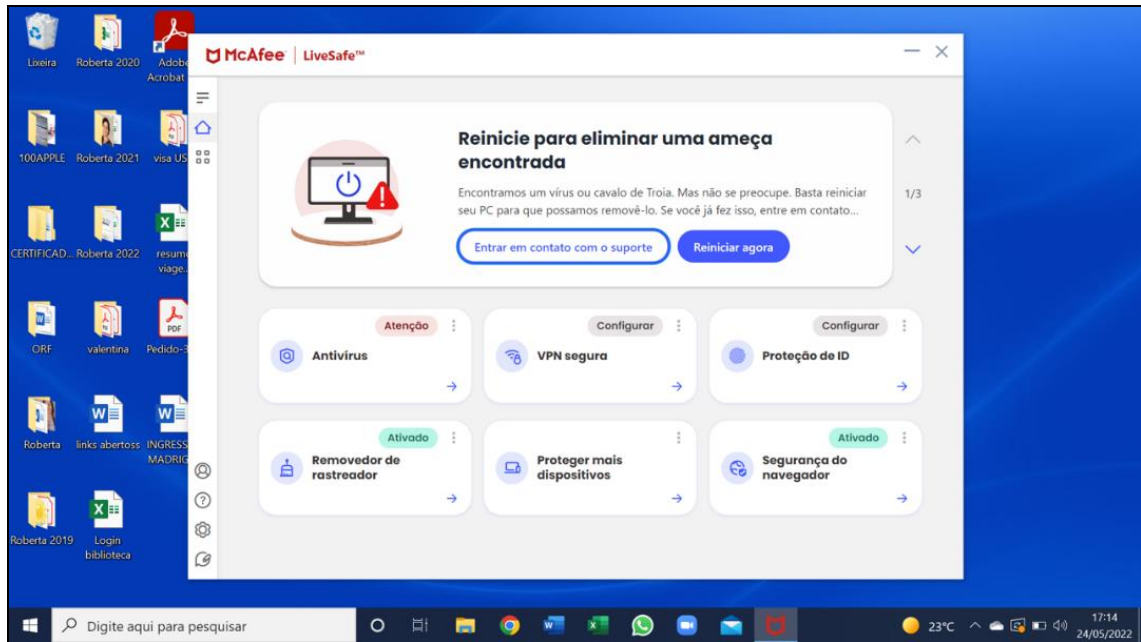
Figura 7 - Captura de tela do Google Meet - segurança nas reuniões por videochamada



Fonte: Google Meet (2022).

Outra maneira de chamar a atenção para o controle de proteção de informações é a partir da contratação de serviços denominados antivírus, que prometem segurar o acesso aos dados de um computador de uma possível ameaça *hacker*, como a sinalização capturada na interface, a seguir, do *software* McAfee LiveSafe, ferramenta paga que utilizo no meu *notebook* para fazer varreduras e monitorar o possível ataque por terceiros:

Figura 8 - Captura de tela (*notebook* pessoal) - mensagem de proteção do antivírus McAfee

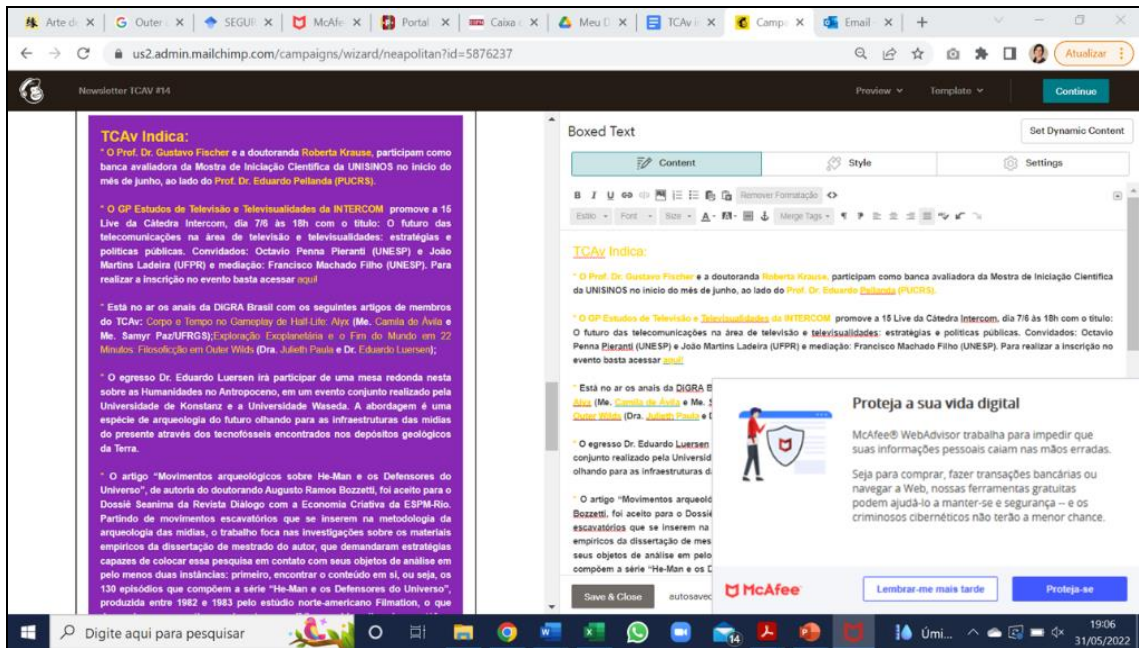


Fonte: Elaborado pela autora (2022).

De forma complementar, as duas capturas de tela, a seguir, mostram o momento de manifestação por mensagem *pop up*, do antivírus, ao identificar um possível acesso estranho no meu computador:

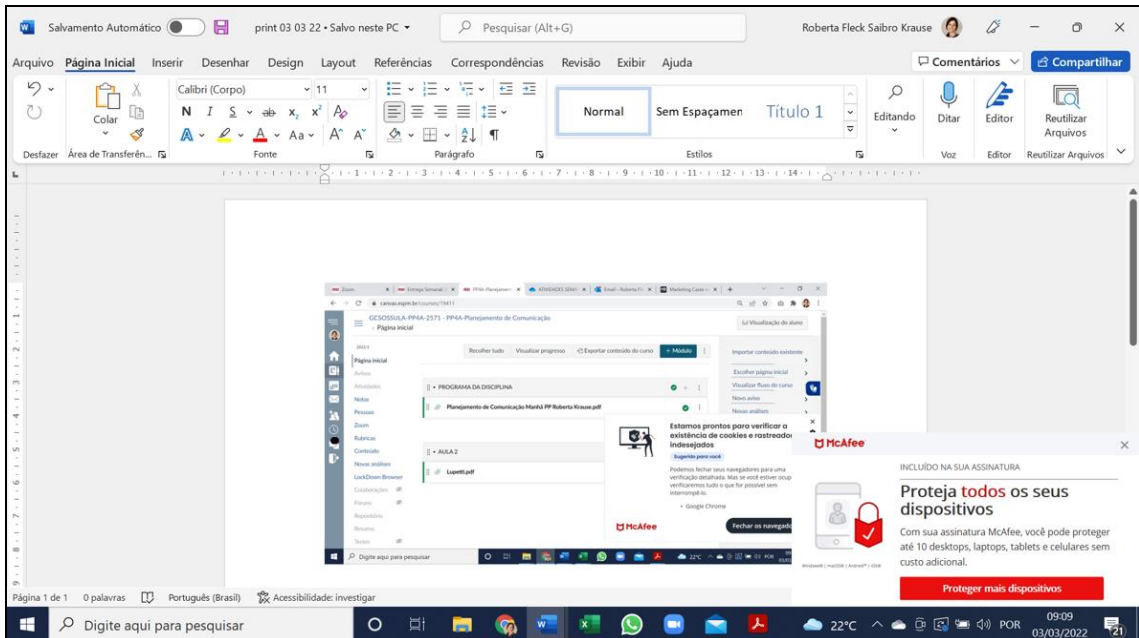


Figura 9 - Captura de tela (*notebook* pessoal) - mensagem do antivírus McAfee informando uma possível ameaça



Fonte: Elaborado pela autora (2022).

Figura 10 - Captura de tela (*notebook* pessoal) com mensagem do antivírus



Fonte: Elaborado pela autora (2022).

Ao longo desse processo de captura de interfaces em diversas iniciativas e colecionadas em meu *notebook* (e posteriormente, por precaução, também estão “salvas” na ferramenta Google Drive), desde antivírus, sistema bancário, publicidade etc., também fui compreendendo que a preocupação com a eficiência da segurança das informações e dos

dados de usuários que perambulam pela internet é um discurso que praticamente nasceu com a sua promessa do mundo *cyber*<sup>11</sup>. Wendy Chun (2006, p. 2, tradução nossa), na obra *Control and Freedom. Power and Paranoia in the Age of Fiber Optics*, já comentava que “O fim da Guerra Fria não dissipou a paranoia, mas a espalhou por toda parte: invisibilidade e incerteza – do inimigo, da tecnologia – invalidou a dissuasão e moveu a paranoia do patológico para o lógico”<sup>12</sup>. A autora comenta que existe uma relação direta entre o lançamento da internet como um meio de massa, e seu discurso combinado com a promessa de liberdade e acesso a tudo por todos, rompendo a centralidade do poder monopolístico, possibilitando o fluxo livre da informação, revigorando o discurso da liberdade de expressão e democracia.

Porém, como ela afirma, a questão central é muito mais importante do que decidir se a internet é vilã ou não, mas, compreender que há uma relação mais forte em discutir disciplina e liberdade sendo imposta na era da fibra ótica. Nesse aspecto, é possível associar o tema segurança com proteção de dados, monitoramento, privacidade, anonimato e confiança. Portanto, todas essas manifestações foram moldando a construção da problematização da tese, conforme descrevo a seguir.

### 1.1 Problema e objetivos de pesquisa

Ao questionar constantemente o que me afeta no objeto empírico, e tentar exercitar a problematização da tese, reforço que “para qualquer desenvolvimento do conhecimento, a pergunta é o ponto de partida. Quem não possui nenhum problema, nenhum questionamento, não pode avançar na produção do conhecimento” (GOMES, 2011, p. 1). Justamente, levando em consideração as inúmeras perguntas que me inquietavam ao encarar as interfaces do FB e da coleção de outras capturas envolvendo o tema segurança, em dispositivos móveis e na *web*, foi logo após a participação no seminário de tese, da linha *Mídias e Processos Audiovisuais*, no qual a crítica proveniente dos demais professores sobre o projeto foi “o que me olha no objeto?”. O que, de fato, poderia ser que estava me provocando a pensar *tecnoculturalmente* a tese? Portanto, me debrucei sobre o empírico e comecei a me deixar ser contagiada pelo

---

<sup>11</sup> No item 1.2 será explorado com mais detalhes outras manifestações midiáticas nas interfaces em relação à temática segurança, privacidade, proteção e anonimato.

<sup>12</sup> “The end of the cold war has not dispelled paranoia but rather spread it everywhere: invisibility and uncertainty – of the enemy, of technology – has invalidated deterrence and moved paranoia from the pathological to the logical.”

estado da arte do tema, pelas leituras das disciplinas e, principalmente, pelos encontros do Grupo de Pesquisa TCAv<sup>13</sup> e do Laboratório do Audiovisual em Rede (LAR).

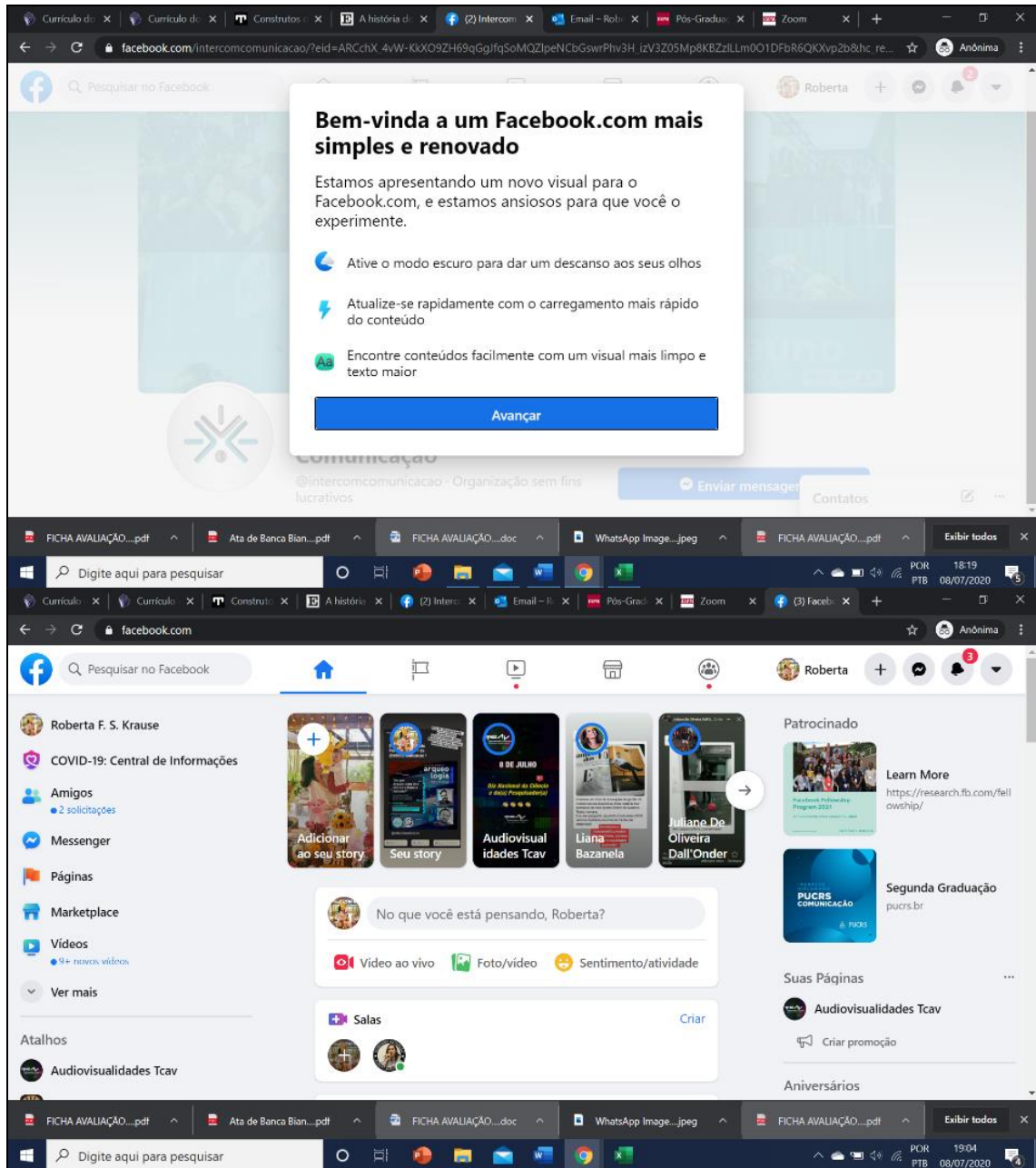
Nesse movimento, surgiram aspectos relacionados à memória e ao arquivamento, à relação com os meios, e à insistente mania de olhar as imagens, principalmente aquelas de Interface Humano Computador (HCI), nos termos de Lev Manovich (2001), como portadoras de memória e de historicidade próprias, a partir da proposta de Georges Didi-Huberman (1998). Nesse exercício surgiram questões como: a rede social FB atualiza sua interface para permanecer o quê? Qual a intenção dessa construção de interface com o usuário? O que a interface deseja guardar e se desfazer, num exercício de regeneração constantemente? O que dura ali? O que dura de “meu” no FB? Por que o FB diz que ali dentro estou “segura”? E, concomitantemente a essas provocações, durante esse período, o FB promoveu uma atualização de sua interface, com sugestão de *design* com cantos arredondados e novas funcionalidades, como novos ícones e atalhos, conforme registro<sup>14</sup> na imagem a seguir:

---

<sup>13</sup> Aqui vale comentar especificamente sobre um exercício de levantamento realizado com os demais colegas discentes do grupo TCAv, ainda em 2019, sobre as iniciativas dos *Media Labs* a partir da obra *What is a media lab? Situated practices in media studies* (2017) de Lori Emerson, Jussi Parikka e Darren Wershler.

<sup>14</sup> Desde o ingresso no doutorado, com o projeto de tese inicial que se propunha a questionar o FB e seu *player* de vídeos, mantive o hábito de registrar muitas interfaces da rede social, construindo uma verdadeira coleção de capturas de telas. Os registros estão armazenados em meu computador para um possível resgate para fins da pesquisa. Essa mania de colecionar interfaces do FB se identifica com a proposta metodológica de Maciel (2009) por coletar, colecionar, inventariar e classificar a partir da escrita.

Figura 11 - Excerto de tela da apresentação do novo *design* de interface do FB



Fonte: Facebook (2020).

Ao ter sido impactada pela mudança da interface do FB, me despertou o olhar para a estética das telas, o design e a forma que a rede social me identificou como do gênero feminino, ao direcionar a mensagem: “Bem-vinda a um Facebook.com mais simples e renovado”; caracterizando uma espécie de monitoramento e registro do meu primeiro contato com essa nova construção de conteúdo. Nesse momento, fiquei novamente intrigada pelo conteúdo do Seminário Intensivo, *Digital transformation and the humanities: contemporary technocultural dimensions for research in the social and human sciences*, com o Professor

Peter Krapp (2020a), da University of California Irvine (UCI), promovido pelo PPGCC UNISINOS em março de 2020. Durante o curso foram debatidas perspectivas sobre a comunicação digital, mas me chamou muito a atenção a linha abordada pelo Prof. Krapp (2020a) sobre as diversas formas de segurança da informação a partir da garantia da comunicação ser eficiente e secreta. Nesse momento, já havia sido provocada sobre o tema da segurança ou da garantia de privacidade na comunicação digital, ao ver potencialidade na discussão acerca de imagens técnicas, reproduzidas pelos *sites* de redes sociais, e o que o pesquisador apresentou durante o seminário, ao trazer uma revisão histórica sobre as mídias, a tecnologia, a comunicação secreta e a preocupação histórica com a segurança na transmissão da comunicação de ponta a ponta.

Portanto, o primeiro passo para exercitar o tema, submeti, ainda, de maneira ensaística em coautoria com o colega doutorando Lucas Ness, ao Congresso da Sociedade Brasileira de Estudos Interdisciplinares da Comunicação (INTERCOM), uma proposta de artigo que tensionava essa reflexão acerca das interfaces e sobre certa preocupação com a eficiência do segredo, a partir de recursos de imagens nas interfaces do Google e FB, por exemplo. O artigo discute, com base no conceito de imagem técnica<sup>15</sup>, de Vilém Flusser (2002), sobre a representação imagética de algo seguro e confiável ao usuário da *web*, que está fornecendo seus dados e suas publicações para *sites* como FB, permanece relacionada a associações tradicionais de segurança do “*modo offline*”, como cadeados, chaves, senhas, escudos, ícones de conteúdo criptografado, códigos QR, verificação de grupos de imagens semelhantes ou o *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA) e, até mesmo, o uso do *login* social<sup>16</sup>.

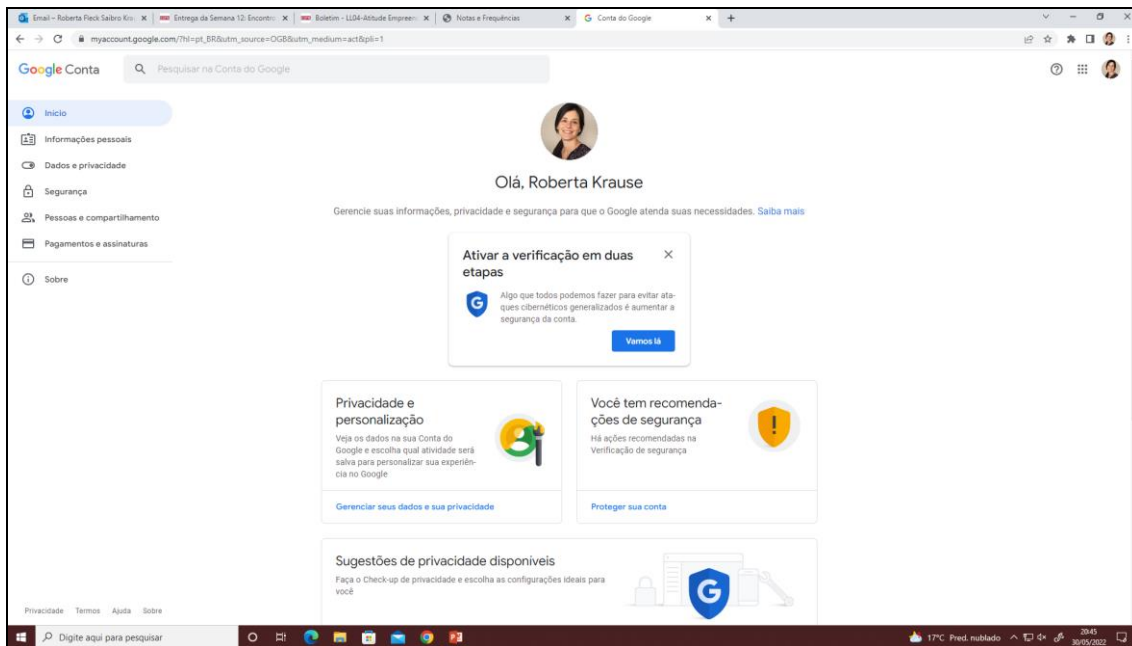
No artigo publicado, articulamos que, através da produção dessas imagens é que também se conduz essa sensação de proteção, ou seja, o FB fornece, ao usuário, a possibilidade de dupla autenticação de *login*, utilizando ferramentas como leitura de códigos QR, envio de mensagem via outro dispositivo, como o celular cadastrado na conta ou, ainda, chave de segurança via entrada USB; as ilustrações utilizadas para indicar as opções de autenticação também estão relacionadas com comunicação sigilosa, com cadeados, chaves e maçanetas “trancadas”. Nesse sentido, também foi possível verificar que o Google possibilita

<sup>15</sup> O autor articula sobre um tipo de imagem e sua relação com a tecnologia, denominada por ele como “imagens técnicas”, e que, resumidamente, seriam imagens produzidas por aparelhos ou “[...] aparelhos são produtos da técnica que, por sua vez, é texto científico aplicado. Imagens técnicas são, portanto, produtos indiretos de textos – o que lhes confere posição histórica e ontológica diferente das imagens tradicionais” (FLUSSER, 2002, p. 10).

<sup>16</sup> O *login* social permite que o usuário utilize seu cadastro já realizado em *sites* de redes sociais para acessar outros conteúdos *online* que exigem registros prévios. Ou seja, é possível entrar em um *site* através de *login* e senha cadastrados em terceiros.

uma série de formas de autenticação do usuário, cujas ilustrações reforçam a ideia de interdependência entre as opções – o *smartphone*, em segundo plano ao lado da chave, ganha destaque quando o serviço passa a falar sobre recuperação de senha, deixando-a em menor destaque, conforme captura a seguir:

Figura 12 - Captura de tela da seção Conta, no Google, e a preocupação com segurança e proteção

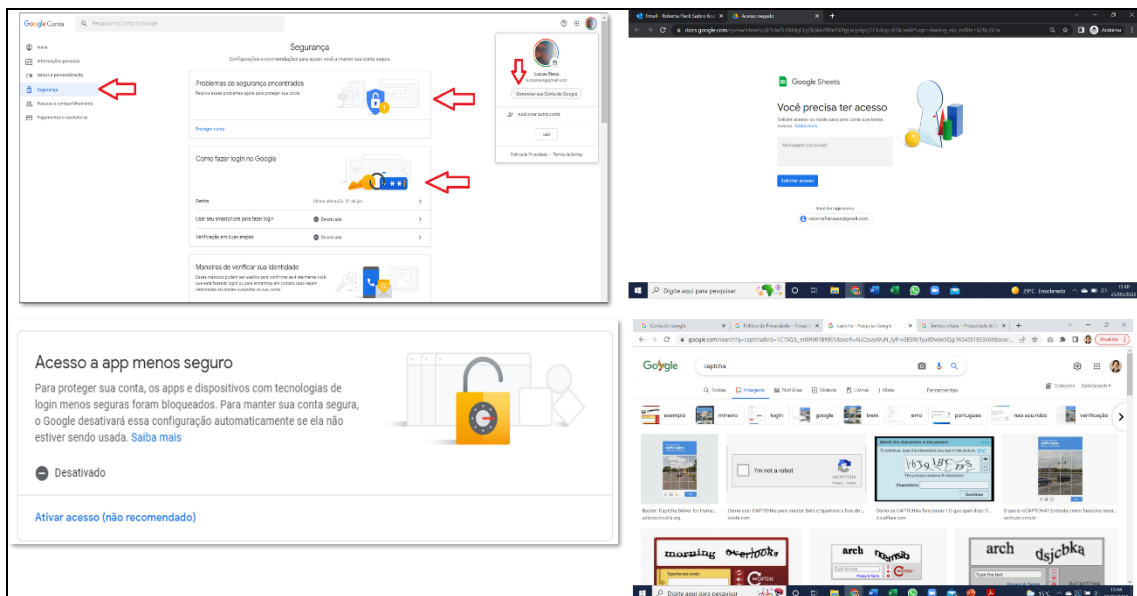


Fonte: Myaccount (GOOGLE, 2022).

O duplo *check* de verificação também sustenta a ideia de segurança e redução de chance de vazamento (ou uso não autorizado) de dados de usuários. E, como os serviços autenticadores não servem como acesso a qualquer serviço de terceiro, eles constroem padrões de segurança que são protocolos que garantem uma díade segurança-confiança:

Pela lógica de operação do mercado, os usuários do FB e Google autenticam muitas entradas em outros sites na internet através de login social, nos quais não há qualquer indicação de cadeado, escudo, chaves, etc. Então pode-se propor que o serviço autenticador conduz a sensação de segurança quando intermedia a entrega de dados e informações confidenciais fornecidos – a princípio, exclusivamente a ele – a um terceiro *player* de mercado (ao qual optou-se por não fornecer informações diretamente). Ou seja, o serviço autenticador parece ganhar o “status” de confiabilidade e segurança – suprimindo a necessidade de preencher um novo cadastro e seu fornecimento de dados, ou mesmo de memorizar uma nova senha de acesso para acessar aquele conteúdo ou serviço (KRAUSE; NESS, 2020, p. 10).

Figura 13 - Arranjo de capturas de telas com manifestações sobre proteção da conta no Google e do recurso Captcha



Fonte: Elaborado pela autora (2021).

Conforme defendido por Krapp (2020a) durante o seminário, a cultura digital está baseada na eficiência da comunicação, lembrando sobre as teorias da Comunicação, como a proposta de Shannon e Weaver de 1949 (WOLF, 1992), onde a matemática explica a lógica de transmissão dos impulsos elétricos entre um emissor e o receptor. Evitando, ao máximo, os ruídos para se obter sucesso na transmissão do sinal, “tratava-se, portanto, de conseguir estabelecer o modo mais econômico, mais rápido, e mais seguro de codificar uma mensagem, sem que a presença do ruído tornasse problemática a transmissão” (WOLF, 1992, p. 100).

Ao trazer a mesma lógica de comunicação segura para a contemporaneidade, onde a comunicação em rede está praticamente nas mãos de grandes empresas, conforme configura a lógica do capitalismo de vigilância, defendido por Zuboff (2020), é natural que os usuários “passivos” desse sistema se sintam mais à vontade ao disponibilizar seus dados e deixar “rastros” na *web*, sustentados por lógicas que apoiam o imaginário<sup>17</sup> de proteção ou segurança de informação.

De forma complementar, infiro que há potencialidades de discussão a partir do uso de imagens técnicas como um recurso visual para a construção de sentidos de segurança nas interfaces do Facebook (FB), que são autenticados por imaginários que enunciam *eticidades* próprias desse ambiente. Entendo haver espaço para refletir sobre a ambivalência entre

<sup>17</sup> Estou tratando como imaginário a definição de Kilpp (2002a, p. 41), em sua tese de doutorado, ao assumir “o imaginário como mediações, que são também um conjunto de marcas de enunciação das culturas (identidades coletivas), manifestas e visíveis nos discursos, na arte, nos produtos culturais..., ou que são por eles mediadas”.



liberdade, controle, monitoramento e segurança, na rede social, através de recursos próprios construídos na *web*, inseridos numa “*infoestética*” pela proposta de Lev Manovich (2012, p. 2), que reside em “mapear a cultura contemporânea para detectar formas estéticas e culturais emergentes específicas em uma sociedade da informação globalizada”.

Portanto, com enfoque nessa reflexão, foi possível intuir sobre o objeto e construir o problema de pesquisa muito mais em função do tempo do que do espaço. Ou seja, em termos bergsonianos, como diria Gilles Deleuze (1999, p. 9) “colocar o problema não é simplesmente descobrir, é inventar. A descoberta incide sobre o que já existe, atualmente ou virtualmente”. Nesse sentido, pensar sobre a construção de segurança a partir da perspectiva de sua **qualidade durante**, fez compreender que parte do exercício que estou fazendo, ao longo do doutorado, em realizar capturas de telas do FB e outras zonas na *web*, junto com a pesquisa da pesquisa e as demais atividades que o processo de doutoramento exige, foram extremamente importantes para a construção do trajeto em direção a pensar sobre os sentidos de *tecnosegurança* pelo FB.

Ao exercitar a construção do questionamento que norteia a pesquisa, primeiramente é preciso compreender que tudo possui dois modos, o de ser e o de agir (BERGSON, 2006a). Partindo dessa perspectiva que “matéria e duração nunca se distinguem como duas coisas, mas como dois movimentos, duas tendências, como a distensão e a contração” (DELEUZE, 1999, p. 131), entendo que é pelo Método da Intuição de Bergson que devo refletir sobre o que dura do objeto de pesquisa, como virtualidade que se atualiza em atuais, preciso compreender que “duração é memória, porque ela prolonga o passado no presente [...] o passado coexiste consigo como presente” (DELEUZE, 1999, p. 134).

Me apoio nas palavras de Gomes (2011, p. 14) “assim como para McLuhan o meio é a mensagem, presentemente se pode afirmar que o processo é o objeto”, nesse sentido, permanecendo com os fundamentos do método intuitivo de Bergson, com base na proposta apresentada por Deleuze (1999), compreendo que, conforme a construção do misto de tempo (virtual) x espaço (atual), o que de fato dura em meu interesse de pesquisa são os sentidos de segurança. Portanto, pensar em duração “é o que difere ou o que muda de natureza, a qualidade, a heterogeneidade, o que difere de si mesmo” (DELEUZE, 1999, p. 130), pressupõe uma coalescência, não uma hierarquia, já que, a partir da intuição, o real é o movimento de duração e atualização.

Assim, passei a encarar a atualização dos sentidos de *tecnosegurança* autenticados pelas interfaces do FB como misto. Mas como foi possível fazer esse movimento? A partir da reflexão de que as enunciações de sentidos de *tecnosegurança* se atualizam no FB seguindo



características próprias da rede social, com centralidade específica, forma e importância na interface, seguindo uma lógica individual, mas sempre inscrita dentro da *tecno cultura*, conforme foi possível verificar como uma preocupação em diversas manifestações nas interfaces apresentadas previamente.

Dessa maneira, olhar para a segurança pela “lente” da *tecno cultura* nos conduziu à compreensão de que é preciso encará-la como independente da internet, ou seja, segurança é um tema socialmente central, mas que vem ganhando cada vez mais protagonismo na cultura digital, e a busca por ela é a audiovisualização da cultura como sintoma de nossa época, por câmeras de segurança, por sistema de reconhecimento facial, pela vigilância e monitoramento de dados, muitas vezes, fornecidos pelos usuários em redes sociais ou coletados por dispositivos conectados à internet; é retratada em nossa cultura, até mesmo em campanhas publicitárias, conforme será mostrado no subcapítulo 1.3. Nesse sentido, a partir da proposta de Zygmunt Bauman, na obra *Comunidade. A busca por segurança no mundo atual* (2003), e da reflexão de Wendy Chun (2006) sobre a ambivalência característica da era da fibra ótica (que alterna entre manter controle e oferecer liberdade), é que organizo parte do suporte teórico para refletir sobre a construção dos sentidos de *tecnosegurança* que são durante na ambiência das interfaces do e no FB.

Bauman (2003) relaciona à comunidade uma série de sensações de ordem otimista, profícua e benéfica e que associa às imagens de um território aconchegante e protegido das ameaças “externas” à interface. Porém, há ambivalência no termo, pois, segundo o autor, em ordem de se manter seguro e protegido em uma comunidade, deve-se renunciar à liberdade, criando uma espécie de “fábricas de obediência”, onde todos seguem regras e doutrinas, sem questionar o poder de controle (BAUMAN, 2003, p. 42).

Portanto, é a partir de toda essa reflexão que chego ao questionamento: **Como são construídos sentidos durante de *tecnosegurança* pela ambiência Facebook?** Assim, configura-se o objeto da pesquisa como **atualizações de *tecnosegurança* pelas interfaces do Facebook.**

Deste modo, o objetivo geral dessa pesquisa visa **compreender como são construídos sentidos durante de *tecnosegurança* pela ambiência Facebook.** No intento de complementar a construção do problema de pesquisa, determinam-se como objetivos específicos:

- a) articular discussões relacionadas à privacidade e à segurança, na cultura digital, à perspectiva das audiovisualidades da *tecno cultura*;

- b) formular o conceito de “*tecnosegurança*” enquanto sintoma da *tecnocultura* contemporânea, que se espalha através e para além das mídias, produzindo uma ambiência;
- c) autenticar sentidos de segurança e de privacidade enunciados pelas interfaces do Facebook.

Junto a isso, é impossível não mencionar que a continuidade das discussões e reflexões nas disciplinas e do Grupo TCAv, que sempre tiveram uma espécie de caráter de orientação coletiva e laboratorial, foram sendo interfaceados no contexto da pandemia via transmissão por *streaming* e *webcams*, a partir do aplicativo Microsoft Teams. Portanto, a reconfiguração da própria ambiência comunicacional foi sendo alterada para um protagonismo das câmeras, interfaces, fluxo de dados e (in)segurança, dentro e fora das mídias, numa troca de imagens e informações que viabilizam nossas atividades acadêmicas e profissionais nesse convívio virtual. Dito isso, organizo no próximo item do capítulo, *Sentidos de tecnosegurança nas mídias*, diversas manifestações encontradas durante esse período de realização do estado da arte, passando por manifestações que demonstram um tipo de preocupação do imaginário coletivo sobre como a *tecnosegurança* foi emergindo ao olhar o objeto empírico.

## 1.2 Sentidos de *tecnosegurança* nas mídias

Conforme dito no subcapítulo 1.1, fomos<sup>18</sup> identificando ao longo do amadurecimento do tema, em diversas manifestações midiáticas, sentidos de segurança na *tecnocultura*. Buscamos trazer para a discussão do estado da arte como o tema vem sendo tratado em alguns espaços, como na publicidade, nas produções de entretenimento via *streaming* e, até mesmo, nos memes que circulam nas redes sociais, em diversas iniciativas da *web* e em aplicativos móveis, passando por *softwares*, como Google e Microsoft, até versões menos reconhecidas. As fontes revisadas aqui não são exclusivamente acadêmicas, mas de jornais, revistas, relatórios e audiovisuais de TV ou internet, na medida em que percebemos o tema da segurança de dados e manutenção de privacidade, sendo cada vez mais mencionado, além de diversas capturas de telas de nosso *notebook*.

Porém, apesar da temática estar ganhando cada vez mais espaço na *tecnocultura* que vivemos atualmente, ela acompanha a promessa de “nascimento” da *internet*, conforme Chun (2006) e teve uma das mais emblemáticas manifestações há quase 30 anos, quando o

---

<sup>18</sup> A partir deste subcapítulo do texto assumo a primeira pessoa do plural, já que as reflexões realizadas não são feitas a partir de escolhas individuais, mas, em diálogo com os autores lidos e meus orientadores.

cartunista Peter Steiner, da revista *New Yorker*, criou um desenho chamado *On the internet, nobody knows you're a dog*<sup>19</sup> (CAVNA, 2013, tradução nossa), para a edição de 1993. A intenção do artista era justamente provocar o debate sobre a possibilidade de uso de diversas identidades no território da internet que estava se popularizando nos anos 1990. Chamando a atenção para aspectos associados à privacidade e anonimato, sua publicação foi feita um ano antes do lançamento no mercado do navegador Netscape Navigator, importante ferramenta para popularização da internet aos usuários, no formato html. O *cartoon* é até hoje a ilustração mais reproduzida da história da revista *New Yorker*, de acordo com matéria publicada no jornal *The Washington Post* (CAVNA, 2013).

Figura 14 - Charge do cartunista Peter Steiner



Fonte: Cavna (2013).

Complementando o relato desse exercício de encontro e coleta de manifestações associadas ao tema segurança, verificamos algumas iniciativas relacionadas à área jurídica, como a Associação de Pesquisa Data Privacy Brasil (DPB), que “produz pesquisas e ações de incidência na intersecção entre tecnologias, uso de dados e direitos fundamentais” (DATA PRIVACY BR, 2020), promovendo cursos de formação e uma série de debates que dão

<sup>19</sup> “Na internet, ninguém sabe se você é um cachorro.”

suporte ao respeito à Lei Geral de Proteção de Dados (LGPD)<sup>20</sup> no Brasil. Além disso, há um mercado em ascensão que busca fornecer consultoria em LGPD, adequando empresas e *publishers* às exigências da legislação em vigor, como a empresa Privacy Tools, líder do segmento, configurando-se como “PrivacyTech, uma plataforma de gerenciamento de privacidade [...] com módulos pensados para o uso em diferentes segmentos do mercado e para cumprir com as obrigações das diferentes legislações, como LGPD e GDPR<sup>21</sup>” (PRIVACY TOOLS BR, 2022).

É importante salientarmos que há uma relação muito forte entre privacidade de informações, a partir dos dados circulando na *web* e dispositivos conectados à internet, com a construção de segurança baseada na confiança que se instaura nesses bancos de dados ao utilizar da maneira correta, ou melhor, adequada à LGPD, as informações coletadas nessa tecnologia.

Figura 15 - Postagem no Instagram do Data Privacy Brasil



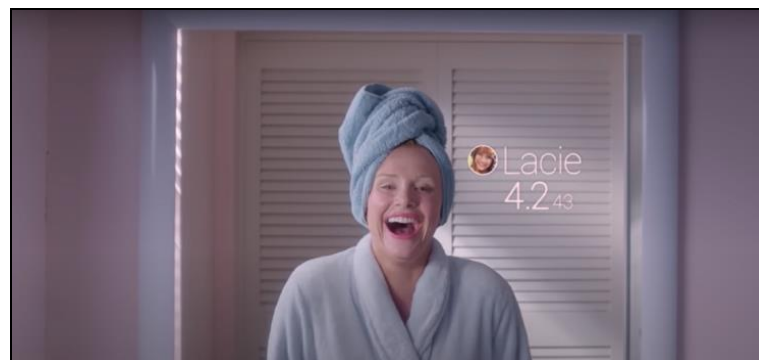
Fonte: Data Privacy BR (2021).

<sup>20</sup> “A Lei Geral de Proteção de Dados Pessoais, conhecida como LGPD, é o normativo brasileiro que fala sobre a proteção de dados pessoais (Lei nº 13.709/2018). Foi sancionada em agosto de 2018 e entrou em vigor em setembro de 2020. Essa Lei se aplica tanto à pessoa jurídica quanto física que promovem o tratamento de dados pessoais no Brasil. Além disso, é importante destacar que a Lei protege esse tipo de informação independente do meio de armazenamento. Dessa forma, estejam em dispositivos tecnológicos ou físicos, como papéis e até mesmo simples anotações, deverão ser protegidos. É importante destacar que a LGPD representa uma evolução no que diz respeito à privacidade e simboliza um equilíbrio nas relações jurídicas, uma vez que estabelece regras para o tratamento de dados pessoais. A Lei já está em pleno vigor, mas ainda é um imenso desafio para todos” (LGPD ESPM, 2022).

<sup>21</sup> Sigla utilizada para a *Global Data Protection Regulation* – regulamentação em vigor no continente europeu.

Essa temática vem ganhando força justamente com a aprovação da LGPD no Brasil, um dos poucos países, além do continente europeu, a ter uma lei que blinda o uso de dados de usuários a partir de iniciativas públicas, privadas e governamentais. Um exemplo dessa propagação da preocupação com a segurança de dados, na internet, pode ser visto em produções de entretenimento como a série *Black Mirror* (BROOKER, 2016), mais especificamente no episódio número 1, da terceira temporada, portanto do ano de 2018, com o título *Free Fall*<sup>22</sup>, onde a personagem principal vive uma obsessão por ser a mais bem avaliada em um sistema de ranqueamento em uma rede social, muito similar ao Tinder, por exemplo, pela pontuação concedida por demais usuários da rede. Esse *score* de todos os usuários é um sistema que acaba por refletir em outros aspectos sociais, como acesso a benefícios na obtenção de melhores oportunidades de emprego, relacionamento e moradia, por exemplo. Esse sistema fictício de classificação de pessoas, do episódio, retrata como as redes sociais acabam por moldar comportamentos e criar falsas expectativas sobre os usuários a partir de um ranqueamento de dados. Forçando-os a uma conduta que supervaloriza um sistema de avaliação a ser concedido por terceiros, simulando um constante monitoramento social baseado em comportamentos adequados à avaliação alheia.

Figura 16 - *Black Mirror* - Netflix 2016



Fonte: Netflix (2021).

Essa espécie de *ranking* de confiança, utilizado a partir de um sistema de inteligência artificial para classificar indivíduos na série *Black Mirror*, entrou em operação na China em 2020, chamado de Sistema Nacional de Crédito Social, que, de acordo com a Human Rights Watch (2019), implementa uma lógica de controle e vigilância dos cidadãos através de um algoritmo.

<sup>22</sup> Em livre tradução: “Queda Livre”.

O mais notável é o “sistema de crédito social”, em que o governo promete punir o mau comportamento, tais como tráfego imprudente e o não pagamento de custas judiciais, e recompensar a boa conduta. A “confiabilidade” das pessoas – conforme avaliada pelo governo – determina o acesso a bens sociais desejáveis, como o direito de viver em uma cidade agradável, colocar as crianças em uma escola particular ou viajar de avião ou trem de alta velocidade (HRW, 2019).

Um modelo de controle social que está embasado na vigilância e argumentado sob a lógica da segurança dos cidadãos, lembrando o *Big Brother* de George Orwell, no livro *1984*, não se trata de mera coincidência. Nesse sentido, a proposta de Shoshana Zuboff (2020, p. 18) ao conceituar por capitalismo de vigilância a prática que justamente “reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais”, nos direciona a refletir sobre as dinâmicas de coleta, armazenamento e uso de informações privadas ou cedidas espontaneamente por usuários na internet. Ao encontro desse posicionamento, recentemente no ano de 2021 a prefeitura da cidade de Recife (PE), alertou sobre a possível implementação de câmeras de vigilância social em tráfego urbano para fins de monitoramento do trânsito na cidade. Para alertar os civis sobre os possíveis danos dessa tecnologia, a Rede Latino-Americana de Estudo sobre Vigilância, Tecnologia e Sociedade (Rede Lavits), criou uma página na internet que concentra informações sobre essa tecnologia e promove a campanha chamada “Sem câmera na minha cara”, na qual visa coletar assinaturas da população, conforme afirma na *homepage*:

A Prefeitura da Cidade do Recife (PCR) quer contratar uma empresa para instalar e gerenciar 108 “relógios” inteligentes com câmeras de reconhecimento facial em toda a cidade. A compra tem como objetivo mapear os rostos dos cidadãos para fins de monitoramento do trânsito. Mas como ela irá usar e armazenar seus dados? Ninguém sabe. O que sabemos é que vários países estão banindo a tecnologia por ela ser imprecisa, antiética e discriminatória, gerando “falsos positivos” que escancaram seu viés racista por encarcerar ainda mais pessoas negras (SEM CAMERA NA MINHA CARA, 2022).

De maneira complementar, no livro *Automating vision: the social impact of the new camera consciousness*, de Anthony McCosker e Rowan Wilken (2020), os autores debatem sobre o impacto causado nos indivíduos sobre ter a consciência intensificada pela presença da câmera, apontando “ambivalência e tensão específicas no cerne das tecnologias automatizadas dirigidas por IA, aquele que surge de forma mais dramática com câmeras e máquinas inteligentes, sistemas de visão como eles se fazem sentir”<sup>23</sup> (MCCOSKER; WILKEN, 2020, p. 3, tradução nossa).

---

<sup>23</sup> “Our core contribution to debates is to point to a particular ambivalence and tension at the heart of automated AI-driven technologies, one that surfaces most dramatically with smart camera and machine vision systems

Os programas piloto para o chamado “sistema de crédito social” da China usam uma série de tecnologias coordenadas, incluindo reconhecimento de rosto, centrado na câmera e técnicas de governança cada vez mais automatizadas. O objetivo final para a China deve gerar um “índice de confiabilidade” e, ao integrar identificação, policiamento assistido por algoritmo e técnicas de exposição social, entra em uma nova fase de governança social e econômica<sup>24</sup> (MCCOSKER; WILKEN, 2020, p. 1, tradução nossa).

Essa “consciência da câmera” se intensifica com a presença das câmeras inteligentes em nosso dia a dia, causando um impacto pela constante vigilância, já que “designa tanto o aumento de poder e mudança na visão e visibilidade que o processamento do computador contribui para o trabalho que as câmeras fazem [...], mas se refere aos casos de ansiedade que se multiplicam e vulnerabilidade que se seguem”<sup>25</sup> (MCCOSKER; WILKEN, 2020, p. 3, tradução nossa). Nessa mesma abordagem, o pesquisador André Lemos (2009, p. 625), em artigo citado previamente nessa pesquisa, alertava sobre uma nova forma de vigilância invisível, criando o que ele designa como o “sujeito inseguro”<sup>26</sup> na contemporaneidade, onde explora “a questão das câmeras de vigilância e das transformações que elas aportam à relação do sujeito com o espaço público e a cultura em geral”. No mesmo artigo, Lemos (2009, p. 625) comenta, ainda, sobre a pesquisadora Mireille Rosello (2008), que trata sobre o tema *subject insecure* em pesquisa proferida na palestra em Montreal, dizendo que “o modo da insegurança passa a ser uma ontologia, uma forma de ser, de conhecer e de ler a contemporaneidade. [...] Essa é a primeira constatação e o pano de fundo para a compreensão do problema da vigilância hoje”.

Levando a mesma temática ao centro, outras produções audiovisuais para a Netflix tomaram espaço ao trazer à tona discussões sobre mau uso de dados e a segurança da informação, como o documentário *Coded Bias*, que relata falhas relacionadas a racismo e discriminação, na tecnologia de inteligência artificial e reconhecimento facial, com base nas pesquisas de Joy Buolamwini, do Laboratório de Mídias, no Massachusetts Institute of Technology (MIT)<sup>27</sup>.

---

as they make themselves felt. With smart cameras, this tension shows up as a new form of heightened camera consciousness.”

<sup>24</sup> “Pilot programs for China’s so called ‘social credit system’ use a range of coordinated technologies, including face recognition, in their camera-centered and increasingly automated governance techniques. The ultimate goal for China is to generate a ‘trustworthiness index’ and, by integrating automated identification, algorithm-assisted policing and social shaming techniques, enter a new phase of social governance and economic order.”

<sup>25</sup> “Camera consciousness designates both the augmenting power and shift in vision and visibility that computer processing contributes to the work that cameras do. It also refers to the multiplying instances of anxiety and vulnerability that follow.”

<sup>26</sup> O conceito de sujeito inseguro será explorado no Capítulo 2 de nossa pesquisa.

<sup>27</sup> Maiores informações em <https://www.media.mit.edu/people/joyab/overview/>.

O argumento da tese de Buolamwini (2018, tradução nossa) intitulada *Tons de gênero: disparidades de precisão interseccional em classificação de gênero comercial*<sup>28</sup>, relata como o uso dos dados de cidadãos são coletados (sem sua autorização) a partir de sistemas de reconhecimento facial implementados por câmeras de “segurança” e vigilância por meio de instituições de poder, como lojas comerciais até governos, por exemplo. O uso desses sistemas de inteligência artificial (IA) instalados nas câmeras em ruas, avenidas, condomínios, *shopping centers*, etc., são utilizados como recursos para fins de controle de violência urbana e vigilância populacional, mas apresentam inúmeras falhas, identificadas e divulgadas pela tese de Buolamwini (2018), como tendência à classificação negativa de indivíduos do gênero feminino e pele negra, por exemplo. Portanto, há imprecisão na classificação das pessoas por meio de dados recolhidos através de IA, e esse tipo de resultado impacta diretamente na maneira como “a vida é traduzida de maneira unilateral em dados, expropriada e modificada em seu propósito como novas formas de controle social, tudo isso em serviços de outrem ou na ausência de nossa consciência e meios de combater esse processo” (ZUBOFF, 2020, p. 71), configurando a proposta do capitalismo de vigilância. Ao encontro da necessidade de sensação de proteção dos dados de usuários, coletados com a tecnologia da engenharia de computação, está o conceito proposto de “*privacy by design*”<sup>29</sup>, que está intimamente relacionado ao conceito de “tecnologias de aumento da privacidade” ou PET.

Esse termo foi usado pela primeira vez no relatório *Tecnologias para aumentar a privacidade: o caminho para o anonimato*, publicado em 1995 (HUSTINX, 2010, p. 253, tradução nossa). Essa proposta, além de estar prevista no art. 46 da LGPD, defende a proteção de dados como premissa inicial para o desenvolvimento de qualquer projeto de uso de tecnologia, como tornar visível a coleta de dados individualmente, mapear corretamente o uso dessas informações coletadas, visando nunca expor o usuário. Esses conceitos foram fundamentais para a construção do que atualmente denominamos por *UX Design* ou *design* com foco na experiência do usuário, tema que será debatido no Capítulo 2, onde abordaremos a *tecnosegurança* contemporânea.

Retomando nossa relação com as câmeras e obsessão por segurança e controle na *tecnocultura*, a partir das imagens e no constante monitoramento, também se reflete em modos de vigiar nossas casas desde os sistemas internos de vigilância, uma vez que, até mesmo, bebês são assistidos em câmeras do tipo “babá eletrônica” para que os pais tenham a sensação de tranquilidade e monitoramento da criança enquanto adormece. Abaixo fizemos

---

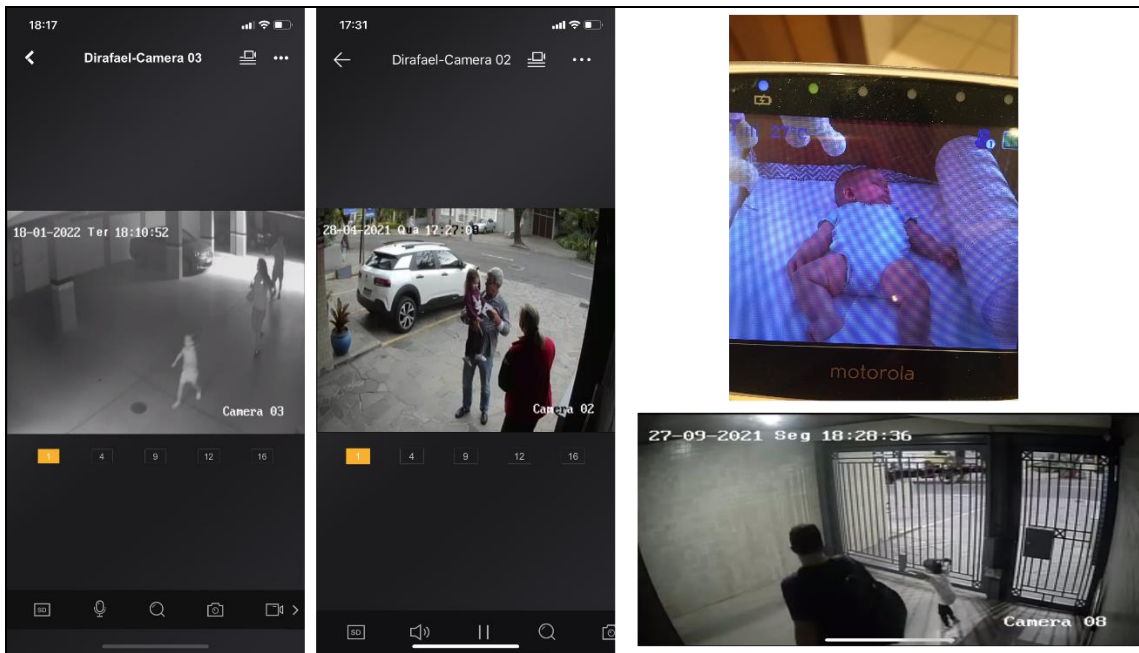
<sup>28</sup> “Gender shades: intersectional accuracy disparities in commercial gender classification.”

<sup>29</sup> “Privacidade desde a concepção.”



uma composição de imagens provenientes da câmera do circuito interno do prédio onde residimos, além de captura de tela da câmera de monitoramento infantil que dispomos, ambas realizadas via aparelho *smartphone* modelo Apple Iphone 11. O sistema de câmeras do prédio é acessado via aplicativo da empresa de segurança condominial contratada, onde todos os moradores têm acesso através de *login* e senha próprios, e a fotografia da câmera de monitoramento Motorola foi feita pelo aplicativo Câmera, já disponível também como uma das funcionalidades do celular.

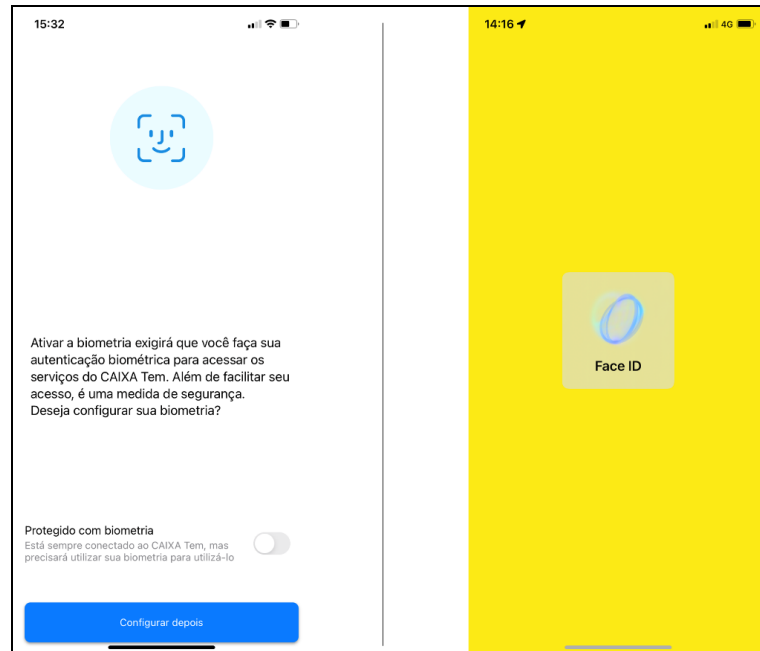
Figura 17 - Arranjo de imagens capturadas nas câmeras de vigilância pessoal



Fonte: Elaborado pela autora (2018; 2021; 2022).

Além de nossos *smartphones* apresentarem câmeras fotográficas, há também a funcionalidade disponível para *softwares* com sistemas de reconhecimento facial, como forma de *login* e acesso às funcionalidades do aparelho, configurando segurança aliada à confiança concedida ao *software* por manter nossas informações privadas. A seguir, realizamos coletas dessa funcionalidade em algumas iniciativas contemporâneas disponíveis em formatos de aplicativos para *smartphone* para fins de otimização dessa tese. Todas elas argumentam seu uso para garantia de segurança e privacidade de acesso a determinado *software*, como no exemplo, aplicativos do sistema bancário brasileiro:

Figura 18 - Arranjo de capturas de telas provenientes de sistemas de reconhecimento facial



Fonte: Elaborado pela autora (2021; 2022).

Identificando a relevância dessa temática na sociedade, a marca mais valiosa do Brasil, Itaú Unibanco, de acordo com a BrandZ Brasil (INFOMONEY, 2020), lançou, em março de 2021, uma campanha institucional com 3 filmes de 30”, e, em 2022, mais 4 filmes de 30” e várias peças para as mídias digitais, com o tema Privacidade, utilizando a *hashtag* *#protegidos*. O texto de apoio apresenta os termos que atravessam toda a campanha, como privacidade, proteção, segurança e confiança:

Na vida, a privacidade é um direito. No Itaú, ela faz parte dos nossos valores. Acreditamos na transparência e responsabilidade no uso dos dados que nos são fornecidos. Nosso aplicativo, website e centrais de atendimento são projetados para proteger os seus dados e respeitar a sua privacidade (ITAÚ, 2021).

Figura 19 - Excerto do YouTube com o comercial Itaú - Privacidade - Informação



Fonte: YouTube (2021).

Trazemos aqui trechos do primeiro filme publicitário de lançamento da campanha que tem o título *Privacidade – Informação*, desenvolvido pela agência de publicidade África, produzido pela O2 filmes e com direção de Fernando Meirelles. O filme traz dois homens caminhando na rua, quando um aborda o outro apresentando todas as informações pessoais sobre ele, como nome completo, endereço, número do cartão de crédito e código de segurança. A locução de assinatura da peça acompanhada do *lettering* Privacidade, é “Proteger seus dados não é brincadeira, o Itaú cuida da sua privacidade. Feito para você confiar”.

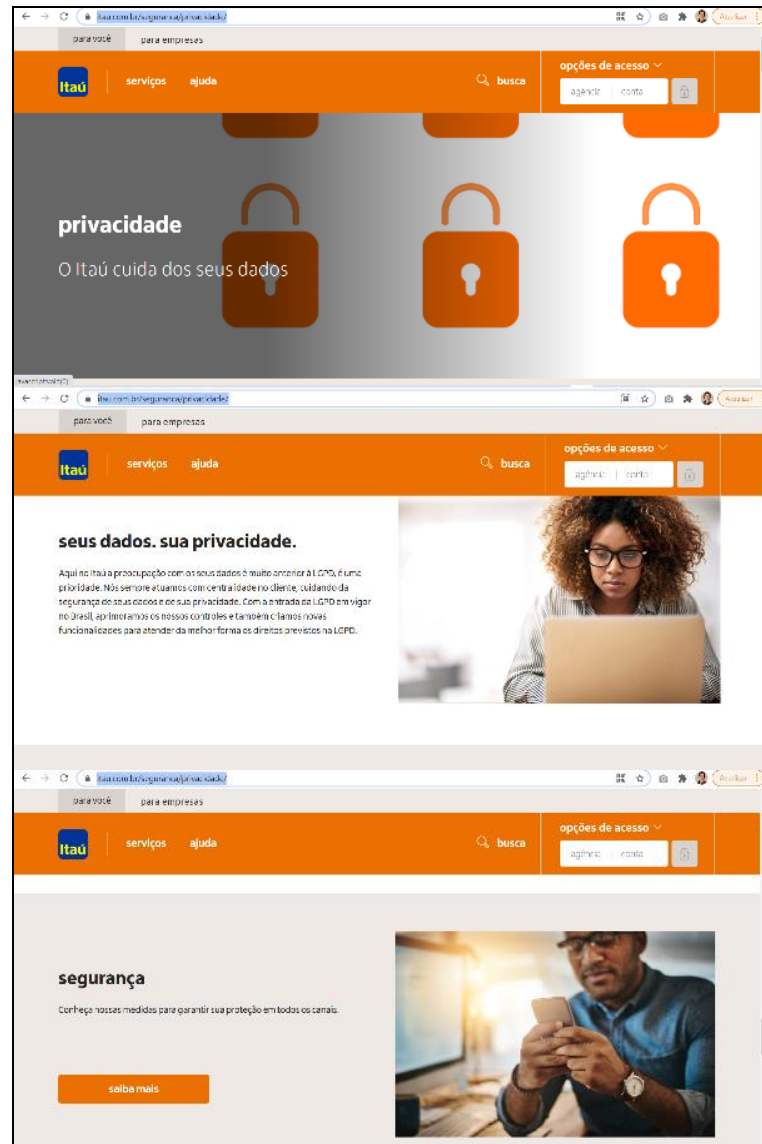
Figura 20 - Captura de tela do último *frame* do comercial Itaú - Privacidade - Informação



Fonte: YouTube (2021).

Como podemos visualizar nas capturas de tela do comercial e do *site* institucional do Itaú, que a campanha apresenta ao longo de seu conteúdo textual e visual, referências associadas à *imageria* para a construção de uma comunicação segura, como os cadeados na tela inicial e ao assinar a peça.

Figura 21 - Excerto da tela da página da campanha institucional banco Itaú - Privacidade

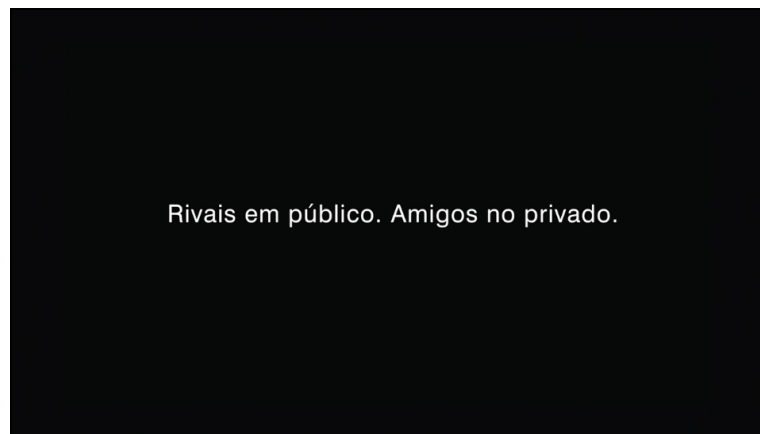


Fonte: Itaú (2021).

A partir da temática central abordada na campanha publicitária, segurança e privacidade de dados ocupam um espaço na discussão pública e social nos últimos anos, e, ao encontro dessa argumentação, o aplicativo de mensagens WhatsApp (META, 2022), que possui “mais de 1,5 bilhão de usuários ativos em 180 países” (ALMAPBBDO, 2022), também fez publicidade lançada em 2020 com a primeira campanha global com início no Brasil. Sob o tema “Fica só entre vocês”, associa diretamente a privacidade do conteúdo das mensagens

restrito aos usuários que estão em contato na mesma conversa, conforme afirmou a líder de *consumer marketing* no Brasil, Taciana Lopes, em entrevista à revista *Meio&Mensagem* em 2020: “Isso permite que as pessoas tenham uma relação verdadeira com o app, e é isso que queremos mostrar. É uma campanha de longo prazo” (SILVA, 2020). O primeiro filme tem duração de 1 minuto e teve veiculação na televisão aberta e fechada, nas redes sociais da Meta, empresa proprietária do Facebook, WhatsApp, Messenger e Instagram e nos cinemas.

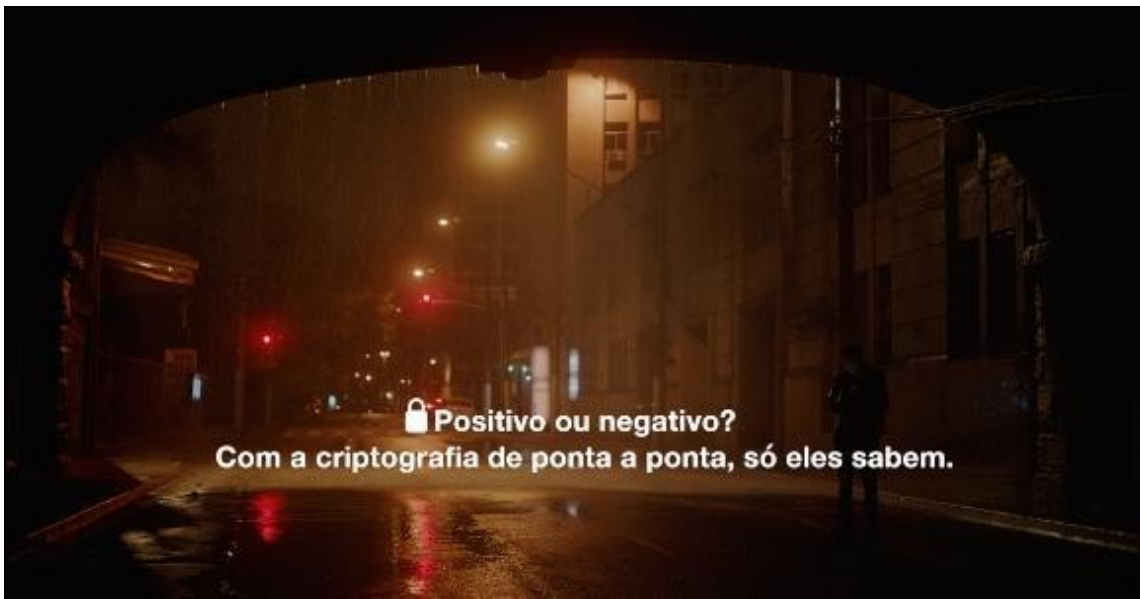
Figura 22 - Captura de tela do comercial do WhatsApp com o tema privacidade



Fonte: *Meio&Mensagem* (2022).

Insistindo no tema segurança e na argumentação da defesa do anonimato nas conversas entre seus usuários, em agosto de 2021, sob o tema “criptografia de ponta a ponta”, o WhatsApp deu continuidade à campanha publicitária no Brasil, com veiculação nos meios televisão aberta, fechada e redes sociais da Meta.

Figura 23 - Captura de tela do segundo filme publicitário do WhatsApp da campanha “Criptografia de ponta a ponta”



Fonte: *Meio&Mensagem* (2022).

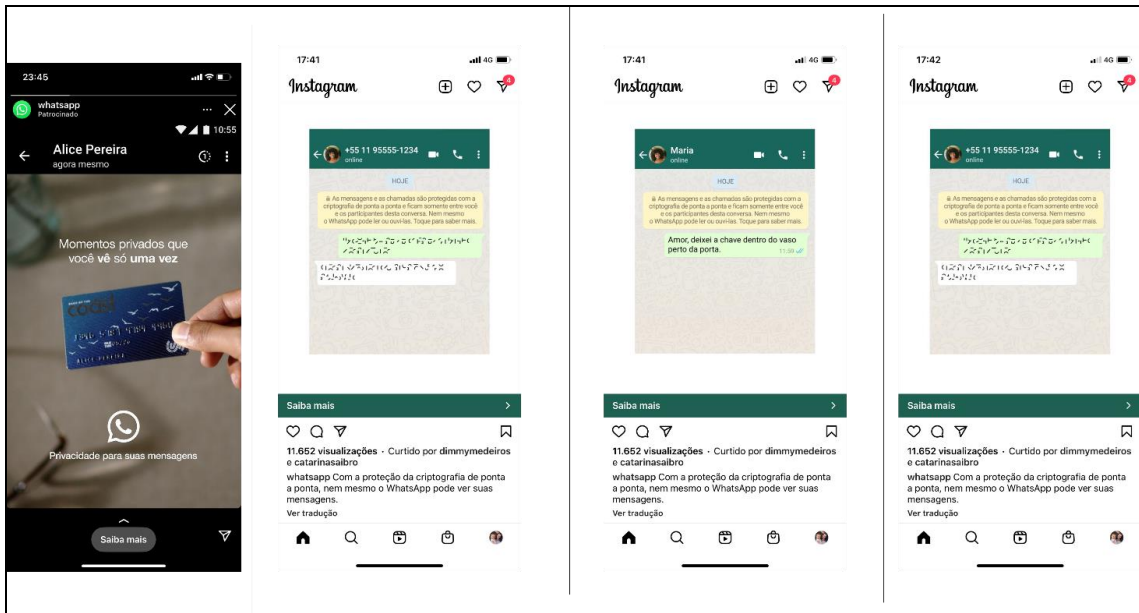
A versão mais recente da campanha, de outubro e dezembro de 2021, conta com filme publicitário e *cards* em formato carrossel, veiculação exclusiva nas redes sociais da Meta, e leva em consideração a preocupação da empresa com a segurança dos dados que circulam em seus aplicativos e plataformas, conforme as imagens a seguir demonstram em capturas realizadas em nosso dispositivo móvel. Vale salientar que a chamada principal do anúncio é *Momentos privados que você vê só uma vez. Privacidade para suas mensagens*. E nos demais *cards* há a simulação de como funcionaria uma mensagem criptografada<sup>30</sup>.

---

<sup>30</sup> O tema da criptografia e sua funcionalidade serão mais bem explorados no item 2.1, onde serão trabalhados os conceitos sobre segurança na e da Comunicação, principalmente pelo trabalho do Prof. PHD Peter Krapp (UC Irvine) (2020b).

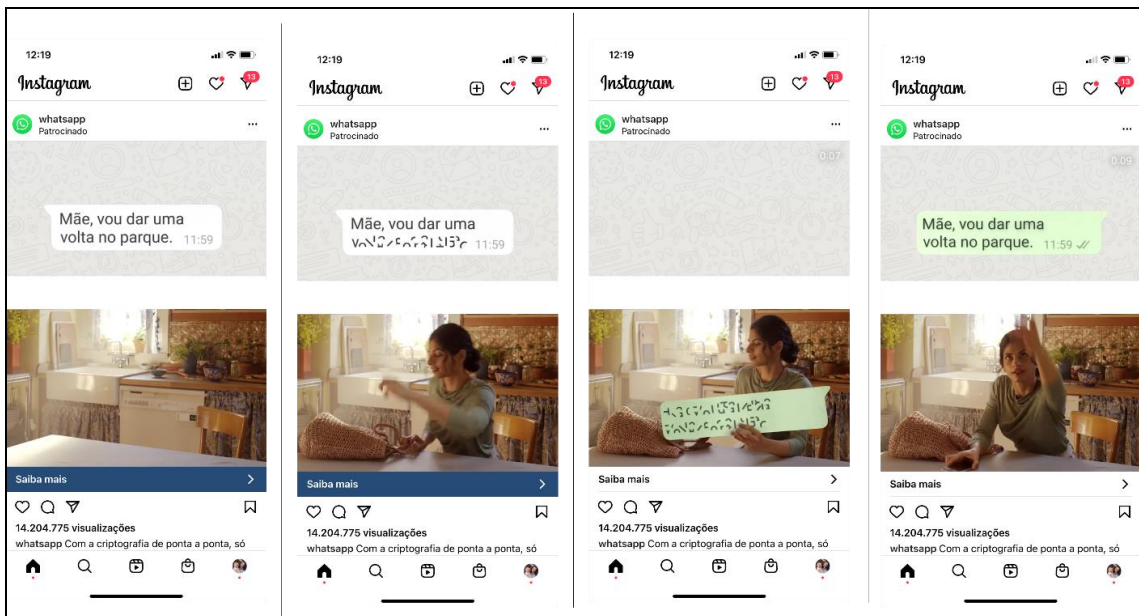


Figura 24 - Captura de tela da campanha publicitária do WhatsApp (out. 2021)



Fonte: Elaborado pela autora (2021).

Figura 25 - Captura de tela da segunda peça da mesma campanha publicitária do WhatsApp (dez. 2021)



Fonte: Elaborado pela autora (2021).

Portanto, ao direcionar nosso olhar para essas manifestações de segurança em diversos espaços midiáticos da contemporaneidade, e como ela está associada a dados, proteção e privacidade, acreditamos ser adequada a apropriação do termo “*imagérie*”, do autor Jacques Rancière (2012), devido à sua característica que remete “a todas as formas de produção e reprodução de imagens, não especificamente às produzidas por ‘equipamento imageador’,

como repertório de imagens disponíveis” (RANCIÈRE, 2012, p. 24). O autor propõe que trabalhar com a imagens, principalmente a partir do viés da arte e do artista, ao criar arranjos, semelhanças e dessemelhanças entre suas associações, nas suas palavras visa “despertar os objetos úteis adormecidos ou as imagens indiferentes da circulação midiática para suscitar o poder dos vestígios de história comum que eles comportam” (RANCIÈRE, 2012, p. 35). Buscamos apoio nas palavras de Pires (2021), quando sintetiza o trabalho de Rancière, dizendo que

Para nós, é onde se encontra a expressão humana, a autoria, não no sentido de posse, mas de marca autoral: reutilização pela montagem. Essas imagens reaproveitadas não voltam intactas, pois são reorganizadas na montagem, reaparecem sob novas formas. Imagens são os objetos de manuseio da artista. Nesse sentido, toda autora é uma bricoleur. Enquanto a imagem bergsoniana é a própria matéria, a imagem da arte rancêriana é a operação no interior da montagem, especificada no termo *imagéité* (PIRES, 2021, p. 30).

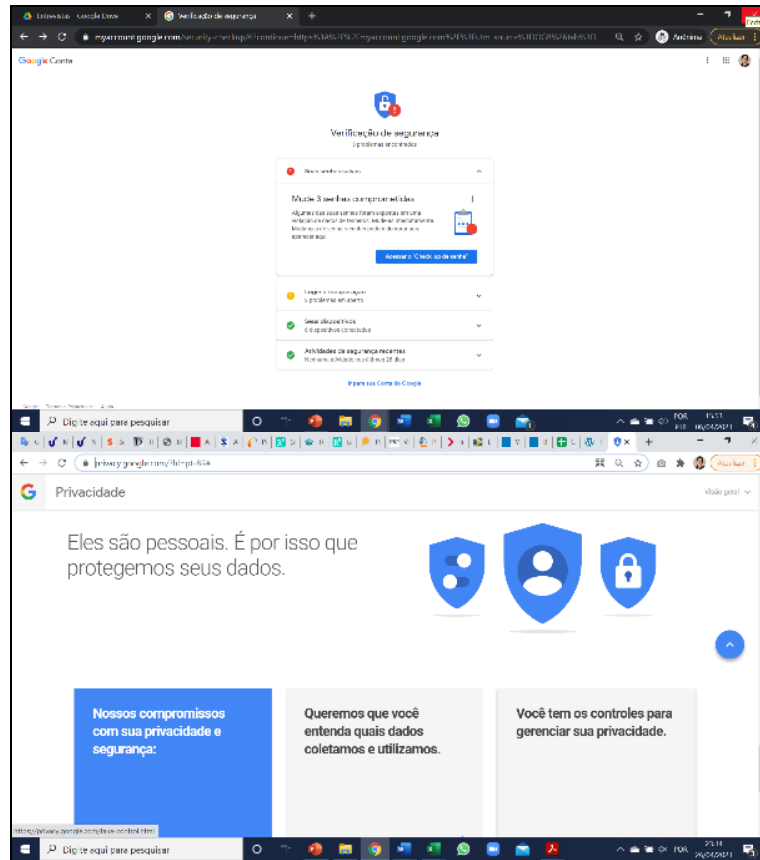
Para o autor, é possível com as imagens, fazer “relações entre um todo e as partes, entre uma visibilidade e uma potência de significação e de afeto que lhe é associada, entre as expectativas e aquilo que vem preenchê-las” (RANCIÈRE, 2012, p. 11). Nesse sentido, ensaiamos uma reflexão sobre as imagens e suas relações como atualizações de construtos de segurança, a partir de imagens técnicas<sup>31</sup> em artigo apresentado do GP Comunicação Digital, no 43º Congresso Brasileiro de Ciências da Comunicação (INTERCOM) em 2020, onde buscamos, com o alicerce do método cartográfico, os serviços de autenticação via FB e Google e sobre os elementos que envolvem *imageria* em torno de comunicação segura e eficiente, nas interfaces culturais, conforme mencionamos brevemente na abertura de nossa tese.

---

<sup>31</sup> Construtos de segurança a partir de suas atualizações em imagens técnicas; apontamentos sobre formas de *login* e serviços autenticadores na *web* (KRAUSE; NESS, 2020).



Figura 26 - Excerto de tela do Gmail sobre verificação de segurança da conta



Fonte: Google (2021).

No artigo publicado, demonstramos que através do movimento de *flânerie* realizado, nos deparamos com iniciativas que dispensam a realização de cadastros, permitindo ao usuário autenticar sua identidade, a partir do *login* social, a quem chamamos de serviços autenticadores. Com base nessas manifestações, observamos um construto de segurança na *tecno cultura*, não apenas baseado em cadeados, escudos e chaves, mas na confiança prometida sobre esses serviços autenticadores na internet.

Figura 27 - Meme circulando no FB sobre proteção de *login* no Gmail



Fonte: Facebook (2021).

Portanto, a partir da construção realizada no presente subcapítulo, que tinha como objetivo apresentar brevemente algumas iniciativas midiáticas que dão sentido à construção de segurança na *tecnocultura*, passamos para o próximo passo que foi realizar o exercício de limitar e especificar, em poucas palavras-chave, o que nos chama a atenção sobre a construção dessa tese para fazer a pesquisa da pesquisa, onde mapeamos, na tentativa de inventariar,<sup>32</sup> trabalhos científicos que abordam perspectivas paralelas ao nosso objeto. Junto a isso, se faz necessário, no processo da pesquisa, “tornar familiar o que é estrangeiro e, ao contrário, estranho o que é familiar” (CANEVACCI, 1997, p. 105), para conseguirmos dar a ver os caminhos ou perspectivas que podem levar a construção de um verdadeiro problema de pesquisa, constatando aqui a perspectiva bergsoniana de construção do misto já apresentado.

A explicação que devemos considerar satisfatória é aquela que adere a seu objeto: nenhum vazio entre eles, nenhum interstício no qual uma outra explicação pudesse alojar-se com a mesma propriedade; ela convém apenas a ele, presta-se apenas a ele. Tal pode ser a explicação científica (BERGSON, 2006a, p. 3).

Portanto, para chegarmos na construção do objeto e conseqüentemente na pergunta norteadora da pesquisa, apresentada previamente, realizamos a busca pelo estado da arte dando ênfase a dois movimentos que foram mutuamente influenciados e nutriram a construção da pesquisa. Partimos para a busca, nas principais plataformas digitais disponíveis,

<sup>32</sup> Iremos aprofundar, no Capítulo 3, o conceito de inventário como técnica de pesquisa a partir de Maciel (2009).

para acesso: Portal Periódicos Capes, Academia.edu, Repositório Jesuíta e Google Acadêmico. Mas, junto a esse exercício, aos poucos fomos ficando cada vez mais alertas a iniciativas das mídias que nos cercam, e que foram mapeadas anteriormente, como redes sociais, televisão e plataformas de *streaming*, expondo diariamente, a partir de produções como campanhas publicitárias e conteúdo de entretenimento, questões relacionadas à segurança, confiança e privacidade de dados de seus usuários inseridos numa ambiência *tecnocultural*.

Então, optamos por registrar todo esse criterioso processo de coleta e reflexão da Pesquisa da Pesquisa, onde inventariamos as principais publicações acadêmicas que circundam nosso tema de trabalho. Nesse sentido, nos identificamos com as palavras de Peter Weibel (2001) ao relacionar aspectos da endofísica, ciência que investiga o surgimento de um sistema quando o observador se torna parte dele, ao fazer uma comparação com a nossa conexão com o mundo e o estudo das interfaces, ou seja, são indissociáveis. Entendemos que neste processo de encontro do tema da pesquisa, nossas tentativas de realizar a busca por algo que nos toca foi sendo extremamente influenciado pelo nosso ambiente, pelos meios, ou melhor, pela realidade também indissociável de nossa sociedade, cujas práticas sociais estão atravessadas por lógicas de operação de mídias.

### 1.3 Estado da arte

Nosso primeiro exercício de pesquisa da pesquisa se deu no momento de preparação para o seminário de tese, conforme relatamos na introdução deste texto, que visava uma problematização e construção de objeto em um contexto anterior. Porém, tendo em vista o recomeço da investigação e o interesse voltado para outras questões que também estão inseridas numa ambiência *tecnocultural*, refizemos o exercício da coleta de produções acadêmicas utilizando uma rota diferente daquela proposta no seminário.

Fomos ao portal de periódicos da Capes<sup>33</sup> e buscamos pela palavra-chave Facebook, nosso objeto empírico, o que resultou em 538.348 resultados filtrados apenas na categoria *Journalism and Communications* até 2021. Para fins de otimizar os resultados, selecionamos a pesquisa desde 2010 até 2022, resultando ainda 513.916 produções, o que nos sinaliza que a grande maioria dos estudos realizados envolvendo nosso objeto empírico se deu nos últimos 11 anos (lembrando que o FB foi lançado em fevereiro de 2004). Vale comentar, também, que realizamos uma busca por publicações mais antigas (sendo a primeira citando a rede social em

---

<sup>33</sup> Maiores informações em <https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php?>

maio de 2004, a partir de um artigo do editor de *The Chronicle of Higher Education*, Brock Read (2004), anunciando sobre um novo *website* que continha várias páginas pessoais dos estudantes de Harvard e pesquisas mais recentes (um estudo da Faculdade de Negócios de Thammasat, Tailândia, utilizando o FB como técnica de coleta de unidade de estudo para a contratação de *personal trainer online*) (CHUPAN, 2018).

Refinamos a busca para artigos (185.385), teses (180), livros (120) e *book chapters* (4), o que totalizou 185.689 resultados. Ao selecionarmos as publicações na língua portuguesa, chegamos em 1.894 trabalhos, e, organizando por publicações brasileiras, chegamos em apenas 20 autores. Essas pesquisas variavam de abordagem, passando por temáticas de negócios utilizando o FB, campanhas eleitorais, questões de gênero, privacidade da saúde, Direito e Psicologia. Nenhum dos resultados trouxe algo sobre segurança ou privacidade das informações, sobre seus usuários ou seu uso a partir das imagens, conforme proposta inicial de tema dessa tese com enfoque ao ponto de vista comunicacional.

Vale salientar que, neste momento de nossa busca, ainda não havíamos definido o que de seguro ou privado estávamos relacionando com a rede social, mas, esses trabalhos foram indicando pistas de que esses aspectos estavam nos inquietando, e, por esse sentido, também foram essenciais para a construção da problematização. Portanto, refizemos a busca pela junção dos termos Facebook + privacidade, mostrando 214 trabalhos desde 2007, e Facebook + segurança, resultando 496 desde 2008. Primeiramente, vamos nos deter na coleta Facebook + privacidade, onde selecionamos pesquisas que abordam aspectos que estão no âmbito das Ciências da Comunicação. O artigo intitulado *Facebook como dispositivo de vigilância e visibilidade: algumas controvérsias em questão*, de Luciana Santos Guilhon Albuquerque e Rosa Maria Leite Ribeiro Pedro (2013), do Programa de Pós-Graduação em Psicologia da Universidade Federal do Rio de Janeiro, versa sobre as controvérsias em torno do FB como dispositivo de vigilância e privacidade, utilizando a Teoria Ator-Rede (TAR) de Bruno Latour, para construir uma rede com notícias de jornal, traçando articulações entre formas de governo e controle, provocando tensões entre a preocupação com a segurança e a defesa da privacidade. As autoras abordam uma análise com foco nos indivíduos com destaque ao monitoramento de seus comportamentos cotidianos. Utilizam perspectivas teóricas calcadas na proposta do panóptico de Michel Foucault, no livro *Vigiar e punir* (1983), e o jogo de poder que se instaura na ordem e controle a partir da vigilância. É interessante que o artigo provoca a ver como

as novas tecnologias de comunicação como o Facebook, põe em cena uma dinâmica de exposição de si, produzindo um desejo de se mostrar publicamente, de abrir sua intimidade, de forma nada coercitiva, mas pelo prazer e a sedução. E como esses dados espontaneamente expostos pelos indivíduos de repente se tornaram interessantes para o governo e usados como peças fundamentais das políticas de segurança (ALBUQUERQUE; PEDRO, 2013, p. 7).

Para as autoras, está claro que por iniciativas governamentais, como por exemplo do governo Obama (BARBOSA, 2013), há ambivalência entre segurança e liberdade, e “é preciso fazer escolhas, ou seja, se a sociedade deseja segurança, precisa abrir mão de alguma privacidade” (ALBUQUERQUE; PEDRO, 2013, p. 7). Nesse sentido, elas relatam, no artigo, casos de coleta e análise de informações de usuários do FB cedidas para o governo com a justificativa de manter sob controle a segurança da população americana. A discussão recai sobre “preservar o direito à privacidade e os princípios democráticos da livre circulação de ideias, embasados na Declaração Universal dos Direitos Humanos” (ALBUQUERQUE; PEDRO, 2013, p. 9), porém, o que as pesquisadoras argumentam no trabalho é o interesse em, de fato, discutir sobre “os efeitos de controle e resistência engendrados no momento em que se supõe que a verdade de cada um pode ser extraída do cruzamento de seus dados mais explícitos (ALBUQUERQUE; PEDRO, 2013, p. 13).

Nesse momento da pesquisa, direcionamos nosso olhar sobre o objeto empírico e iniciamos uma reflexão sobre como a dinâmica da rede social FB, constantemente, estimula a exposição de informações privadas a partir de seus usuários, cedidas facultativamente, tornando-as públicas naquele ambiente *online*, apesar do usuário ter a possibilidade de limitar quais “amigos” de sua rede podem ter acesso ao conteúdo. Albuquerque e Pedro (2013, p. 13) argumentam sobre essa prática afirmando que o FB “nos ajuda a banalizar e naturalizar a exposição de si como prática cotidiana. E cada vez que nos expomos, voluntariamente ou não, fornecemos material para sermos vigiados”.

Distanciando brevemente de nosso objeto empírico, mas de forma complementar à visão sobre vigilância, a partir de dados fornecidos, ou inferidos sobre usuários de redes sociais, encontramos nas referências do mesmo artigo, o trabalho da mesma autora, Rosa Maria Ribeiro Pedro, em coautoria com Fernanda Bruno, ambas professoras e pesquisadoras da Universidade Federal do Rio de Janeiro, e que compõem o Núcleo de Pesquisa em Tecnologias da Comunicação, Cultura e Subjetividade (CIBERIDEA)<sup>34</sup>, vinculado ao

---

<sup>34</sup> Este grupo de pesquisa foi formado em 1998, desenvolvendo pesquisas abarcando os universos das novas tecnologias de comunicação, das transformações cognitivas, das lutas biopolíticas e dos processos culturais de subjetivação. A temática das transformações éticas da sociedade contemporânea, apreendidas através das mediações e dos dispositivos comunicacionais, é o viés que caracteriza o trabalho do grupo. Os resultados destas investigações se repercutem em dissertações, teses, artigos científicos, conferências, palestras e

Conselho Nacional de Desenvolvimento Tecnológico (CNPQ). O artigo sob o título *Entre aparecer e ser: tecnologia, espetáculo e subjetividade contemporânea*, foi publicado 9 anos antes, portanto em 2004, e já dava indicações de pesquisa em Comunicação relacionando a intenção de exposição de intimidade de usuários em blogs e *webcams*, tanto que o artigo busca “problematizar a questão da produção de subjetividade na atualidade, na sua relação com as transformações no estatuto do olhar do outro e no espetáculo” (BRUNO; PEDRO, 2004, p. 1).

O que as autoras chamam por “espetacularização da intimidade”, problematizando a proposta de Guy Debord (1967) sobre a sociedade do espetáculo e sobre a instrumentalização midiática e seu “espraiamento no espaço, na constituição de uma espécie de que opera por irradiação, e no espetáculo integrado tempo, na produção de uma geração que teria se socializado submetida a suas leis” (BRUNO; PEDRO, 2004, p. 10). Nesse sentido, interessa para as autoras analisar as motivações e o impacto social causado pelo hábito de expor conteúdos espontaneamente por pessoas comuns, realizados em suas *webcams*, blogs, e *sites* pessoais, envolvendo o uso da tecnologia; e, para problematizar a subjetividade e os limites entre público e privado, a partir dessas informações, dados e imagens compartilhadas com outros usuários e por plataformas que coletam e analisam dados para fins comerciais e de vigilância.

Dando continuidade aos resultados da busca na ferramenta da Capes, tivemos acesso ao artigo *Monitoramento, classificação e controle nos dispositivos de vigilância digital*, da autoria de Fernanda Bruno (2008). Ela realiza uma reflexão envolvendo a privacidade dos dados de usuários da internet, utilizando como exemplo central o sistema de publicidade divulgado pelo FB chamado Beacon Ads, ferramenta de segmentação de audiência para fins de campanhas comerciais. Em 2007, o FB tornou pública essa informação ao compartilhar informações sobre usuários e seus dados de navegação com seus parceiros comerciais, como o jornal *The New York Times*, por exemplo. O Beacon Ads realiza a análise de comportamento dos usuários com base em seu histórico de navegação, e desenvolve um estudo preditivo do que esses perfis poderiam se interessar, para, assim, estimular o consumo a partir da exibição de publicidade segmentada.

“Chamei estes mecanismos de dispositivo de vigilância digital e analisei os seus elementos centrais seguindo indícios mais ou menos seguros, dado que boa parte das ações deste dispositivo permanece pouco visível e conhecida” (BRUNO, 2008, p. 10). Diante dessa

proposta, a autora realiza uma discussão mais ampla envolvendo processos de monitoramento, coleta, classificação, arquivamento e controle de dados sobre indivíduos, na internet, pela noção de dispositivo de Foucault (1983). Sugerindo um jogo de poder instaurado na vigilância digital, tratando da violação da privacidade como algo relevante, porém, de superfície, ela defende que o foco da discussão deveria estar na problematização dos jogos de controle, saber e poder instaurados nos interesses monetários de empresas privadas.

Permanecendo nos resultados da Capes, ao encontro da problemática proposta por Bruno (2008), o artigo de Grace Quaresma Fugazza (UNIRIO) e Gustavo Silva Saldanha (UFRJ), com o título *A questão do direito à privacidade no Facebook: um estudo à luz da ética da informação*, publicado em 2018 na *Revista Informação*, da Universidade de Londrina, Paraná, traz aspectos relacionados à efetividade do direito à privacidade no ciberespaço. A pesquisa é um estudo de caso, aplicado com um questionário aos usuários da rede social FB, demonstrando que a “personalização de conteúdos operacionalizada pelas empresas digitais em troca da ampla liberdade de acesso aos dados pessoais de seus usuários ameaça os princípios de autonomia e liberdade [...]” (FUGAZZA; SALDANHA, 2018, p. 462), mas reforça que a circulação de dados também corre livre entre os próprios usuários. Os autores se baseiam, fortemente, no pensamento do filósofo uruguaio Rafael Capurro (2013) e nos seus trabalhos relacionados à ética da informação e aspectos interculturais de privacidade em redes sociais *online*.

Intrigados pela proposta de Rafael Capurro (2013), buscamos dois trabalhos publicados pelo autor que tratam especificamente sobre privacidade no ciberespaço, sendo o primeiro de 2005, chamado *Privacidade. Uma perspectiva intercultural*<sup>35,36</sup>, onde ele aborda as diferenças sobre os conceitos de privacidade nas culturas japonesas e ocidentais, mas, especificamente, no item 5 do artigo, o autor trata sobre privacidade no ciberespaço, questionando se somos mestres da nossa própria casa, argumentando que há uma linha tênue entre as esferas públicas e privadas na ambiência da “infosfera”, principalmente tratando do objeto empírico de sua pesquisa, os *weblogs*, já que esses diários, na *web*, revelam aspectos privados da vida de quem espontaneamente produz esses conteúdos e opta por compartilhar na internet, tornando-os públicos.

O segundo trabalho, que identificamos como relevante para nossa pesquisa da pesquisa, também de Rafael Capurro, é de 2013, intitulado *Questões éticas das redes sociais*

---

<sup>35</sup> Os títulos foram traduzidos para um melhor entendimento do leitor.

<sup>36</sup> “An Intercultural Perspective. Ethics and Information Technology.”

*on-line na África*<sup>37</sup>, mais especificamente, quando aborda a privacidade em redes sociais, sendo necessário entender o que ocultamos e o que exibimos, o que tornamos público em nossas redes sociais *online*, reside no tema da liberdade humana.

Se, então, olhar para o atual mundo digital globalizado ou ciber mundo, não é difícil ver que em tal mundo, que não é apenas cibernético espaço, isto é, nós mesmos, somos representados como algo por cadeias de bits. Com base em tais eus reificados como cadeias de bits, novas formas de interação para o reconhecimento individual e social são possibilitadas, tendo impacto não apenas sobre quem somos, mas também sobre o que somos capazes de produzir e valorizar tanto no físico quanto no digital<sup>38</sup> (CAPURRO, 2013, p. 167, tradução nossa).

Esse impacto produz um efeito relevante na sociedade, pois acabamos sendo instruídos por modelos de comportamentos que não necessariamente retratam a realidade daquele indivíduo. “Aquilo com que nos importamos, como indivíduos e como comunidades, surge dentro do horizonte de cuidado por um mundo divulgado compartilhado” (CAPURRO, 2013, p. 168), ou seja, há inversão sobre aquilo que nos importamos e que caracteriza o cuidado dentro de uma comunidade. Identificamos, no trabalho de Capurro (2013), potencialidade para enriquecer a discussão sobre a construção de comunidade dentro de nosso objeto empírico, proposta também articulada com o conceito de Bauman (2003), sobre haver uma construção da sensação de conforto e aconchego nas interfaces do FB.

Para encerrar o levantamento das pesquisas a partir da busca por Facebook + Privacidade, no portal da Capes, encontramos o artigo *Os conceitos de público e privado nas redes sociais e suas implicações pedagógicas* (2014), de Ana Maciel de Quadros e Karina Marcon (ambas atuam na educação à distância, da UNISINOS e UDESC, respectivamente), tratando sobre implicações pedagógicas, relacionando o conceito de privacidade e publicização de sujeitos no FB. Com relação aos conceitos de Bauman (2001) sobre a sociedade líquida, elas comentam que há um “[...] borramento entre as fronteiras de público e privado e ocorrem principalmente pela enxurrada de manifestações privadas na esfera pública” (QUADROS; MARCON, 2014, p. 72), ou seja, a mistura de informações sobre o cotidiano de usuários do FB tornando-se públicas, a partir das suas publicações na rede social, proposta que vai ao encontro de Capurro (2013), conforme apresentado anteriormente.

---

<sup>37</sup> “Ethical Issues on online social networks in Africa.”

<sup>38</sup> “If we then look at the present-day digitally globalized world or cyberworld, it is not difficult to see that in such a world, which is not just cyberspace, we, that is to say, our selves, are represented as somewhats by bit-strings. On the basis of such selves reified as bit-strings, new forms of interplay for individual and social recognition are enabled, having impact not only on who we are, but also on what we are able to produce and value in both the physical and digital worlds.”



Em nosso último movimento na busca por trabalhos acadêmicos relacionados ao objeto empírico, FB, associado à palavra-chave segurança, no portal da Capes, nos indicou apenas três pesquisas (do total já mencionado anteriormente de 496 resultados), que problematizam o FB e segurança. A pesquisa de Christian Luis Schaeffer (2016), publicada na *Revista Foco - Interdisciplinary Studies*, de Curitiba, sob o título *Monitoramento de mídias sociais no processo de análise de percepção dos usuários sobre a segurança de Porto Alegre*, realiza a análise de conteúdo sobre como os moradores de POA percebem a segurança pública da cidade, a partir de comentários e publicações dentro do FB, relacionadas à criminalidade e violência.

Já o artigo de Carlos Cesar Santos e Jefferson David de Araújo Sales, da Universidade Federal de Sergipe, com o título *O desafio da privacidade na internet das coisas* (2015), traz o debate acerca da coleta e análise de dados de usuários de dispositivos conectados em rede, a partir do conceito de *Internet of Things* (IoT), explorando possibilidades legais para a extração e limite de uso dessas informações. É importante salientar, que nesse estudo, a palavra segurança vem sempre relacionada à segurança da informação, e relaciona não somente ao uso em *sites* de redes sociais, mas abre o leque da discussão para qualquer dispositivo que tenha conexão com internet e que seja capaz de recolher dados sobre usuários. Nesse sentido, privacidade e vigilância fazem parte dos riscos sociais e éticos relacionados à IoT; e os autores abordam, ainda, nas considerações finais deste trabalho, a necessidade de refletir sobre novas regulamentações para poder dar conta das possibilidades de extração e exploração de dados pela IoT.

Por fim, a última pesquisa da base de dados da Capes indica o artigo *Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais*, de autoria de Fabrício Assumpção, Ricardo Santana e Plácida Santos, da Universidade Estadual Paulista, de 2015. A pesquisa trata como as redes sociais FB e Instagram coletam dados de seus usuários por meio de imagens cedidas por eles durante o uso das redes, e como suas políticas de uso de dados abordam esse aspecto em seus termos, sendo bastante vagos sobre o que, de fato, é coletado e onde está esse material, não sendo possível o usuário ter acesso ao conteúdo coletado/armazenado sobre ele pelas plataformas.

Nosso próximo passo, para fazer a pesquisa da pesquisa, foi em Academia.edu<sup>39</sup>, onde encontramos 19 trabalhos de autores estrangeiros na busca pelos termos *security + facebook*. Fizemos a busca pelo termo em Língua Portuguesa que resultou no mesmo trabalho já citado

---

<sup>39</sup> Maiores informações em <https://www.academia.edu/>.

nos termos em inglês. Os resultados não abordam aspectos relacionados às Ciências da Comunicação, mas, estão muito relacionados à Tecnologia, Engenharia e Direito, com interesse especial na regulamentação sobre vigilância e monitoramento de dados de usuários no FB. Nesse sentido, buscamos, dentro do *site* Academia.edu, as pesquisas do Prof. Dr. Göran Bolin, da Universidade de Södertörn, Suécia, que tivemos contato em 2020 durante o *Seminário Internacional em Midiatização* promovido pela UNISINOS. No artigo intitulado *Vigilância através da mídia, pela mídia, na mídia*<sup>40</sup> (2018, tradução nossa), escrito em coautoria com Anne Jerslev (Universidade de Copenhague), eles fazem uma análise desde o dispositivo panóptico, de Foucault (1983), relacionando-a com a maneira como as mídias – cinema, televisão e as digitais –, caracterizam a vigilância através da falsa noção de segurança. “A partir dessa caracterização da vigilância como enunciação em filmes recentes, diferentes gêneros dentro do entretenimento de TV, em particular reality shows, usaram a vigilância panóptica como um tropo estruturante”<sup>41</sup> (BOLIN; JERSLEV, 2018, p. 12, tradução nossa).

Este artigo introdutório tem como objetivo mapear o principal terreno da vigilância por meio, pela e na mídia. Primeiro, discutimos o fenômeno e o trabalho acadêmico sobre a vigilância por meio e pela mídia, levando em consideração a vigilância estatal e corporativa e como essas atividades cresceram com as novas mídias digitais e pessoais de hoje. Em seguida, discutimos a vigilância como o fenômeno é representado na mídia e como as representações se relacionam com as práticas de vigilância<sup>42</sup> (BOLIN; JERSLEV, 2018, p. 3, tradução nossa).

A pesquisa do Prof. Göran Bolin (2018) nos deu importante suporte para direcionar nosso pensamento ao redor das mídias e a construção do imaginário de segurança e privacidade construída nos meios. Havíamos ensaiado uma primeira proposta de reflexão sobre o papel das imagens nessa construção de comunicação segura, e, conseqüentemente, que promete o respeito pela privacidade dos usuários dentro de uma mídia digital, no artigo submetido ao GP Comunicação e Cultura Digital do Congresso Brasileiro em Ciências da Comunicação em 2020. Esse tema será mais bem explorado no item 2.2 *Tecnosegurança*.

---

<sup>40</sup> “Surveillance through media, by media, in media.”

<sup>41</sup> “Following from this characterization of surveillance as enunciation in recent films, different genres within TV entertainment, in particular reality TV, have used panoptic surveillance as a structuring trope.”

<sup>42</sup> “Following the spread of digital media, the interdisciplinary field of surveillance studies has gained prominence, engaging scholars from the humanities and the social sciences alike. This introductory article aims to map out the main terrain of surveillance through, by and in the media. First, we discuss the phenomenon of, and the scholarly work on, surveillance through and by media, taking into consideration both state and corporate surveillance and how these activities have grown with the new digital and personal media of today. We then discuss surveillance as the phenomenon is represented in the media and how representations relate to surveillance practices. We conclude by presenting the articles of this special issue.”

Ainda, usufruindo do *site* Academia.edu e constantemente dos eventos acadêmicos promovidos pela UNISINOS, durante o encontro *Histories of AI*, em abril de 2021 – iniciativa do Digilabour<sup>43</sup> – laboratório de pesquisa, coordenado pelo Prof. Dr. Rafael Grohman, tivemos contato com o pesquisador Gabriel Pereira da Universidade de Aarhus, Dinamarca. Seus principais interesses circundam inteligência artificial, uso de dados e tecnologia, e por intermédio de seu trabalho de revisão da obra de Anthony McCosker e Rowan Wilken (2020, tradução nossa), *Visão automatizada: o impacto social da nova consciência da câmera*<sup>44</sup>, que mencionamos previamente. Refletimos sobre o impacto da visão das câmeras em nossas vidas, sejam câmeras de vigilância para fins de segurança pública, *webcams*, câmeras de *smartphones*, sistemas de reconhecimento facial, *drones*, carros com direção automática, etc. Essa abordagem da resenha realizada por Pereira (2021) reforça a necessidade de explorarmos, no capítulo seguinte, o impacto da questão da segurança digital, a partir de duas frentes que identificamos até o momento: a proteção da circulação de dados de usuários na internet e o viés da captação e monitoramento de imagens de indivíduos em livre circulação nas ruas.

Para encerrar a pesquisa da pesquisa e desde sempre valorizando a relevância dos trabalhos realizados por colegas discentes e professores da UNISINOS, selecionamos produções que abordam especificamente o FB como objeto empírico, mas, também, aquelas que desenvolvem reflexão acerca da *tecnocultura* e das audiovisualidades, chave inicial que desperta nosso interesse pelo trabalho científico por meio de nosso objeto empírico, e, ainda, pesquisas que orbitam em áreas adjacentes ao conceito de privacidade e segurança de dados na internet. A nossa coleta se deu por indicações de colegas do PPGCC e por trabalhos desenvolvidos em nossa linha de pesquisa, *Mídias e Processos Audiovisuais*, discussões enriquecidas no grupo de pesquisa TCAv, reflexões e leituras coletivas a partir de encontros do Laboratório do Audiovisual em Rede (LAR), iniciativas provocadas pelo Laboratório de Memória das/nas Mídias Online (LabMem), participação como ouvinte em bancas de defesa e qualificação de mestrado e doutorado, e por um levantamento no repositório jesuíta, ferramenta do sistema digital da biblioteca da universidade que carrega em sua memória o acervo de produções acadêmicas da UNISINOS.

Na Linha 1, na qual estamos inseridos em nosso PPGCC, *Mídias e Processos Audiovisuais*, há duas teses que apresentam recorte como *corpus* da pesquisa o FB, sendo a primeira defendida por William Mayer e tem o título *Audiovisualidades e construtos de*

<sup>43</sup> Maiores informações no endereço <https://digilabour.com.br/quemsomos/>.

<sup>44</sup> “Automating vision: The social impact of the new camera consciousness.”

*movimento nas imagens e imagéités do Facebook* (2019), sob orientação da Profa. Dra. Suzana Kilpp, e, a segunda tese, é de autoria de Lorena de Risse Ferreira: *A efemeridade na tecnocultura: escavações em aplicativos de imagens feitas para sumir* (2019), orientada do Prof. Dr. Gustavo Daudt Fischer. Em ambas as pesquisas os autores carregam uma atualização sobre o fenômeno do *software* na nossa cultura, compreendendo a necessidade de debater questões relacionadas à percepção enquanto usuários de dispositivos e tecnologias que habitam nossa rotina, e como pesquisadores, que tensionam, refletem, debatem e propõem perspectivas ao olhar (e se deixar ser olhado) por fenômenos que ali são enunciados.

Mayer (2019) buscou compreender como a construção de movimento no FB é capaz de produzir imagens e *imagéités* próprias, caracterizando uma audiovisualidade durante própria desse ambiente. Por um mapeamento de diferentes interfaces da rede social, o autor deu a ver a ilusão de “movimento” construída no FB, ou melhor “construto de movimento que busca simular uma experiência do imaginário” (MAYER, 2019, p. 184), com base nos comentários de usuários que seriam *imagéités* do FB (por exemplo), e que fogem do controle do algoritmo, possibilitando a troca de mensagens entre os indivíduos. Para Mayer (2019, p. 186), “o exercício de construção de movimento entre um usuário e outro é certamente parte desta audiovisualização da cultura que demanda que estejamos em movimento”. A tese defende a proposta de que o FB produz construtos de movimento, ou melhor, atualiza a ilusão de imagem-movimento, gerando um fluxo de dados, ou *data stream*, responsável por caracterizar uma experiência sem cortes (muito inspirada no cinema), e totalmente prevista pelos algoritmos. Tanto que qualquer ação que o usuário deseje realizar dentro da rede social já foi programada pelo *software*, representando a ação e reação do usuário ao algoritmo.

Já a tese de Lorena de Risse Ferreira (2019), trata sobre a efemeridade enquanto qualidade *tecnocultural* que se atualiza em imagens de aplicativos como FB, Instagram e Snapchat. Apoiada no método intuitivo de Bergson (2006a), a autora realiza uma cartografia pelos aplicativos em movimento, também influenciada no olhar da arqueologia da mídia, escavando os dispositivos, propondo constelações com base em suas descobertas. Ao final da tese ela sugere propostas conceituais para a imagem efêmera, podendo se manifestar a partir da imagem-fluxo e de imagens-espectação. Também nos chama a atenção, na proposta de Ferreira (2019), o modo pelo qual ela se apropriou das telas que compõem o *corpus*, indicando zonas próprias dos aplicativos que têm sua função identitária, funcionando como molduras limite, ou áreas fixas no fluxo desses territórios.

Há outras 14 pesquisas desenvolvidas no PPGCC da UNISINOS que, de alguma maneira, lidam com o FB como *corpus*, mas pertencentes às demais linhas de pesquisa do

programa, passando por análise de usuários pertencentes a grupos específicos do FB, eleitores no FB, construções de cidadania dentro do FB, abordagens religiosas em usuários do FB e *fanpages* do FB. Avançando nas pesquisas dentro da universidade UNISINOS, mas que não foram desenvolvidas dentro do Programa de Pós-Graduação em Ciências da Comunicação, mas, que de certa forma, tratam a relação com privacidade ou segurança através de dados, estão os trabalhos que transitam pelas Ciências Jurídicas, como o de Ana Paula Jacobus Pezzi (2007), *A necessidade de proteção de dados pessoais nos arquivos de consumo: em busca da concretização do direito à privacidade*, e a dissertação de Patrícia Maino (2010), *Faces da Visibilidade: a tensão entre publicidade e privacidade*, mas nenhuma delas aborda redes sociais.

Por fim, nos direcionando para uma área adjacente à privacidade e segurança na *web* e nos dispositivos conectados à internet, chegamos na questão do uso de dados pessoais coletados a partir das políticas de segurança e privacidade em aplicativos e *sites* na internet. Buscamos por abordagens paralelas e, talvez, complementares à noção de segurança e privacidade em redes sociais, que tratam da questão da vigilância de dados, e encontramos, no repositório digital da UNISINOS, no PPGCC, a dissertação de Julia Dreher Pacheco da Silva (2017), orientanda da Prof. Dra. Adriana Amaral, sob o título *Internet como dispositivo de vigilância: um estudo sobre geração Y e suas adequações*, no mesmo sentido, e na tese de Vinícius dos Santos Flôres (2021), *Vigiar e compartilhar: marcas da violência armada nas redes digitais do Fogo Cruzado*. A pesquisa de Flôres (2021) reflete sobre os processos midiáticos e os atravessamentos de vigilância na sociedade, a partir de dispositivos técnicos e mídias locativas, viabilizando uma nova forma de controle social, como o laboratório de dados Fogo Cruzado, no Rio de Janeiro e Recife.

Portanto, buscamos realizar aqui uma breve coleção de pesquisas científicas que abordam, a partir de suas especificidades, nosso objeto empírico, mas também alguns aspectos que orbitam a construção do tema de nosso trabalho, como aqueles relacionados à privacidade e à segurança, com base nos dados coletados por meio de dispositivos conectados à internet. Esse exercício de busca pela pesquisa da pesquisa foi bastante extenso e demandou algum critério nosso de escolha para exclusão e seleção do que poderia fazer parte da tese. Esse movimento exigiu um certo deslocamento nosso por renunciar a algumas pesquisas e optar por outras que, nesse momento, parecem provocar mais a nossa reflexão acerca da construção do objeto, e, nos inspiramos na obra de Maria Esther Maciel (2009, p. 16), *As ironias da ordem: coleções, inventários e enciclopédias ficcionais*, para nos deixar selecionar as pesquisas tendo como ponto de partida um julgamento nosso,

Assim, as categorias duram apenas até que, pela força das exceções, das diferenças e das descobertas, tenham que ser revistas e modificadas a partir de novos critérios e divisões. Logo que uma ordem se impõe, ela tente a caducar, como bem demonstrou Perec. Isso graças, sobretudo, ao que é inclassificável (MACIEL, 2009, p. 16).

Portanto, selecionamos as pesquisas que, de certa forma, tiveram maior participação na construção de nosso olhar ao objeto. Buscamos demonstrar pela coleta um sentido de construção, não evolucionista, mas de muitas idas e vindas, recomeços, quedas e levantadas, de como nosso objeto de investigação foi sendo construído, num contágio de olhar a empiria e, conseqüentemente, perceber no estado da arte como determinados aspectos foram nos provocando.

Portanto, para dar continuidade ao texto e apresentarmos ao leitor(a) a estrutura que forma a construção dessa tese, no Capítulo 2, denominado como *(Tecno)segurança contemporânea*, estamos nos dedicando à discussão sobre as lentes teóricas que nos auxiliam a refletir sobre o objeto. Nossa observação apresenta um percurso que carrega suporte de autores da comunicação mais recentes e àqueles que auxiliam a fundamentar a área. Nesse sentido, optamos por subdividir o capítulo em duas etapas, a primeira, 2.1 *Construtos tecnoculturais de segurança e privacidade*, se propõe a pensar sobre *tecnocultura* e seus autores fundamentais. No subcapítulo seguinte, 2.2 *Tecnosegurança*, nos dedicamos à construção de segurança orbitando o tema das mídias, da relação com as imagens e com o universo *cyber*.

No terceiro capítulo, apresentamos a metodologia e nosso itinerário que é um contágio de diversas iniciativas que utilizamos para manusear o objeto. A primeira parte do capítulo justamente demonstra quais são essas referências que nos auxiliam a responder o questionamento de pesquisa, passando por movimentos inspirados no *flâneur*, no(a) trapeiro(a), colecionador(a), escavador(a), dissecador(a), que intui sobre o objeto e desenvolve uma cartografia dando a ver um mapa de estrelas, ou constelações. No segundo subcapítulo, demonstramos como fomos nos aproximando da empiria, situando o *corpus* pela *tecnosegurança* contemporânea.

No Capítulo 4, demonstramos como fizemos nossas inferências sobre o objeto, ou seja, apresentamos as três constelações, subdivididas em suas respectivas coleções de imagens que dão a ver as *ethicidades* que nos levam a compreensão das molduras e moldurações enunciadas em nossos exercícios de dissecação das interfaces coletadas. São três constelações, a primeira chamamos por Confiança Programada, que contém 2 coleções de imagens de capturas de interfaces do FB, sendo elas: Coleção Infância e Coleção Guardião de Memórias. Já a segunda constelação, denominada Usuário Vulnerável, é composta por três coleções de

imagens coletadas, Sujeito Inseguro e Lógica Suspeita, *Tecnoinsegurança* e Políticas de Pergaminho. Por fim, a última constelação estamos chamando por Ambiência da *Tecnosegurança* Contemporânea, onde há 2 coleções de imagens: Medo e Vigilância; e Serviços Autenticadores.

Nas Considerações Finais organizamos uma reflexão acerca do que acreditamos ser os principais pontos de contribuição da pesquisa para a área da Comunicação na “era da privacidade”<sup>45</sup>, além de alertar para os desafios que encontramos ao longo do desenvolvimento da nossa tese, assim como suas limitações e sugestões de encaminhamentos futuros a partir de nossos achados. Para finalizar, apresentamos as referências acadêmicas e documentais que foram essenciais para a construção do pensamento aqui materializado.

Acolhemos o(a) leitor(a) e convidamos a acompanhar, nas páginas seguintes, o debate sobre os sentidos durante de *tecnosegurança* contemporânea pela ambiência FB, com o carinho, entusiasmo e uma certa *insegurança*, num misto de sentimentos que nos acompanhou durante os últimos quatro anos e meio de pesquisa.

---

<sup>45</sup> Termo utilizado pela empresa Google, em artigo publicado em agosto de 2022, alertando sobre como o mercado da comunicação irá se readequar ao fim do uso de *cookies* de terceiros a partir de 2023, priorizando a defesa dos dados dos usuários com maior proteção. Devido ao impacto dessa alteração no mercado da comunicação, consumo e tecnologia, a empresa sugere três pontos centrais que caracterizam esse movimento, sendo eles: construir relacionamentos significativos e transparentes com os usuários, gerando dados proprietários em todos os pontos de contato (*on* e *off*); mensurar a eficácia da nova estratégia preenchendo as necessidades de mensuração com soluções que respeitam a privacidade dos usuários; e ativar experiências relevantes e personalizadas: mostrar aos consumidores a vantagem de se relacionar com a marca (GOOGLE, 2022).

## 2 (TECNO)SEGURANÇA CONTEMPORÂNEA

O presente capítulo é dedicado à discussão teórica que dá sustentação aos conceitos centrais que fazem parte da construção dessa tese, passando por autores que debatem temas mais contemporâneos da pesquisa em Comunicação, como *tecnocultura* e o uso de dados para construção de informação, até propostas que dão “origem”, ou melhor, atualizam nosso pensamento, entre elas, as influências mcluhanianas, benjaminianas e bergsonianas. Para organizar a apresentação de nosso percurso imersivo nos eixos teóricos que julgamos fundamentais e que foram, aos poucos, sendo demandados pelo próprio objeto, para incitar ver o que nos olha nas interfaces do FB, estruturamos o capítulo em dois momentos. O primeiro subcapítulo é dedicado à reflexão sobre *tecnocultura* e as audiovisualidades, à apresentação da proposta, a partir de autores fundantes, para chegar ao uso de dados e à construção de segurança na nossa sociedade. E, no subcapítulo seguinte, vamos tratar sobre as mídias e a segurança, e como diversas iniciativas, desde o capitalismo de vigilância até a estrutura da LGPD, sigilo nas comunicações e o conceito de *privacy by design*, são aspectos relevantes para refletir sobre os objetos midiáticos dentro da *tecnocultura* em que estamos inseridos.

### 2.1 Construtos tecnoculturais de segurança e privacidade

Dar início à reflexão sobre *tecnocultura* implica compreendermos que o conceito não está exclusivamente relacionado ao uso da técnica como dimensão cultural, mas, justamente, perceber que a *tecnocultura* na qual vivemos é resultante do vínculo indissociável entre as ferramentas, os dispositivos e as pessoas. Contudo, nossa visão parte da afirmação de Debra Shaw (2008, p. 1, tradução nossa), na obra intitulada *Technoculture. The key concepts*, ao dizer que “quando falamos sobre tecnologia, estamos nos referindo ao conjunto de ferramentas ou ‘técnicas’ que atendem aos requisitos de qualquer cultura”<sup>1</sup>, e, por este motivo, atualmente há certa devoção por profissionais tidos como *experts* capazes de lidar e recriar a tecnologia, como engenheiros, designers, programadores, e que, de certa forma, reflete na sociedade como um todo, a partir de uma valorização econômica e social sobre aqueles que “dominam” a técnica. Complementarmente às ideias de Shaw (2008), Gustavo Fischer (2013, p. 41) faz a relação da *tecnocultura* com diversas angulações, algumas explicitadas por ele

---

<sup>1</sup> “When we speak about technology, we are referring to the set of tools or ‘techniques’ that serve the requirements of any given culture.”



criticamente como geralmente “associadas ao tensionamento entre fenômenos estritamente oriundos da tecnologia informática e seus ‘impactos’ ou ‘potência’ no tecido sociocultural”, trazendo, então, uma proposta de abordagem ao discutir o conceito aliado à perspectiva das audiovisualidades como substância da cultura, impactada pela importância crescente do *design* em seu devir.

É justamente a partir da proposição de Fischer que compreendemos a necessidade do debate ao ver nosso objeto, pois está relacionada às pesquisas desenvolvidas junto ao Grupo Audiovisualidades, *Tecnocultura*, Comunicação, Memória e Design (TCAv)<sup>2</sup>, que encara a construção das audiovisualidades como potência, virtualidade que se atualiza em diversos formatos e perspectivas com sentidos audiovisuais. Essa proposta traz a Intuição como método proposto por Henri Bergson (2006a) (que já falamos anteriormente na problematização do objeto), havendo um misto de virtual (memória e tempo) x atual (espaço e matéria), caracterizando que as coisas possuem dois modos: o de ser e o de agir.

De maneira complementar, Fischer (2013, p. 43) informa que, a partir dessa proposta, pretende-se evidenciar “uma angulação de pesquisa que se apresenta interessada nas materialidades midiáticas, pensadas em suas técnicas e estéticas, mas como substâncias da cultura”. Reforçando a ideia, Debra Shaw (2008, p. 4, tradução nossa) complementa a construção dos aspectos sociais e tecnológicos e seu entrelaçamento na nossa cultura ao dizer que “podemos, portanto, descrever o estudo da *tecnocultura* como uma investigação sobre a relação entre tecnologia e cultura e a expressão dessa relação em padrões de vida social, estruturas econômicas, política, arte, literatura e cultura popular”<sup>3</sup>.

Portanto, a partir da crítica dos autores citados, não se trata de cairmos no reducionismo ao ver apenas a soma de **tecnologia** (técnica) + **cultura** = *tecnocultura*, mas compreendermos que o imbricamento entre esses dois aspectos possui um impacto constitutivo nas nossas vidas, que logicamente transcende o limite das duas palavras, e amplia o horizonte para problematizar aspectos sobre nossa maneira de experienciar a técnica e a estética na vida cotidiana, conseqüentemente, impactando a sociedade. Também vale ressaltar que a proposta não se limita à discussão sobre tecnologias digitais, mas uma perspectiva calcada nas entranhas do desenvolvimento da técnica e seu impacto na cultura, conforme traçado por Marshall McLuhan, em 1964, onde podemos ver pistas de um sentido *tecnocultural*:

---

<sup>2</sup> Conforme já apresentamos na introdução desse texto a nossa relação com o GP TCAv.

<sup>3</sup> “We can therefore describe the study of technoculture as an enquiry into the relationship between technology and culture and the expression of that relationship in patterns of social life, economic structures, politics, art, literature and popular culture.”

Numa cultura como a nossa, há muito acostumada a dividir e estilhaçar todas as coisas como meio de controlá-las, não deixa, às vezes, de ser um tanto chocante lembrar que, para efeitos práticos e operacionais, o meio é a mensagem. Isto apenas significa que as consequências sociais e pessoais de qualquer meio – ou seja, de qualquer uma das extensões de nós mesmos – constituem o resultado do novo estalão introduzidos em nossas vidas por uma nova tecnologia ou extensão de nós mesmos (MCLUHAN, 1964, p. 21).

Dessa maneira, implica compreendermos o impacto da nossa própria construção da técnica, extensão de nós mesmos, em reestruturarmos nossas vidas, não apenas aos *media*, mas, também, à essência da tecnologia em atividades rotineiras, como trabalho, consumo, deslocamento, alimentação, etc., ou seja, “estamos aqui nos referindo, contudo, às consequências psicológicas e sociais dos desenhos e padrões, na medida em que ampliam ou aceleram os processos já existentes” (MCLUHAN, 1964, p. 22). É por esse viés que Fischer (2013, p. 49) designa McLuhan como um “autenticador de tecnoculturas ao afirmar que qualquer novo meio tecnológico introduz mudanças de escala, velocidade e padrão nas atividades humanas”. Ao identificar o papel da técnica como essencial para construção de rupturas culturais, McLuhan (1964, p. 27) designa ao cinema o papel de meio responsável por apresentar uma nova forma de pensamento à civilização ocidental ao trazer a possibilidade da “transição da sucessão linear para a configuração, portanto trazendo o que à época da publicação de sua obra na década de 1960, retrata sobre o papel da tecnologia ‘se funciona, então é obsoleto’”. De maneira complementar, Tiago Lopes (2014, p. 24), em sua tese de doutorado, defendida na linha de pesquisa Mídias e Processos Audiovisuais, no PPGCC UNISINOS, propõe como **ambiência tecnocultural** o conceito que carrega uma compreensão associada a um quadro maior dos fenômenos, como

Analisá-los no nível das redes de relações que estabelecem com distintas formas culturais, sejam elas reconhecidamente audiovisuais, como a TV e o cinema, ou outras que tangenciam o campo expandido do audiovisual, como a arquitetura, escultura, as instalações e artes performáticas.

Complementar à reflexão de Lopes (2014), é possível ampliar a relação do papel da tecnologia com as maneiras como percebemos o mundo, e, justamente nesse ponto, é que Debra Shaw (2008, p. 4, tradução nossa) atenta ao impacto especificamente na cultura visual, que designa ser

[...] atualmente um importante campo de estudo acadêmico, não só porque o cinema e a televisão são onipresentes, mas porque reconhecemos que qualquer diagnóstico de condições contemporâneas deve levar em consideração a ampla influência dessas tecnologias e seus efeitos em todos os outros aspectos da cultura, incluindo a

maneira como nos experienciamos e o que isso implica para a estrutura das sociedades.<sup>4</sup>

Nesse sentido, é possível compreendermos que, ao observarmos os objetos culturais, como os audiovisuais que estamos em busca de suas audiovisualidades durante, migram por diversos dispositivos, meios e formatos. Esse aspecto modular é articulado por Lev Manovich (2001) quando aborda princípios que poderiam, de certa forma, caracterizar as “novas mídias”, dando a elas uma espécie de possibilidade de encaixe e adaptabilidade característicos do *software* da *web*, por exemplo. É nesse ponto que resgatamos aspectos da *tecnocultura* para refletir e tentar explicar fenômenos que envolvem nossos objetos, como dizem Suzana Kilpp e Sonia Montañó (2015, p. 8), ao inclinarem o pensamento sobre a relação das audiovisualidades, *tecnocultura* e as imagens,

Enquanto se canibaliza imagens produzidas pelas mídias, e as provindas de outras áreas e produzidas por outros saberes e finalidades, e se dispõe ao consumo quaisquer umas dessas imagens, por fim situadas na interseção de campos, tecnologias e suportes, verifica-se haver uma grande diversidade de sujeitos-usuários envolvidos no processo de sua produção e compartilhamento.

O tema que pretendemos trabalhar, sentidos de *tecnosegurança* produzidos pela ambiência FB, está extremamente imbricado no conceito de *tecnocultura* e dos autores que dissertam sobre o assunto, ao explorarem conjuntamente as imagens, mídias, a “softwarização” da cultura e a construção de segurança orbitando esses aspectos. Nessa direção, nosso objeto de pesquisa está inserido no ambiente da *web* e, portanto, passamos a encará-la como um meio que *remidia*<sup>5</sup> diversas outras mídias, num debate aliado ao conceito de ambiência *tecnocultural* e à relação do computador com as novas mídias. Essa característica de contágio das mídias e entre as mídias impacta nossa cultura e, conseqüentemente, a maneira como consumimos os dispositivos e *softwares*, a partir de suas possibilidades de usos e apropriações. A afirmação de Bolter e Grusin (1999) nos leva ao encontro das “raízes” *tecnoculturais* de McLuhan (1964, p. 22), ao propor que o que “dura” em um meio é justamente outro meio, “este fato característico de todos os veículos, significa que o ‘conteúdo’ de qualquer meio ou veículo é sempre um outro meio ou veículo”. Bolter e Grusin (1999) definem a referida relação como uma genealogia de afiliações, em que nenhum

<sup>4</sup> “Visual culture is currently an important field of academic study, not only because cinema and television are ubiquitous but because we recognize that any diagnosis of contemporary conditions must take into account the widespread influence of these technologies and their effects on all other aspects of culture, including the way that we experience ourselves and what this implies for the structure of societies.”

<sup>5</sup> Conforme o conceito de remediação dos autores Jay Bolter e Richard Grusin (1999) na obra *Remediation, understanding new media*.

meio de comunicação é capaz de funcionar de maneira independente no espaço cultural, mas sempre relacionado a outro.

Em seu importante estudo da nova Remediação da mídia, Jay David Bolter e Richard Grusin definem meio como ‘aquilo que remedia’. Em contraste com a visão modernista que tem como objetivo definir as propriedades essenciais de cada meio, Bolter e Grusin propõem que todos as mídias se ‘remediam’, ou seja, remodelando, reformando outros meios de comunicação, tanto nos níveis de conteúdo quanto forma. Se estamos pensando na interface homem-computador como outra mídia, sua história e desenvolvimento atual definitivamente se encaixam nesta tese. A história da relação homem-máquina é a de contração de empréstimos e reformulações, ou, para usar a nova linguagem da mídia, reformatando outros meios de comunicação, tanto do passado quanto do presente: a página impressa, cinema, televisão<sup>6</sup> (MANOVICH, 2001, p. 83, tradução nossa).

De forma complementar, a refletir sobre aspectos durante dos meios sobre outros meios, e, conseqüentemente, sobre as audiovisualidades como virtualidades da *tecnocultura*, Bruno Polidoro (2008, p. 1) sintetiza que se trata de “[...] com isso, compreender o sentido de linguagem nesses diversos suportes de som e imagem”. Outra possibilidade para se pensar um objeto audiovisual é “desde a perspectiva de sua irredutibilidade a qualquer mídia, admitindo que o audiovisual também é uma virtualidade que se atualiza nas mídias, mas que as transcende” (KILPP; FISCHER, 2010, p. 39). Nesse sentido, Fischer (2013, p. 46) faz ligação da *tecnocultura* com a proposta de Walter Benjamin (1986) para pensarmos as mídias e o envolvimento com a tecnologia, envolvendo esta como papel importante na capacidade de reprodução ao desafiar a autenticidade (como em seu livro *A obra de arte da era de sua reprodutibilidade técnica*, de 1986),

Ainda que pensando em fonogramas e fotografia na cultura parisiense do século XIX, as reflexões de Benjamin sobre o que se toma a experiência humana a partir do imbricamento das tecnologias de (re) produção de imagens e sons são embebidas de uma perspectiva tecnocultural absolutamente essencial para as discussões contemporâneas que marcam as reflexões dos autores que observam a sociedade midiaticizada e softwarizada (FISCHER, 2013, p. 46).

Portanto, como uma das características do ambiente da *web* é incentivar o compartilhamento e a dispersão de conteúdo *online*, incentivando o fluxo de dados, a ação de um usuário ao compartilhar para sua rede de amigos, no FB, um arquivo de texto, foto ou

---

<sup>6</sup> “In their important study of new media Remediation, Jay David Bolter and Richard Grusin define medium as ‘that which remediates’. In contrast to a modernist view aims to define the essential properties of every medium, Bolter and Grusin propose that all media work by ‘remediating’, i.e. translating, refashioning, and reforming other media, both on the levels of content and form. If we are to think of human-computer interface as another media, its history and present development definitely fits this thesis. The history of human-computer interface is that of borrowing and reformulating, or, to use new media lingo, reformatting other media, both past and present: the printed page, film, television.”

vídeo<sup>7</sup>, publicado anteriormente por outro usuário, podemos inferir que há dispersão de conteúdo “sem limites”, onde cada usuário compartilha, comenta ou curte e, assim, estimula/incita sucessivamente uma ação de sua rede de amigos.

A dispersão e convergência assim proposta como virtualidade, tal como as audiovisualidades, atualiza-se hoje especialmente nas plataformas de compartilhamento de vídeos na internet, nas quais a imagem aparece ao lado de outras tornadas afins segundo os mais diferentes critérios de afinidade imaginada pelos detentores do site ou imaginada por seus usuários, sejam eles realizadores, empresas de comunicação ou apenas colecionadores, sendo a dispersão um dos critérios da convergência (KILPP, 2012, p. 224).

De maneira complementar ao comentário de Kilpp (2012), buscamos nas palavras de Vilém Flusser (2008, p. 24), a possibilidade de articular um tipo de imagem e sua relação com a tecnologia, que ele denomina por “imagens técnicas”, ou “[...] tentativas de juntar os elementos pontuais em nosso torno e em nossa consciência de modo a formarem superfícies e destarte taparem os intervalos”, o que resumidamente seriam imagens produzidas por aparelhos. Nas palavras do próprio autor, “aparelhos são produtos da técnica que, por sua vez, é texto científico aplicado. Imagens técnicas são, portanto, produtos indiretos de textos – o que lhes confere posição histórica e ontológica diferente das imagens tradicionais” (FLUSSER, 2002, p. 10). Portanto, cabe aqui fazer a relação com as propostas McLuhaniana (1964) e *remediadora* de Bolter e Grusin (1999), assumindo a genealogia de afiliações, interligando substancialmente técnica e cultura.

Retomando as possibilidades de intervenção nas imagens e suas associações através dos *softwares*, o usuário da *web* acaba por fazer a sua captação de imagens, por editar e intervir conforme desejar – e o *software* permitir. Iniciativas dentro do FB, por exemplo, permitem ao usuário “curtir” e intervir na imagem via interface com *emojis* de corações, sorrisos ou choros, mesmo este usuário não sendo o responsável por postar ou captar/produzir o vídeo que está sendo transmitido. Há quase 20 anos, Lev Manovich (2001) reforçou a reflexão que o hibridismo entre os meios não está restrito aos aplicativos de *softwares* “recentes”, interfaces ou ao ambiente digital da *web*, mas está presente nas produções estéticas das imagens, principalmente através de intervenções de cineastas, animadores e designers que sofreram forte influência nos anos 1990, lançando uma nova estética híbrida.

---

<sup>7</sup> Nossa intenção aqui não é designar os “tipos” de audiovisuais, visto que justamente essa atitude provocaria um falso problema, na perspectiva de Bergson. Mas o que, de fato, estamos buscando são devires audiovisuais que se atualizam em materialidades midiáticas, ou o que dura das audiovisualidades em matéria/espço.

Hoje, essa linguagem domina a cultura visual de dezenas de países. Nós vemos isso todos os dias em comerciais, vídeos de música, gráficos animados (gráficos em movimento), gráficos de TV, design de crédito, interfaces interativas de celular e outros dispositivos, menus dinâmicos, páginas animadas, gráficos móveis e todos os tipos de narrativas, interfaces e conteúdo que são produzidos por profissionais (empresas e designers independentes e artistas) e por estudantes. No entanto, estimamos que pelo menos 50% das imagens em movimento de curto prazo sigam essa linguagem (MANOVICH, 2001, p. 214).

Para pensar na interface que realiza a mediação entre o *software* e o usuário, Priscila Arantes (2012, p. 172) comenta que este “seria um dispositivo que possibilita um fluxo de informações, manifesta-se também dentro do próprio sistema computacional a partir dos códigos de programação”, e, nesse sentido, há um hibridismo entre formatos de mídia acontecendo nesse ambiente da *web*. As palavras da pesquisadora levam a perceber sobre as diversas formas de consumo de conteúdo audiovisual na *web*, atualmente, e as distintas possibilidades de posicionar o usuário como participante ativo dentro desse fluxo, seja através da produção/captação de vídeo, até ser o responsável por disseminar postagens de terceiros por meio da resposta aos incentivos do FB para curtir, compartilhar, participar, comentar e simplesmente assistir ao que acontece no *feed* de notícias de cada usuário ativo.

Ao encontro dessas possibilidades de intervenção direta do usuário, Lev Manovich (2001) propõe que o conceito de interface esteja diretamente relacionado com a definição de uma interface cultural, ou seja, a interface gráfica realizando a mediação entre um computador e o usuário da máquina. Para o autor, “em termos semióticos, a interface do computador atua como um código que transporta mensagens culturais em uma diversidade de suportes” (MANOVICH, 2001, p. 113). Nesse sentido, complementa sua justificativa pelo termo, ao dizer que

Eu introduzi o termo “interfaces culturais” para descrever as interfaces usadas pela hipermídia autônoma (CD-ROM e DVD títulos), sites, jogos de computador e outros objetos culturais distribuídos através de um computador. Acho que precisamos de um termo, pois como o papel do computador está se deslocando de ser uma ferramenta para uma máquina de mídia universal, estamos cada vez mais “interfaceando” com dados predominantemente culturais: textos, fotografias, filmes, músicas, documentos multimídia, ambientes virtuais. Portanto, a interface humano-computador está sendo complementada pela interface humano-computador cultura, que eu abrevio como “interface cultural (MANOVICH, 2001, p. 79).

Portanto, o termo interface entre homem e computador, ou interface de usuário, descreve as maneiras pelas quais interagimos com o computador, por meio dos dispositivos físicos de entrada e saída, como o monitor, o teclado e o mouse (MANOVICH, 2001). Nesse sentido, o pesquisador ainda comenta que não se pode encarar a interface como algo que simplesmente está “entre” o homem e a máquina, mas que impõe regras e novas lógicas de

raciocínio e pensamento no usuário, indo além das funcionalidades operacionais, implementando uma nova maneira de encarar a relação de tempo e espaço

Em suma, a interface, longe de ser uma janela transparente para os dados que abrigam o computador, vem com suas próprias mensagens poderosas. Como um exemplo de como a interface impõe sua própria lógica na mídia, vamos pensar nas operações de “cortar e colar”, comuns em todos os softwares que funcionam com a moderna interface gráfica do usuário. É uma operação que torna insignificante a distinção tradicional entre meios espaciais e temporais, a partir do momento em que podemos recortar e colar fragmentos de imagens, regiões do espaço ou pedaços de uma composição temporal exatamente da mesma maneira. Também é “cego” às diferenças tradicionais de escala: podemos recortar e colar um único pixel, uma imagem ou um filme digital inteiro da mesma maneira. E, finalmente, é uma operação que também torna insignificantes as diferenças tradicionais entre a mídia: o “recortar e colar” pode ser aplicado a textos, bem como a imagens fixas e em movimento, ou a sons e objetos em três dimensões (MANOVICH, 2001, p. 114).

Para o autor, o termo “interface cultural” representa também o resultado da evolução e relação de hibridismo entre as mídias, como, por exemplo, a passagem da impressão, do cinema até o que temos de interfaces humano-computador.

Há outra maneira de pensar sobre a diferença entre o design e a arte das novas mídias em relação ao conteúdo, e é a dicotomia da interface. Ao contrário do design, na arte a conexão entre forma e conteúdo (ou, no caso de novas mídias, entre a interface e o conteúdo) é motivada; ou seja, a escolha de uma determinada interface é motivada pelo conteúdo do trabalho, a tal ponto que você não pode mais pensar nele como um nível separado. O conteúdo e a interface são combinados em uma única entidade e não podem mais ser separados (MANOVICH, 2001, p. 116).

De maneira complementar, Gustavo Fischer (2015, p. 61) comenta sobre o conceito da *graphical user interfaces* ou interface gráfica do usuário (GUIs), ao relacionar o conceito de interface defendido por Manovich e o ambiente da *web*, interagindo com “o campo das interfaces digitais e suas propriedades midiáticas”:

Talvez um dos truques mais bem-sucedidos das Graphical User Interfaces (GUIs), quando passamos a encontrar nelas a colorida, hipertextual e janelizada world wide web (mas quem sabe também antes mesmo disso, com os softwares off-line cujo funcionamento disparamos pela abençoada metáfora do desktop), seja o de nos propor que há um lugar ou destino específico para o audiovisual: “ser vídeo”. Aprendemos, como usuários comuns, que o audiovisual é formato que se encaixa e se fixa em determinadas situações (páginas web). O audiovisual seria, como dizem os protagonistas do mercado de comunicação digital (os realizadores, por que não dizer?), parte cada vez mais relevante da ideia de “conteúdo” (FISCHER, 2015, p. 61).

Assim como as interfaces são resultado da técnica e da cultura, operando a partir de um *software*, no caso das GUIs, ao direcionarmos nosso olhar para a participação da construção visual que temos hoje de nosso cotidiano, é possível inferir o processo reverso, ou

seja, um *looping* do impacto da estética das interfaces e seu reflexo em nosso cotidiano. Seja na produção cultural, econômica e social, na forma como nos referimos a diversas manifestações oriundas de movimentos de tela, ao tentarmos expandir imagens com os dedos em uma interface que não possui a tecnologia *touchscreen*, ou, então, o desejo de buscar algum termo em livro impresso com o tentador comando “Ctrl + F” que é “nativo” da leitura digital. Adriano Rodrigues (2000, p. 1) comenta sobre como a nossa percepção de mundo hoje é impactada pelos dispositivos de midiatização “[...] que marcam o ritmo da nossa vida quotidiana, sobrepondo-se cada vez mais não à nossa percepção imediata do mundo, mas também aos ritmos do funcionamento das instituições que formam os quadros da nossa experiência individual e coletiva”.

Ao encontro dessa perspectiva, a interface digital, como ambiente de imbricamento de uma experiência que funde cultura e técnica, poderia ser encarada, nos termos de Steven Johnson (2001, p. 5) como “todo o mundo imaginário de alavancas, canos, caldeiras, insetos e pessoas conectados – amarrados entre si pelas regras que governam esse pequeno mundo”. Dentro (e fora) desse ambiente é que vamos nos debruçar a problematizar sua forma, estética, sua maneira de operar que nosso objeto empírico constrói, então, como “segurança” em suas interfaces.

Mas, ao tratarmos sobre estética da *tecnocultura*, a construção de imagens, formas, texturas e cores que se fundem numa interface, julgamos ser necessário recorrer novamente à proposta de Walter Benjamin (2013), ao fazermos uma crítica sobre a perda da aura da arte ao implicar a morte da estética artística a partir da capacidade de reprodução causada pela tecnologia. Como reforça Priscila Arantes (2012, p. 159), “a reprodutibilidade técnica transformaria o caráter e a natureza intrínseca da obra de arte, bem como sua relação com o receptor e produtor”, desde a perda da aura, sua autenticidade, “o aqui e o agora da obra de arte – sua existência única no local em que se encontra. No entanto, é nessa experiência única, e somente nela, que está realizada a história à qual a obra de arte esteve submetida no decorrer de sua duração” (BENJAMIN, 2013, p. 54).

Justamente por percorrer esse ambiente fluido, disperso e convergente das *webpages* e aplicativos conectados à internet, é que as imagens se reproduzem pelas telas ou interfaces, compondo o que Fischer (2008, p. 43, grifos do autor) nomeia como sendo uma das “facetas da *web*”<sup>8</sup>, o seu ambiente de relacionamento no qual “[...] o usuário estabelece uma relação de

---

<sup>8</sup> Fischer (2008) complementa com a proposta de se trabalhar com três facetas para a caracterização da internet: banco de dados, mídia e ambiente de relacionamento.



diversos níveis de marcação da sua presença na *internet*, e, por conseguinte, na *web*". Exemplificativamente, podemos citar os diversos *sites* de relacionamento ou as redes sociais, no que "diz respeito às diversas dinâmicas de expressão e interlocução dos sujeitos que se estabelecem em várias ocorrências percebíveis da mesma" (FISCHER, 2012b, p. 142).

Essa proposta nos leva a refletirmos sobre a cultura contemporânea e a estética de "nosso tempo", ou, nas palavras de Lev Manovich (2012, p. 2), "para detectar formas estéticas e culturais emergentes específicas em uma sociedade da informação globalizada", mas não se trata de caracterizar um estilo ou gênero, mas uma *infoestética* para "às práticas culturais que podem ser melhor compreendidas como resposta às novas prioridades da sociedade da informação: dar sentido à informação, trabalhar com ela e produzir conhecimento a partir da informação". A *infoestética* não está relacionada à cultura digital, programação ou algo relacionado estritamente à informática, como o nome pode parecer, mas sim à informação e como o grande volume de conhecimentos gerados em nossa forma de comunicação hoje se reflete em diversas manifestações a partir desse fluxo constante de dados.

O conceito de *infoestética* propõe olhar para manifestações da nossa cultura contemporânea muito contagiada por lógicas de dados, podendo ser articulado com a nossa reflexão sobre as audiovisualidades durante em objetos midiáticos, como, por exemplo, atualizações no sentido da coalescência de tempos de Bergson proposto por Deleuze (1999), ou como determinadas virtualidades se materializam em nossa cultura.

Nas cenas audiovisuais (tanto as midiáticas quanto as marginais) que circulam nos ambientes (todos – online e offline) por onde circulam os sujeitos da cultura, a dispersão e irregularidade de formatos, linguagens e estéticas estão relacionadas a cenas da cultura, atualizada por usos e protagonismos também dispersos e irregulares, que "fluem entre" padrões, normalizações e controles tradicionais (KILPP, 2010, p. 184).

Ao nos propor estudar a "cultura contemporânea em geral", Manovich (2012, p. 3-4) argumenta que "a *infoestética* pode se referir à experiência de se viver numa sociedade da informação através do seu design, textura, composição, estrutura, construção, sensibilidade e outras dimensões artísticas". Justamente nessa maneira de enxergar nosso objeto empírico é que acreditamos ser possível verificar a *infoestética* que se manifesta nas interfaces do FB, por exemplo. Inferimos que a estética, o design, as cores e as maneiras que o FB utiliza em ícones, ilustrações e animações, apresentam uma estética que acreditamos se tratar de atualizações de muitas memórias e imaginários construídos para seu usuário (e pelo usuário) dentro do ambiente da rede social.

Portanto, nosso objeto de pesquisa, os sentidos de *tecnosegurança*, se atualizam nas interfaces do FB de diversas formas, e são estéticas que vão desde a *imageria* relacionada ao mundo “*offline*”, como cadeados, chaves, etc., mas também com uma estética própria do FB, que preconiza o cuidado, de se sentir seguro entre amigos, da lembrança da infância, de um momento de alegria, de estar em comunidade, e vários outros sentidos encarados como “seguros” e que iremos explorar na dissecação do objeto. Salientamos que estamos adotando o termo *imageria* a partir da proposta de Jacques Rancière (2012, p. 24) ao sugerir o termo que “deve ser tomado aqui em sentido amplo – relativo a todas as formas de produção e reprodução de imagens, não especificamente às produzidas por ‘equipamento imageador’, como repertório de imagens disponíveis”.

Paralelamente, há ambivalência no sentido da segurança, pois, para que o usuário tenha acesso a esse ambiente cheio de sentidos “seguros”, renuncia-se à privacidade, ao ceder informações e dados pessoais para o FB e seus parceiros comerciais. Nesse sentido, entramos no próximo item a ser abordado neste capítulo, *tecnosegurança* e uso de dados, onde exploramos conceitos que envolvem o uso de dados e como as mídias trabalham as construções de sentido de sigilo, confiança prometida e privacidade dos dados e dos conteúdos publicados por seus usuários, caracterizando uma preocupação própria da cultura contemporânea, uma *tecnosegurança*.

## **2.2 *Tecnosegurança***

Na medida em que fomos nos aprofundando na fenomenologia bergsoniana, onde é possível encarar que todas as coisas têm dois modos: de ser (virtualidade/duração) e de agir (durações ou realizações na matéria), compreendemos que nas imagens capturadas das interfaces da rede social FB, é possível percebermos as audiovisualidades como potência. Isso significa que a imagem assume o papel central nessa tese, entendendo-a como materialidade que carrega atualizações em seu devir, ou seja, sendo portadora de memória. Essa reflexão, a partir de Bergson, é estruturante para dar continuidade ao conceito de memória das imagens com forte inspiração no estudioso francês Georges Didi-Huberman (2015), ao defender que há um imaginário contido nas imagens, e, conseqüentemente, não há memória sem imaginação “Assim como não há forma sem formação, não há imagem sem imaginação. Então, por que dizer que as imagens poderiam ‘tocar o real’? Porque é um enorme equívoco querer fazer da

imaginação uma pura e simples faculdade de desrealização”<sup>9</sup> (DIDI-HUBERMAN, 2015, p. 1, tradução nossa).

Se para Didi-Huberman (2015) as imagens apresentam memória, é desse olhar que nos apropriamos ao encararmos as interfaces do FB como uma imagem que atualiza em sua materialidade ou espaço, sentidos de tecnosegurança baseados em iniciativas que reconvocam alguns imaginários em seus usuários. Paralelamente, o que significa a representação imagética de algo seguro e confiável ao usuário da *web*, muitas vezes, permanece relacionada a associações tradicionais de segurança, como verificado no exercício de *flânerie*<sup>10</sup> realizado nas interfaces, através da representação de cadeados, chaves, senhas, escudos etc., e, também, conforme apresentado na introdução de nossa tese, a partir de diversas iniciativas contemporâneas, como entretenimento, vigilância, monitoramento de circulação urbana, campanhas publicitárias, mídias e dispositivos.

Nessa direção, Didi-Huberman (2015, p. 15) desenvolve uma reflexão sobre a relação do tempo com as imagens como são indissociáveis

Sempre, diante da imagem, estamos diante do tempo. Como o pobre iletrado da narrativa de Kafka, estamos diante da imagem como Diante da lei: como diante do vão de uma porta aberta. Ela nada nos oculta, bastaria entrar, sua luz quase nos cega, nós a respeitamos. Sua própria abertura - e eu não me refiro ao guardião - nos faz parar: olhá-la é desejar, é esperar, é estar diante do tempo. Mas que tipo de tempo? De que plasticidades e fraturas, de que ritmos e embates do tempo poderiam se tratar nessa abertura da imagem?

Por esse viés, é que entendemos que pelas interfaces do FB, os sentidos de *tecnosegurança* são enunciados para algo além dessa construção formal do termo, mas desde toda arquitetura que promove e incentiva a confiança do usuário a conceder suas informações voluntariamente, estimulando o uso da rede social, a partir da promessa de proteção de seus dados. Como mencionado por Göran Bolin e Anne Jerslev (2018, tradução nossa), no artigo *Segurança através da mídia, pela mídia e na mídia*<sup>11</sup>, é possível fazermos uma relação dessa construção de confiança do usuário com a plataforma, abrindo o debate para aspectos relacionados à vigilância realizada dentro da mídia, na mídia e pela mídia, como o FB, por exemplo, ao coletar dados e utilizar essas informações para fins comerciais e institucionais,

<sup>9</sup> “Al igual que no hay forma sin formación, no hay imagen sin imaginación. Entonces, ¿por qué decir que las imágenes podrían ‘tocar lo real’? Porque es una enorme equivocación el querer hacer de la imaginación una pura y simple facultad de desrealización.”

<sup>10</sup> O conceito de *flâneur* – proposto por Walter Benjamin, será aprofundado no capítulo dedicado ao procedimento metodológico, onde vamos nos apoiar na cartografia como maneira de mapear os sentidos de segurança nas interfaces do FB.

<sup>11</sup> “*Surveillance through media, by media, in media.*”

O aumento das oportunidades para empresas e administrações estaduais monitorar o comportamento do cliente e do cidadão 24 horas por dia por meio de várias tecnologias de mídia em uma arquitetura de informação digital aberta aumentam uma gama de questões éticas, legislativas e políticas relativas à mídia no que diz respeito privacidade, cidadania, poder e direitos individuais versus o bem comum<sup>12</sup> (BOLIN; JERSLEV, 2018, p. 4, tradução nossa).

Embora o aspecto da vigilância não seja o tema central dessa tese, ele nos interessa no que diz respeito aos sentidos de *tecnosegurança*, pois entendemos que eles são construídos por determinados territórios que atravessam aspectos associados à privacidade, controle, monitoramento, confiança e proteção. Fernanda Bruno (2013, p. 7) reflete sobre o papel das tecnologias e das mídias, assim como Bolin e Jerslev (2018), e relaciona as práticas de intimidade e sociabilidade que prevalecem nas redes sociais, onde “uma série de questões de ordem estética, política e social endereçam-se às dinâmicas de produção e circulação dessas imagens, marcadas por ambiguidades [...]”.

Nesse sentido, o jornal *The Wall Street Journal* (ANGWIN; SINGER-VINE, 2012), realizou uma pesquisa, há aproximadamente 10 anos, alertando para questões éticas envolvendo a coleta, armazenamento e uso de dados para capitalizar a empresa jornalística com essas informações, que vale lembrar, foram todas cedidas voluntariamente por usuários. O problema é que a empresa utilizou dados sensíveis<sup>13</sup> fornecidos por esses usuários e compartilhou com uma vasta lista de desenvolvedores de aplicativos, anunciantes e diversas outras oportunidades comerciais, conforme relato do jornal americano:

Esse apetite por dados pessoais reflete uma verdade fundamental sobre o Facebook e, por extensão, a economia da Internet como um todo: o Facebook oferece um serviço gratuito pelo qual os usuários pagam, na verdade, fornecendo detalhes sobre suas vidas, amizades, interesses e atividades<sup>14</sup> (ANGWIN; SINGER-VINE, 2012, p. 1, tradução nossa).

Esse envolvimento de diversas iniciativas privadas que gira em torno da coleta, armazenamento e uso de dados de usuários, por exemplo, caracterizam um fluxo de monitoramento de dispositivos que deixam rastros de seus usuários por toda internet. Eles

---

<sup>12</sup> “The increased opportunities for corporations and state administrations to monitor customer and citizen behaviour around the clock through various media technologies in an open digital information architecture raise a range of ethical, legislative and political questions relating to the media concerning privacy, citizenry, power and individual rights versus the common good.”

<sup>13</sup> Dados considerados sensíveis pela LGPD – dados biométricos, sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genético ou biométrico, quando vinculados a uma pessoa natural (DATA PRIVACY BR, 2021).

<sup>14</sup> “This appetite for personal data reflects a fundamental truth about Facebook and, by extension, the Internet economy as a whole: Facebook provides a free service that users pay for, in effect, by providing details about their lives, friendships, interests and activities.”

formam um ambiente onde estrutura-se um relacionamento entre os usuários finais, consumidores e produtores de conteúdo, com parceiros comerciais e o próprio *software*, denominando um ambiente de plataforma,

Uma “plataforma” online é um programa maleável de arquitetura digital projetada para organizar as interações entre os usuários – não apenas usuários finais, mas também entidades corporativas e órgãos públicos. É voltado para a coleta sistemática, processamento algorítmico, circulação e monetização do dados do usuário<sup>15</sup> (VAN DIJCK; POELL; WALL, 2018, p. 4).

Essa proposta de plataformização da sociedade se estende para muitos ambientes, como alimentação, deslocamento, moradia, viagens, mídia, etc., onde usuários necessitam conceder suas informações, desde dados tidos como sensíveis, até suas publicações, textos, fotos e vídeos às plataformas. Mas o que nos interessa aqui é a relação de segurança, via promessa de confiança e privacidade por essas iniciativas de um “ecossistema de plataformas”, conforme denominam Van Dijck, Poell e Wall (2018), onde não há uma plataforma independente da outra, mas todas constituindo uma lógica própria do contexto *online*. Nesse sentido, é possível relacionarmos a segurança prometida pelas plataformas aos usuários finais, com a vigilância estruturada a partir da interpretação de dados de navegação desses indivíduos, que são utilizados para fins comerciais, análise preditiva e molde de comportamentos futuros. Shaw (2008, p. 35) a relaciona com uma das características que estão engendradas na *tecnocultura*, a ambivalência entre segurança e vigilância:

Desde os acontecimentos de 2001 e com o surgimento de técnicas de infiltrações mais sofisticadas, como vermes, vírus e “bots” (robôs de software que podem desativar um sistema de computador), controles e estratégias de vigilância cada vez mais rigorosos têm sido implementados, que ameaçam a privacidade individual e anteriormente liberdades não regulamentadas da rede mundial de computadores.

Fernanda Bruno (2012) faz um levantamento do que ela chama de “rastros digitais”, como “traços” ou vestígios que todos deixamos na rede ao utilizarmos as tecnologias digitais. Traçamos caminhos por pesquisas que realizamos, quais redes sociais utilizamos, como interagimos, compras ou cadastros em *sites*, e essas informações alimentam uma lógica de operação e monetização de plataformas de dados de seus usuários,

---

<sup>15</sup> “An online ‘platform’ is a programmable digital architecture designed to organize interactions between users – not just end users but also corporate entities and public bodies. It is geared toward the systematic collection, algorithmic processing, circulation, and monetization of user data.”

Este texto nasce desta ocasião e explora o problema a partir das pistas encaminhadas pela teoria ator-rede (TAR)<sup>16</sup>, especialmente pelo trabalho de Bruno Latour (2007). A quantidade e a qualidade dos rastros digitais, hoje presentes na internet oferecem às ciências sociais, segundo este autor, a possibilidade de renovar tanto suas metodologias quanto suas abordagens teórico-conceituais. Tais ciências jamais estiveram diante de uma riqueza tão grande de dados: rastros subjetivos, comportamentais, linguísticos, financeiros, bem como interações, associações e conflito de diversas escalas tornam-se significativamente mais fáceis de serem descritos e retrçados (BRUNO, 2012, p. 687).

A relação de vigilância realizada nas mídias carrega, em sua origem, a inspiração na proposta de Michel Foucault na obra *Vigiar e punir* (1983), onde o autor traz a perspectiva de controle e punição na sociedade embasada na ideia de constante vigilância para a supremacia do poder. Foucault (1983, p. 24) sugere um novo modelo prisional para as Ciências Jurídicas que não envolve métodos repressivos, ou uso da tecnologia política do corpo, mas como “uma função social complexa”, onde o modelo panóptico é estipulado para implementação do bom adestramento para aprisionados, sempre sob a vigilância de quem está no poder.

“O exercício da disciplina supõe um dispositivo que obrigue pelo jogo do olhar; um aparelho onde as técnicas que permitem ver induzam a efeitos de poder, e onde, em troca, os meios de coerção tornem claramente visíveis aqueles sobre quem se aplica” (FOUCAULT, 1983, p. 144). Esse modelo de vigilância hierárquica, onde quem controla é consequentemente quem tem mais poder, se relaciona com a proposta do capitalismo de vigilância que Zuboff (2020) sintetiza, já que os dados e informações sobre as pessoas estão nas mãos de grandes iniciativas privadas e governamentais, que têm largas condições de investimento e desenvolvimento de tecnologia para coleta e armazenamento a partir de uma vasta estrutura de inteligência de dados.

Esse aspecto também esbarra na ambiguidade do termo vigilância, pois vigiar também pode significar tomar conta, proteger ou manter a segurança de alguém ou alguma coisa, por exemplo. É nesse sentido que vamos explorar a ambivalência do termo para refletirmos sobre os sentidos de *tecnosegurança* nas interfaces do FB, que ora podem ser acompanhados pelo imaginário de cuidado, ora a construção de segurança pode se atualizar a partir de construtos como privacidade do usuário e dos seus dados confiados ao FB.

Mas, a cultura do cuidado e da segurança é premissa da proposta de se viver em comunidade, conforme afirma Bauman (2003), onde o confortável e seguro é a garantia de estar em um ambiente que caracteriza o zelo entre seus habitantes. Foi necessário apoiar-nos

---

<sup>16</sup> Pelo interesse da perspectiva das audiovisualidades já explicitadas nessa tese e que nosso objeto demanda, o arranjo metodológico proposto no próximo capítulo não contempla a TAR, mas uma proposta que envolve *flânerie*, cartografia, coleção, dissecação e emolduramento, conforme será explicitado no capítulo dedicado à metodologia.

na proposta do autor para debatermos a construção de sentidos de *tecnosegurança* nas interfaces do FB, pois, no exercício de *flânerie* e posterior escavação que realizamos na plataforma, seja na sua versão para *web* ou aplicativo, identificamos com o conceito de Bauman na obra *Comunidade. A busca por segurança no mundo atual* (2003), em que o autor associa à comunidade uma sensação positiva, confortável e que carrega associações de imagens de lugar acolhedor e protegido das ameaças “de fora”.

Os significados e sensações que as palavras carregam não são, é claro, independentes. “Comunidade” produz uma sensação boa por causa dos significados que a palavra “comunidade” carrega – todos eles prometendo prazeres e, no mais das vezes, as espécies de prazer que gostaríamos de experimentar, mas que não alcança mais (BAUMAN, 2003, p. 7).

Percebemos pela *flânerie* que realizamos que a construção da comunidade segura e confortável acontece dentro do FB, onde há constante tentativa da rede social em manter seu usuário dentro de seu ambiente o tempo possível, estimulando seu engajamento e relacionamento com os demais usuários da rede. Acreditamos que os sentidos de *tecnosegurança*, construídos nas interfaces perpassam por uma série de construção de imaginários que estão alicerçados na comunidade de Bauman (2003), com o recurso das imagens que evocam memórias associadas a sensações positivas, agradáveis e relacionadas a um imaginário de proteção. Estar dentro dessa comunidade, ou melhor, logado no FB e dentro daquele ambiente colorido e cheio de “amigos” pode se associar ao sentimento que “se tropeçarmos e cairmos, os outros nos ajudarão a ficar de pé outra vez” (BAUMAN, 2003, p. 8), ou seja, há uma espécie de tentativa de construção de um ambiente alegre, com som e movimento que nos remete à sensação de pertencimento, de acolhimento, muitas vezes relacionadas ao universo infantil<sup>17</sup>. A própria lógica do algoritmo do *software* do FB em manter sugestões de publicações com conteúdo similares àqueles que tendem a agradar o usuário é uma tentativa de criar um mundo favorável ao contexto de interesses e comportamentos compreendidos, interpretados e, posteriormente, moldados pelo FB.

Dessa maneira, permanecer nas interfaces do FB pode sugerir uma construção de sensação de escape do mundo de “fora”, ou seja, uma relação de utopia ou sonho, ao mesmo tempo que constrói dicotomia entre permanecer naquela comunidade que é lar e exílio do mundo de fora, “não é só a “dura realidade”, a realidade declaradamente “não comunitária” ou, até mesmo, hostil à comunidade, que difere daquela comunidade imaginária que produz

---

<sup>17</sup> Os sentidos de *tecnosegurança* no FB serão exibidos melhor no Capítulo 4, serão apresentadas as constelações, onde inferimos construções a partir de imaginários que emergem das imagens.

“sensação de aconchego” (BAUMAN, 2003, p. 9), tornando nossa admiração por esse sentimento de pertencimento e segurança cada vez mais atraente. O interesse da plataforma em manter o usuário “retido” dentro de seu ambiente por um longo período configura uma das métricas de avaliação de tráfego *online* do ambiente digital, demonstrando o tempo de permanência na página como algo positivo, entregando relevância daquele conteúdo para o usuário. Esse tipo de métrica serve para comprovar ao mercado anunciante, ou parceiros comerciais do FB, que dentro de seu ambiente há identificação com seu *target*, ou seja, um campo fértil para gestão de marcas a partir de conteúdo pago via publicidade.

A pesquisadora Wendy Chun (2016, p. 10, tradução nossa) comenta sobre esse paradoxo que foi criado entre público x privado nas mídias e sua suposta liberdade prometida, caracterizando-as como “maravilhosamente assustadoras<sup>18</sup>” pois são fascinantes, viciantes, revolucionárias e revoltantes. Para a autora, as novas mídias apresentam um caráter curioso, e se faz necessário romper com diversas suposições que surgiram com a promessa do “ciberespaço” como um território anônimo que preconizava a liberdade. Na verdade, o *cartoon* que ilustramos na introdução de nossa tese, publicado pela revista *New Yorker* nos anos 1990, perdeu o sentido por meados de 2010, com a revolução das mídias sociais que, segundo Chun (2016), fez com que a internet passasse a ser um espaço privatizado e de vigilância total, mudando alguns imaginários associados à internet e sua (falta de) liberdade.

Diante disso, por que imaginamos a Internet – que é, em sua base, um protocolo de controle – como um espaço anônimo de liberdade? Por que os dispositivos de rede são descritos como “pessoais”, quando são tão tagarelas e promíscuos? Além disso, dada a efemeridade da informação digital, como a memória eletrônica se confunde com o armazenamento? Dá muito trabalho – pelo menos a Agência de Segurança Nacional dos EUA, sites de mídia social que promovem “identificadores únicos” multiplataforma e vastas fazendas de servidores que contribuem para a mudança climática global – para tornar a Internet a base para a vigilância mundial. Se a frase “uma vez que está lá, está lá para ficar” faz algum sentido, é porque a vigilância agora é coproduzida transnacionalmente por estados e corporações privadas<sup>19</sup> (CHUN, 2016, p. 10).

Romper com um imaginário associado ao lançamento da internet como promessa de espaço livre de controle, é o que sinaliza o uso das novas mídias, já que a rastreabilidade é um

---

<sup>18</sup> “Wonderfully creepy.”

<sup>19</sup> “Users constantly download their neighbor’s traffic. Given this, why did we ever imagine the Internet—which is, at its base, a control protocol—to be an anonymous space of freedom? Why are networked devices described as ‘personal’, when they are so chatty and promiscuous? Further, given the ephemerality of digital information, how has electronic memory become conflated with storage? It takes a lot of work—at the very least the U.S. National Security Agency, social media sites that foster cross-platform ‘unique identifiers’, and vast server farms that contribute to global climate change—to make the Internet the basis for world wide surveillance. If the phrase ‘once it’s there, it’s there to stay’ makes any sense, it is because surveillance is now co-produced transnationally by states and private corporations.”



dos fatores-chave para monetização de plataformas e *publishers*. Algo que reforçou essa expectativa na “origem” da internet em ser um espaço livre, se deve ao fato dela romper com os grandes monopólios de mídia, possibilitando ao usuário uma utopia de fluxo “livre” de informação, defendendo a democracia e a liberdade de expressão. Além disso, Chun (2006, p. 2, tradução nossa) comenta que o surgimento da retórica da internet como discurso de liberdade também esteve acompanhado por rumores de se tratar de uma “máquina escura de controle”<sup>20</sup>, pois a autora questiona se a internet é uma ferramenta de liberdade ou controle? Para a pesquisadora, a resposta pode estar associada a dois eixos importantes para reflexão na “era da fibra ótica”, que seria a relação de paranoia criada ao uso de poder na contemporaneidade, ou seja, caímos ao reducionismo de aspectos políticos para os tecnológicos que “mostram que essas questões e suas suposições não são apenas equivocadas, mas também sintomáticas da resposta paranoica cada vez mais normal ao uso do poder”<sup>21</sup> (CHUN, 2006, p. 3, tradução nossa).

Conforme citamos na introdução de nossa tese, acerca do escândalo de vazamento de informações denunciado por Edward Snowden, o que Chun (2016) chama a atenção neste fato é justamente de ser encarado como escândalo, pois a prática de monitoramento e vigilância de usuários na internet é algo estruturante do próprio meio.

Ainda mais perturbador do que a revelação que não foi revelação, foi a indignação corporativa que não foi nenhuma indignação. A raiva e as alegações de traição expressas por empresas como Google e Facebook contra o governo dos EUA soam falsas em vários níveis, pois as informações da NSA eram e são tão inestimáveis e insidiosas por causa de *backdoors*, nomes reais e identificadores exclusivos implementados por essas corporações<sup>22</sup> (CHUN, 2016, p. 94, tradução nossa).

Em complemento aos identificadores e métricas e voltando nosso olhar para as práticas de vigilância na mídia, e pela mídia, Bolin e Jerslev (2018) comentam que esse interesse das empresas de comunicação em conhecer sua audiência vem da necessidade de transformá-la em produto para sustentar o modelo de negócio das empresas de comunicação, a começar pelo ramo do jornalismo impresso e, posteriormente, a televisão. Com o desenvolvimento do ramo da informação e do entretenimento como negócio, surge a demanda de agrupar o consumidor desses produtos em nichos de audiência para atender o pedido, e,

---

<sup>20</sup> “dark machine of control.”

<sup>21</sup> “[...] argues that these questions and their assumptions are not only misguided but also symptomatic of the increasingly normal paranoid response to and of power.”

<sup>22</sup> “Even more disturbing than the revelation that was no revelation was the corporate outrage that was no outrage. The anger and allegations of betrayal expressed by companies such as Google and Facebook against the U.S. government ring false on multiple levels, for the NSA’s information was and is so invaluable and insidious because of back doors, Real Names, and unique identifiers implemented by these corporations.”

consequentemente, investimento de verba, de um mercado publicitário e anunciante. Dessa maneira, as mídias digitais surgem com a promessa da capacidade de segmentação, rastreabilidade, monitoramento e conhecimento sem limites sobre os rastros, ou melhor, dados, fornecidos muitas vezes sob o consentimento, outras não, de usuários na internet, o que configura o *behavioral targeting* – segmentação comportamental, no mercado publicitário atual. Conforme afirmam Bolin e Jerslev (2018, p. 4, tradução nossa), “Big data não é apenas sobre tamanho, mas sobre as possibilidades de fazer conexões entre bancos de dados e de mineração dos dados de comportamento do usuário anteriormente impossível”<sup>23</sup>.

Por isso é que Chun (2016, p. 95, tradução nossa) comenta que as plataformas de mídia social “invertem a posição de público/privado, porque o sujeito que age está cada vez mais dentro e não fora. Os sujeitos agem publicamente em privado, ou são ‘apanhados’ em público agindo em privado. Isso leva à ansiedade sobre privacidade e vigilância [...]”<sup>24</sup>. De forma complementar, Shoshana Zuboff (2020) atenta para esse aspecto em massivas iniciativas de pesquisa e tecnologia que vão ao encontro à prática de coleta de informações e de fornecimento de dados para as “*big techs*”, fazendo o que ela denomina por “*hiding in our own lives*”, ou seja, adotando o hábito de tentar manter privado o direito da própria informação. Uma dessas atitudes caracteriza o crescimento da informação criptografada, por exemplo, onde há o interesse em manter o sigilo de informação entre os correspondentes, ou as ferramentas chamadas “*ad blocks*”, que interrompem a coleta de informação do usuário em navegadores na internet e bloqueiam a exibição publicitária segmentada ao *target* específico, como Google Ads, por exemplo. A preocupação com a privacidade, conforme cita Zuboff (2020), foi concebida como algo individualizado, quando, na era do capitalismo de vigilância, a privacidade não é restrita a algo privado, mas sim social, tratando-se de uma questão de ação coletiva no século XXI, e o único caminho para tratar do tema, de acordo com a relevância que merece, é a partir de regulamentação do setor e da defesa constante da democracia. Por isso, Chun (2016, p. 70) comenta justamente sobre a retórica da internet “[...] como crítica, que ajudou a transformar a Internet de uma rede de comunicações principalmente acadêmica e militar em um meio global, ainda está conosco hoje, mesmo que

---

<sup>23</sup> “Big data are not only about size, but about the possibilities of making connections between databases, and of data-mining of user behaviour previously not possible.”

<sup>24</sup> “As I argue in chapter 4, existing social media platforms reverse the position of public/private, because the subject who acts is increasingly on the inside rather than the outside. Subjects act publicly in private, or are ‘caught’ in public acting privately. This leads to anxiety about privacy and surveillance [...]”

a experiência diária de uso da Internet não tenha correspondido ao hype”<sup>25</sup> (CHUN, 2016, p. 70, tradução nossa).

Shoshana Zuboff (2020, p. 19) alerta sobre uma promessa das tecnologias digitais conectadas à internet que coletam dados de usuários, em parte para utilizar essas informações com fins de aprimoramento de produtos, mas, também, com a finalidade de utilizar o *machine learning*<sup>26</sup>, para manufaturar “produtos de predição que antecipam o que um determinado indivíduo faria [...] são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamento futuros”. Nossas informações são coletadas a partir de captura de voz, dados cadastrais, conteúdos compartilhados e com os quais interagimos, para que esses sistemas de inteligência artificial conheçam, aprendam e moldem nossos comportamentos em grande escala.

Os produtos e serviços do capitalismo de vigilância não são objeto de uma bolsa de valores. Não estabelecem reciprocidades construtivas produtor-consumidor. Em vez disso, são “ganchos” que seduzem usuários para suas operações extrativas nas quais nossas experiências pessoais são sucateadas e empacotadas como meios para fins de outros (ZUBOFF, 2020, p. 21).

Zuboff (2020, p. 33) comenta que esse tipo de uso de conhecimento, transformado em poder, confere ao capitalismo de vigilância uma nova espécie de poder, o instrumentalismo, que visa

organizar, arrebanhar e sintonizar a sociedade de maneira a adquirir uma confluência social semelhante, uma na qual a pressão do grupo e a certeza computacional substituem a política e da democracia, extinguindo a realidade tal como a percebemos e a função social da existência do indivíduo.

Esta autora se refere justamente à coleta e uso de dados extraídos de plataformas digitais que são minerados para negociação comercial, sendo que, muitas vezes, cedemos nossas informações por meio de um “aceite” ao consenso nos termos de uso e políticas de privacidade mascaradas, ou superficialmente apresentadas aos usuários de plataformas. Nesse sentido, a prática já havia sido sinalizada por Chun (2006, p. 3, tradução nossa), quando alertava sobre as formas de controle na internet operarem por fragilidades demonstradas em seus usuários assim que “as formas de controle que a internet possibilita não são completas, e

<sup>25</sup> “This rhetoric of the Internet as critical, which helped transform the Internet from a mainly academic and military communications network into a global medium, is still with us today, even if the daily experience of using the Internet has not lived up to the hype.”

<sup>26</sup> Em livre tradução quer dizer “inteligência de máquina”.

a liberdade que experimentamos decorre desses controles; as formas de liberdade que a internet permite derivam de nossas vulnerabilidades”<sup>27</sup>.

Ao mesmo tempo em que a sensação de segurança nas mídias digitais pode vir acompanhada de cadeados, chaves, escudos, códigos e senhas, a relação da comunicação com a segurança na transmissão das mensagens é indissociável da história das mídias. Peter Krapp (2020b) relata que o agendamento da preocupação com a “eficiência do segredo”, seja no conteúdo das mensagens transmitidas, seja pelo anonimato dos dados pessoais fornecidos, pode ser contada através da imagem e da representação fantasiosa das mídias, principalmente as mídias audiovisuais como televisão e cinema, ao sofrer ataques cibernéticos:

A história das mídias pode ser contada como a história das comunicações secretas – desde muito antes das primeiras transmissões de rádio e das suas interceptações, até muito depois da televisão, que uniu comercialmente a tecnologia militar ao entretenimento. Restam poucas dúvidas de que a cultura digital carrega, por todos os lados, as marcas dos debates sobre encriptação, segurança e confiança da comunicação entre os sujeitos e seus bancos, médicos, advogados e parceiros de negócios. Além disso, quando aqueles que se opõem a uma comunicação mais segura apelam a falácias sobre o “lado sombrio” da comunicação mediada por computadores, é preciso que enfrentemos o tema da encriptação partindo de uma análise crítica das suas representações deturpadas (KRAPP, 2020b, p. 148).

Atualmente, a discussão sobre privacidade, segurança e sigilo das informações nas mídias ganhou grandes proporções com os relatos do fenômeno das “informações falsas” que se popularizou principalmente a partir das eleições norte-americanas de 2016, durante a disputa eleitoral entre os candidatos Donald Trump e Hillary Clinton (ABREU; PELLEGRINI, 2018). Para Krapp (2020b) a importância da segurança e a confiabilidade das informações seguem sendo preocupações fundamentais para a área da Comunicação, atualmente, principalmente para o jornalismo, onde credibilidade é a própria essência da atividade. E na área das redes sociais, o FB, em novembro de 2007, tornou visível parte de sua vigilância sobre seus usuários, ao mostrar como a ferramenta de publicidade Beacon Ads, coletava informações e compartilhava dados pessoais de seus membros com terceiros, ou parceiros comerciais, conforme mencionamos anteriormente (BRUNO, 2008). Mais recentemente, a ex-diretora de desenvolvimento de negócios da Cambridge Analytica, no livro *Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque* (2020), conta em detalhes a maneira como o FB compartilhou informações sobre seus usuários para seus parceiros com o objetivo de motivar intenções eleitorais com norte-americanos.

---

<sup>27</sup> “the forms of control that the internet enables are not complete, and the freedom we experience derives from these controls; the forms of freedom that the internet enables stem from our vulnerabilities.”

Nesse sentido, entramos em um debate acerca da relação entre sigilo, anonimato e segurança na *web* pois são muitas as nossas motivações como usuários da internet em zelar pela comunicação segura de nossos dados, e, conforme relata Krapp (2020b, p. 149), contamos com as garantias de integridade da comunicação às suas várias formas de autenticação, seja via duplo-*check* de verificação, códigos QR, *e-mails* de segurança e códigos via SMS, “a introdução da questão tecnológica nas Ciências Humanas altera o foco para as redes de tecnologias e instituições que permitem que determinada cultura escolha, armazene e processe dados importantes”. Mas conforme relata o pesquisador, há confusão ao compreender ocultação e segurança como sinônimos, e tratamos a partir de uma *imageria* fantasiosa as cifras e os códigos como garantias de uma privacidade nas mídias:

É fato irrefutável de que a maioria das representações midiáticas das comunicações secretas são batidas, estereotípicas, deturpadas, enganosas ou simplesmente erradas. É sob este aspecto que a exposição ao uso prático e experimental das ferramentas digitais se torna uma necessidade pedagógica (KRAPP, 2020b, p. 152).

Para Krapp (2020b) as produções midiáticas possuem um forte papel na *imageria* que se criou em torno do que configura vigilância, anonimato e segurança na comunicação via computadores, e, em recente artigo, o autor relata sua experiência como docente de maneira extremamente interessante, trazendo sua percepção sobre o que seus alunos compreendem sobre criptologia e segurança nas mídias atualmente.

Cultuar o sigilo poderia facilmente nos levar a um ressurgimento global de rumores irracionais e, infelizmente, isto é o que se vê efetivamente em boa parte da cultura da internet. O nosso futuro tende a ser consideravelmente empobrecido quando as teorias da conspiração assumem o lugar de uma cultura computacional crítica. Seguramente, ensinar os conceitos básicos de cibersegurança e algumas linhas gerais da Comunicação secreta e história da criptologia aos alunos de cinema e de estudos de mídia pode aumentar, ainda em tempo, as chances de que os seus roteiros e cenas produzam representações audiovisuais mais precisas e inteligentes da computação e da segurança da comunicação (KRAPP, 2020b, p. 158).

Mas, a representação imagética e fantasiosa sobre coleta e mineração de dados na internet dá suporte a uma construção do que poderia configurar um ambiente hostil ao usuário, o que nos auxilia ainda mais a refletir sobre as práticas do capitalismo de vigilância, que, conforme Zuboff (2020, p. 22) comenta, “[...] impõe uma escolha fundamentalmente ilegítima, que os indivíduos do século XXI não deveriam ter de fazer, e essa normalização nos deixa aprisionados, mas com a sensação de felicidade”. Temos a falsa impressão de que temos acesso a diversos conteúdos e serviços de maneira gratuita em plataformas na internet, mas, na verdade, o preço que os usuários pagam para ter acesso a estes serviços é com a própria

privacidade sob a bandeira da “[...] personalização, uma camuflagem para operações agressivas de extração que mineram o que há de mais íntimo na vida cotidiana” (ZUBOFF, 2020, p. 31).

Sob outro aspecto, ao refletir sobre a gigantesca quantidade de dados coletados por usuários em plataformas digitais, Lev Manovich (2017) comenta sobre a influência dessa prática de coleta, armazenamento e uso de dados em nossa cultura. Pois não basta somente “saber ler” os códigos de programação por trás de grandes iniciativas e listar esses códigos, mas devemos observar como eles atuam em cada sessão de internet particular, do usuário, para que os pesquisadores sejam capazes de realizar questionamentos a respeito de *softwares* que estão “dominando” o espaço social. Um exemplo disso é um projeto do autor em que são agrupados, em poucos padrões, mais de 2,3 milhões de *posts*/fotos de 13 cidades do mundo no aplicativo Instagram (pertencente a Meta). Ou seja, a grande quantidade de imagens postadas respeita padrões de poucos filtros agrupados, o que faz Manovich (2017, p. 23) questionar “como o software que usamos influencia o que expressamos e imaginamos?” ao mantermos acesso aos dados restritos aos seus *softwares* de coleta,

As redes sociais e suas empresas disponibilizam certas informações para seus usuários armazenados em interações de visitantes em páginas, blogs ou contas de suas empresas, e também fornecem visualizações interativas para ajudar as pessoas a saber quais são as questões publicadas mais populares e de onde vêm seus visitantes. No entanto, as empresas geralmente mantêm mais registros detalhados para eles próprios. Portanto, se você é um dos poucos sociólogos e especialistas que trabalham dentro de um gigante como o Facebook ou o Google, você terá uma enorme vantagem sobre seus colegas da academia. Você pode fazer perguntas que outras pessoas não podem. Isso pode criar uma lacuna real no futuro entre pesquisadores acadêmicos e corporativos. Enquanto este último será capaz de analisar padrões culturais e sociais em ambos os níveis supermicro como supermacro, o primeiro terá uma “lente” normal, que não pode ser chegar perto demais ou chegar longe o suficiente para uma visão planetária. Quem se beneficia da análise das atividades culturais de centenas de milhões de pessoas? O posicionamento automático de anúncios nas redes do Google, Facebook ou Twitter já usa tanto os textos dos posts dos usuários quanto os e-mails e outros dados, mas saiba como centenas de milhões de pessoas interagem com imagens e vídeos em redes sociais não serve apenas para anunciantes para posicionar melhor sua publicidade visual. Mas para os acadêmicos perguntar; podemos analisar o código de programas de software? Não é tão simples como você pode pensar. O código em si é “big data” (MANOVICH, 2017, p. 23).

Manovich (2017) comenta que essa construção permanente, nas tecnologias digitais, requer uma nova maneira de analisar as mídias e a cultura, e, conseqüentemente, devemos focar nosso olhar para a pesquisa em dados. “Em outras palavras, precisamos pensar em como representar adequadamente ‘atos de software’ como dados” (MANOVICH, 2017, p. 22). O autor diz que há uma tendência de investimentos em pesquisa de grandes empresas para

entender como experiências sociais podem ser mediadas por um *software*, e se faz necessário desenvolver um método próprio de análise das experiências interativas dos usuários, coincidentemente ao encontro do que Shoshana Zuboff (2020) comenta sobre a informação e o conhecimento estarem nas mãos de grandes empresas de tecnologia, e, conseqüentemente, o poder, configurando o capitalismo de vigilância.

De forma complementar, a discussão sobre segurança e privacidade dos dados dos usuários é tema de discussão há anos na *International Telecommunication Union*, como retrata a reflexão publicada na edição de abril de 2005 acerca do *paper* intitulado *Privacy and Ubiquitous Network Societies*, redigido pelo Prof. Dr. Gordon A. Grow, do Departamento de Mídias e Comunicação da *London School of Economics and Political Science*. De acordo com a definição proposta, existe um paradoxo no *design* de dispositivos e redes, contribuindo para uma relação de não transparência com a coleta e uso de dados em sistemas que acabam por ser “invisíveis” aos usuários desses ambientes,

A privacidade é uma questão central na visão da computação ubíqua e foi identificada como tal desde seus primeiro começo. Muitos na comunidade de pesquisa e desenvolvimento reconhecem claramente o desafio inerente que um sistema invisível, intuitivo e penetrante de computadores em rede vale para as normas sociais atuais e valores relativos à privacidade e vigilância<sup>28</sup> (GROW, 2005, p. 6, tradução nossa).

É compreensível que a preocupação com a privacidade dos cidadãos esteja pautada paralelamente à popularização da conexão em rede, ou principalmente desde os anos 2000, que essa temática ganha cada vez mais espaço em debates acerca de tecnologia e comunicação. No *paper* de Grow (2005), há indícios de que o “avanço” tecnológico iria se dar em ferramentas e *softwares* com leitura biométrica, reconhecimento facial, etiquetas *Radio Frequency Identification* (RFID), *chips* implantados em dispositivos que são lidos mesmo a distância, por exemplo. Todo esse arsenal, associado às mídias, monitoramento e vigilância que se fez presente em nosso cotidiano conectado, auxilia a construir a ideia de que estamos vivendo numa sociedade cada vez mais *insegura*. Conforme mencionado na introdução de nossa tese, a visão sugerida por Lemos (2009, p. 626), que a partir das mídias locativas “[...] parece mostrar a cultura do medo e da insegurança: medo da deriva e da desorientação transformada em uma ação racionalizante de tudo indexar, etiquetar e reconhecer no espaço”.

---

<sup>28</sup> “Privacy is a central issue in ubiquitous computing vision and has been identified as such from its earliest inception. Many in the research and development community clearly recognize the inherent challenge that an invisible, intuitive and pervasive system of networked computers holds for current social norms and values concerning privacy and surveillance.”

A sensação de monitoramento constante, a partir de câmeras de vigilância nas ruas, nos elevadores, nos ambientes externos e internos que frequentamos, demonstram o que Lemos (2009) chama de construção de um sujeito inseguro, pois basta a instalação de câmeras ou a sinalização “sorria, você está sendo filmado”, ou “este ambiente está sendo monitorado”, para criar uma cultura do medo e de vulnerabilidade entre os cidadãos. Conforme cita o autor, a câmera estabelece um conceito de criminalidade, assumindo três pontos importantes sobre a construção do sujeito inseguro,

A câmera estimula, por um lado, uma reação positiva, produzindo a ideia de que há um problema de segurança no lugar e que ela vai resolver. Por outro, ela cria uma sensação e medo e de insegurança temporal, no passado, no presente e no futuro: em relação ao presente porque a simples introdução do dispositivo traz a ideia de que “algo acontece aqui”, em relação ao passado pois “algo poderia ter acontecido” e em relação ao futuro pois “algo pode acontecer” (LEMOS, 2009, p. 627).

Se a possível presença da câmera é responsável pelo estímulo da sensação de insegurança nos cidadãos, podemos fazer uma relação com o dispositivo panóptico de Foucault (1983), conforme mencionamos anteriormente, onde a vigilância permanente é responsável por instaurar o medo social, e, portanto, a obediência por temor da consequência. As câmeras e sistemas de monitoramento invisíveis, como geolocalização, *smartphones* e mídias locativas, por exemplo, aumentam a sensação de insegurança e provocam paranoia, como propôs Chun (2006), sugerindo uma nova forma de controle e poder. Lemos (2009, p. 628) complementa esse pensamento ao dizer que “os sujeitos incivilizados cresceram e ganharam novas formas e propriedades mais performáticas, já que agora são dotados de memória em banco de dados, mobilidade em redes telemáticas e fácil localização”.

De forma complementar, Lemos (2009, p. 629) diz que o “sujeito inseguro” tem consciência da utopia de segurança das câmeras de vigilância, “sabe que elas geram medo e intolerância e que, ao invés de resolver o problema, elas só o agravam, produzindo mais sentimento de insegurança”. Podemos chamar por cultura da insegurança, pois, ao invés de promover a sensação de proteção, acaba por carregar em formas visíveis e invisíveis de controle, promovendo a invasão de privacidade, estimulando o anonimato e o segredo, distribuindo a capacidade de vigiar (e de ser vigiado) para o cidadão.

Nesse sentido, as mídias locativas carregam a responsabilidade tanto por dar a falsa sensação de liberdade, de movimento e de poder ao usuário, quando paralelamente retroalimentam uma sociedade do controle e do monitoramento, quando se renuncia à liberdade para se viver conectado. A mobilidade “prometida” pelas mídias locativas, na verdade, pode também ser encarada como uma forma de controle tão perversa que renuncia o



confinamento, quando a verdadeira clausura é invisível, está nas entranhas do *big data*. Conforme propõe Lemos (2009, p. 629) “a sociedade do controle está em toda parte. Para além do que vigia o confinado, as *panopticom* – atuais câmeras de vigilância, cartões com chips, perfis na internet, GPS e sensores, controlam o sujeito ‘inseguro’ em sua mobilidade cada vez maior”. Nesse sentido, Lemos (2009, p. 638) sintetiza sobre a

[...] faceta da sociedade de controle: uma vigilância sutil, difusa, deixando o usuário com a sensação de liberdade de produção de informação e de mobilidade. Os exemplos com as câmeras de vigilância, as multisenhas bancárias, os life-loggs, as redes sociais móveis, as etiquetas RFID e os celulares com redes mostram que a computação ubíqua, bluetooth que a internet das coisas com suas tecnologias, redes e sensores eletrônicos transformam a vigilância panóptica em um controle invisível, modular e distribuído, ao mesmo tempo em todos e em nenhum lugar.

Portanto, para avançarmos na compreensão sobre como nosso objeto empírico apresenta suas políticas de privacidade, segurança e coleta de informações de seus usuários (*in*)seguros, o próximo capítulo, é dedicado à apresentação de nosso itinerário metodológico e do FB, onde vamos contextualizar seu surgimento e apresentar a plataforma construída por uma perspectiva da arquitetura que promove constantemente a confiança do usuário. A partir dessa reflexão é que preparamos o nosso terreno para posteriormente realizarmos o ato de “sujar as mãos” com o objeto empírico e dar a ver as atualizações dos sentidos de *tecnosegurança* pela ambiência FB.

### 3 METODOLOGIA

Este capítulo apresenta a proposta de metodologia adotada em nossa tese, levando em consideração um “arranjo” de iniciativas que acreditamos ter dado conta da problemática de nosso objeto. Nossas motivações dão a ver uma espécie de conjunto de estruturas fundamentadas em autores e conceitos que acreditamos nos auxiliar a irmos ao encontro de respostas para nossas inquietações e nos provocam a refletirmos a partir de novos questionamentos. É claro que, muitas dessas iniciativas foram experimentações que estamos fazendo desde o ingresso no Grupo de Pesquisa TCAv, investigando nosso objeto empírico com “lentes” de autores e alguns *modus operandi* para trabalharmos com nossos objetos da linha de pesquisa. A principal iniciativa, que já apresentamos na introdução da nossa tese, dedicada ao exercício de problematização da pesquisa, é a fenomenologia bergsoniana, e que nos alicerçamos no conceito de tempo.

Assumimos a **Intuição** como método, ancorada também em outras três perspectivas: a **Cartografia**, realizada através do movimento do *flâneur* e na posterior constelação benjaminiana (dando a ver coleções criadas com base em afinidades eletivas que emergem de nossos observáveis), o movimento de escavação que auxiliou a explorar algumas das interfaces de nossa empiria, e, por fim, a **Metodologia das Molduras** para dissecar as interfaces (KILPP, 2010, p. 26), “procedimento que está baseado em movimentos como a própria cartografia, aliada à intuição, cartografia, desconstrução e dissecação”. Entendemos que há um sentido durante do audiovisual, desde a análise do objeto, como virtualidade, caracterizando uma tendência que se atualiza nas materialidades selecionadas para nossa tese, a partir do FB. Portanto, vamos explorar os principais conceitos metodológicos e autores na primeira etapa do presente capítulo, construindo uma espécie de itinerário conceitual e metodológico para auxiliar a refletirmos *como* olhar nossas materialidades em um movimento demandado pelo próprio objeto.

#### 3.1 Itinerário metodológico

A concepção de Henri Bergson (2006c, p. 6) sobre as coisas e sobre a evolução é crítica frente àquela forma matemática como medimos o tempo, mas sobre a evolução do real de uma constante maneira de durar, ele resume “quando falamos do tempo, pensamos na medida da duração, e não na própria duração. Mas essa duração, que a ciência elimina, que é difícil de ser concebida e expressa, sentimo-la e vivemo-la”. Para o autor, não há como

tratarmos tempo e espaço, ou memória e matéria no mesmo plano, como coisas que pertencem ao mesmo gênero. Para ele, pensarmos em duração, é memória, é virtual, é “uma continuidade indivisível” (BERGSON, 2006c, p. 8), portanto, não existe como medir ou calcular a duração, mas podemos pensar em duração como atualização, algo em constante movimento, que faz parte de “outra coisa”.

Pensarmos em duração é compreendermos que o tempo é indivisível, não fragmentado ou medido, já que a “ciência da duração é fluir e que o estável acostado ao estável não resultará nunca em algo que dura”, mas de uma “mudança sempre aderente a si mesma numa duração que se alonga sem fim” (BERGSON, 2006c, p. 8-9).

Digamos, portanto, que na duração, considerada como uma evolução criadora, há criação perpétua de possibilidade e não apenas de realidade. Muitos repugnarão admiti-lo, por julgarem sempre que um acontecimento não se teria realizado se não tivesse podido realizar-se; de modo que, antes de ser real, é preciso que ele tenha sido possível (BERGSON, 2006c, p. 15).

Utilizando o exemplo das cores, onde o autor comenta sobre a junção dos tons amarelo e vermelho, dando origem ao alaranjado, significa, resumidamente que nessa nova criação, existe em duração ainda sua origem, o amarelo e o vermelho. Porém, isso não quer dizer que o alaranjado deixa de ser menos ou mais que as cores que lhe deram origem, mas algo que se atualiza, que existe virtualmente, o tom alaranjado, a evolução criadora. Conforme Bergson (2006c, p. 23) na ideia de tempo, implica compreendermos que “o passado se contrai no presente – ao plano do sonho, no qual se desdobra, indivisível e indestrutível, a totalidade do passado”. É indivisível, já que a ciência da duração é fluir. Na introdução da obra que estamos citando, *O pensamento e o movente*, Bergson (2006c, p. 27) organiza a proposta do método da intuição tendo o conceito de duração como centro, pois afirma que “essas considerações iniciais sobre a duração nos pareciam decisivas. Gradualmente, fizeram-nos erigir a intuição em método filosófico”.

Dessa forma, ao compreendermos a intuição como método que estamos adotando ao deixar “ser olhado” por nosso objeto de pesquisa, e, ao flunar pelas interfaces de nossa empiria, entendemos que havia algo que nos inquietava e que **durava** nesses movimentos de descoberta pelo FB e em suas “zonas paralelas”, como as interfaces coletadas e apresentadas na introdução dessa tese, assim como as manifestações *tecnoculturais* mencionadas. Nesse sentido, é relevante trazermos a proposta de Bergson (2006c) pois critica a ciência positivista, cartesiana, que dá o enfoque ao materialismo e que opera sobre um dualismo das coisas, espírito x matéria, onde cada parte apresentaria seu próprio “real”.

Conforme propõe Benjamin (2015, p. 134) “a acreditar em Bergson, é a presentificação da *durée* que liberta a alma humana da obsessão do tempo”, mas essa ideia imobiliza os objetos e relativiza o real em matéria **ou** espírito, renunciando o conjunto, como experiência mista, é nesse sentido que a duração para Bergson é a experiência, a dependência de espírito **com** matéria. Nas palavras do autor é “como se a coisa e a ideia da coisa, sua realidade, e sua possibilidade não fossem criadas ao mesmo tempo quando se trata de uma forma verdadeiramente nova, inventada pela arte ou pela natureza” (BERGSON, 2006c, p. 17).

Outro pensador que desenvolveu muitas reflexões a partir de Bergson, foi Gilles Deleuze, e, em sua obra *Bergsonismo* (1999), explica detalhadamente o método da intuição, suas etapas e como operar em diversos objetos. Deleuze (1999, p. 131) faz a relação da dualidade atual e virtual, como o misto de Bergson (conforme já apresentamos na construção do problema), e afirma que “a intuição aparece como um verdadeiro método de divisão: ela divide o misto em duas tendências que diferem de natureza”. Portanto, nesse sentido, podemos verificar que matéria e duração são coisas que não diferem de grau, mas são “dois movimentos, duas tendências, como a distensão e contração” (DELEUZE, 1999, p. 131), diferem de natureza *como* tendência. Em outra obra, *Memória e vida*, Bergson (2006a, p. 47) afirma que a duração

é o progresso contínuo do passado que rói o porvir e incha à medida que avança. Uma vez que o passado cresce incessantemente, também se conserva indefinidamente. A memória... não é uma faculdade de classificar recordações numa gaveta ou de inscrevê-las num registro [...] na verdade, o passado se conserva por si mesmo, automaticamente.

É importante para nossa reflexão sobre o objeto de nossa tese, compreendermos que a duração é indivisível, imensurável, mas que tem característica própria na atualização, uma mudança sem cessar, portanto, um instante dura no outro, num *continuum* que se diferencia constantemente de si mesmo. Ao olharmos as imagens de nosso objeto, compreendemos que o que dura, se atualiza nas materialidades observadas, é o sentido de segurança nas interfaces da plataforma FB. Vamos explorar na análise, a partir das imagens das interfaces, autenticar esses sentidos de segurança, atualizados em diversas manifestações na matéria de nosso objeto empírico.

Com ênfase nessa concepção de tempo e memória mais do sentido de sucessão do que de sobreposição, e que a partir desse fenômeno o que se diferencia em função do tempo, não do espaço, se contrai e se distende no tempo real (BERGSON, 2006a) é que o autor traz o

conceito de *memória*, o qual relacionamos com a proposta de outro pensador-chave para nossa problematização do objeto, Walter Benjamin (2006, p. 349), que inclusive, traz referência à Bergson na seguinte citação na obra *Passagens*:

Ao final de *Matière et Mémoire*, Bergson desenvolve a ideia de que a percepção é uma função do tempo. Poder-se-ia dizer que, se vivêssemos segundo um outro ritmo – mais serenos diante de certas coisas, mais rápidos diante de outras –, não existiria para nós nada “duradouro”, mas tudo se desenrolaria diante de nossos olhos, tudo viria de encontro a nós.

Para aprofundar a reflexão acerca de Benjamin e o conceito de memória, Santos (2003, p. 115) publicou, em sua obra *Memória coletiva e Teoria Social*, um relato sobre o pensador alemão, dedicando o debate na visão dele sobre a história. Para Benjamin, o cartesianismo e a linearidade representavam uma visão restrita sobre tempo e memória,

A compreensão de Benjamin da história associou-se a conceitos muito próprios, como imagens dialéticas, alegoria e crítica redentora [...] as ideias de evolução e progresso tiveram nele um crítico consistente capaz de apontar todos os usos, manipulações e perigos dela decorrentes.

A proposta de Benjamin, ao criticar a ciência positivista é defender que o tempo pode ser *ahistórico*, e, nesse sentido, faz uma apropriação de colocar a imagem no centro desse pensamento, a imagem dialética. Ao encontro de Bergson, aonde vimos que o tempo em sua realidade movente caracteriza a duração, para Benjamin (2013, p. 57), “a unicidade e duração estão tão unidos nesta, quanto transitoriedade e repetibilidade naquela”, ou seja, o autor propõe que seja refletido sobre a imagem, e especificamente a obra de arte, contendo no tempo o aqui e o agora, um instante que dura, sua aura. “Mas o que é a aura, de fato? Uma trama peculiar de espaço e tempo: a aparição única de uma distância, por mais próxima que esteja” (BENJAMIN, 2013, p. 57). No livro *A obra de arte na era de sua reprodutibilidade técnica*, Walter Benjamin (2013, p. 54) condena o caráter reprodutível da indústria cultural, alegando que o fator mercantil e de distribuição massiva produzem o aniquilamento dessa experiência única de tempo,

mesmo na reprodução mais perfeita *uma coisa* se perde: o aqui e o agora da obra de arte – sua existência única no local em que se encontra. No entanto, é essa existência única, e somente nela, que está realizada a história à qual a obra de arte esteve submetida no decorrer de sua duração.

Segundo o autor, a experiência de estar em frente a uma obra de arte única, que contém seu aqui e agora, sua aura, acaba por atrofiar na era da reprodutibilidade técnica, já

que preconiza a massificação e a reprodução por conta da monetização. Na visão de Benjamin (2013, p. 58), a perda da autenticidade da obra de arte se esvai com toda sua multiplicação, pois é “decisivamente significativo que esse modo de ser aurático da obra de arte jamais se liberte totalmente de sua função ritual. Em outras palavras o valor singular da obra de arte “autêntica” fundamenta-se sempre no ritual”.

Portanto, a proposta de Benjamin é fundamental para se compreender a ideia de *tempo* e seus anacronismos, não linearidade e, conseqüentemente, podemos dizer que a memória e o passado sobrevivem em si, dialogando com o conceito de duração de Henri Bergson. “Porque essa sobrevivência mesma é a duração, a duração é em si memória. Bergson, nos mostra que a lembrança não é a representação de alguma coisa que foi, o passado é isso em que nós nos colocamos de súbito para nos lembrar” (DELEUZE, 1999, p. 135). De forma complementar, Benjamin comenta sobre a intuição de Bergson como proposta filosófica estruturada a partir da experiência da biologia, rejeitando uma determinação histórica:

O título mostra que a estrutura da memória é por ele considerada como decisiva para a estrutura filosófica da experiência. De fato, a experiência é matéria da tradição, na vida coletiva como na privada. Constitui-se menos a partir de dados isolados rigorosamente fixados na memória, e mais a partir de dados acumulados, muitas vezes não conscientes, que afluem à memória (BENJAMIN, 2015, p. 107).

No sentido de refletir sobre a memória e tempo, o pesquisador francês Georges Didi-Huberman (1998, p. 148) reforça a proposta de Walter Benjamin para a perspectiva metodológica sobre o aqui e agora *das imagens*, para ele “o objeto aurático supõe assim uma forma de varredura ou de ir e vir incessante, uma forma de heurística no qual as distâncias contraditórias – se experimentariam umas às outras, dialeticamente”. Para o ele, há um segundo aspecto da aura, que está dedicado ao “poder do olhar atribuído ao próprio olhado pelo olhante: ‘isto me olha’” (DIDI-HUBERMAN, 1998, p. 148).

Compreendemos que olhar as atualizações do tempo de nosso objeto, em materialidades, como as interfaces do FB demanda perceber o que “nos olha” nessas imagens para perceber a memória contida nelas. Para isso, nos apoiamos fortemente em conceitos como o da imagem dialética de Benjamin (2006) e na releitura metodológica de Didi-Huberman (1998) para contextualizarmos a memória e o imaginário contido nessas imagens.

Para fazer esse movimento, de olhar a imagem dialética e crítica, e perceber o devir que ela contém, é necessário recorrer novamente à Benjamin para a noção de evolução e a relação com o historicismo, pois, conforme sua visão, o cerne não está no conceito de progresso, mas sim de **atualização**. O autor reforça que a noção de historicidade, assim como

propõe Didi-Huberman (1998) posteriormente, que envolve os anacronismos, temporalidades contraditórias que colocam em choque essas memórias, pensamento também à defesa de Gilles Deleuze (1999, p. 135) sobre tempo, já que “o passado não se constitui depois de ter sido presente, ele coexiste consigo como presente”.

A primeira etapa desse caminho será aplicar a história o princípio de montagem. Isto é: erguer as grandes construções a partir de elementos minúsculos, recortados com clareza e precisão. E, mesmo, descobrir na análise do pequeno momento individual o cristal do acontecimento total. Portanto, romper com o naturalismo histórico vulgar. Aprender a construção da história como tal (BENJAMIN, 2006, p. 703).

Ao encontro dessa proposta, Didi-Huberman (2015), no livro *Diante do tempo*, defende a história da arte como disciplina anacrônica, e propõe que seja compreendida a partir das imagens, pois remete a uma nova estratégia de montagem do tempo, que reside na proposta central da imagem dialética. Portanto, a ideia de tomar as coisas a *contrapelo* (termo utilizado originalmente por Walter Benjamin, na obra *Origem do drama barroco alemão*, de 1984, é assumida em nossa tese, ao propormos olhar para as imagens e perceber sua própria historicidade, sentidos e imaginários, isso implica em compreender a história a partir dos anacronismos, fugindo da teoria positivista e linear de compreender os fatos, e encontra uma perspectiva diferente daquela tida socialmente como “correta”, aceita ou vencedora.

Essa maneira vai ao encontro de outra visão sobre o tempo, e conseqüentemente as mídias, ambiente desse estudo, que provoca e instiga tomarmos determinados caminhos alternativos para compreender alguns fenômenos. Estamos nos referindo a voltarmos o olhar também para aquilo que estamos chamando de “cacos” ou os resíduos, como aqueles objetos ou materiais que pelo cartesianismo seriam descartados, ou seja, as interfaces da empiria que não são valorizadas para monetização da plataforma, ou espaço para interação dos usuários com sua rede de contatos dentro do FB. Seriam zonas intencionalmente negligenciadas pela plataforma, por não se tratar de um espaço de interação e rentabilidade via anúncios publicitários.

Essa perspectiva, de nossa tese, nos provoca a olhar para algo que compreendemos ao longo de nosso flamar pela plataforma FB, seria menos importante comercialmente, menos relevante para reter a atenção do usuário, uma espécie de resíduo de informação, fragmentos intencionalmente deixados para trás pela plataforma, conteúdos que deveriam receber a mínima atenção do usuário. As materialidades que iremos explorar dão a ver justamente a possibilidade de se encontrar “algo de novo no velho”, ideia que está baseada na proposta

arqueológica do tempo, ou na vertente designada como arqueologia da mídia, que tem origem em Michel Foucault (1972), na obra *Arqueologia do saber*.

O pensamento arqueológico nos acompanha em toda a tese, visto que propõe uma visão sobre o tempo que tensiona as diversas temporalidades das imagens, partindo de sua historicidade própria renunciando à noção linear e progressiva de analisar os “sucessos”, mas recorrendo a descontinuidades e retornos, conteúdos que, a partir do *design* da interface do FB, poderiam ser “menosprezados” pelos usuários e parceiros comerciais, e descartados, já que não apresentam o mínimo de incentivo para permanência na página, como os termos de uso de contratos firmados com a plataforma e o usuário final, ou o que estamos chamando de “pergaminhos” das políticas de privacidade e segurança da conta. São ambientes onde não há recurso para interação com o usuário, apenas textos associados à regulamentação das práticas de uso, geralmente acompanhados por explicações extensas, com linguagem pouco atraente ou acessível à compreensão do usuário. Conforme será apresentado no Capítulo 4, esses espaços também se caracterizam por ser pouco atraentes em termos de recursos de cores e ilustrações.

Acreditamos que esses espaços são tanto mascarados como menosprezados para, justamente, não reter atenção, sem estímulo visual para que o usuário permaneça ali. Iremos explorar melhor esses materiais a partir de um movimento de escavação, pois buscamos intencionalmente ver essas interfaces, “revolver a terra” nesses ambientes para preparar os materiais para a intervenção da dissecação das imagens.

Para desencavar as audiovisualidades, presentes nas interfaces do FB, vamos ao encontro da proposta de Siegfried Zielinski, no seu livro chamado de *Tempo profundo das mídias*<sup>1</sup> (2006, p. 11, tradução nossa), sobre a vertente que designa a chamada arqueologia da mídia em que “Trata-se de desvelar no registro médio-arqueológico momentos dinâmicos que abundam em heterogeneidade e, desse modo, entrar em uma relação de tensão com os vários momentos do tempo presente, relativizá-los e torná-los mais decisivos”, através da perspectiva da memória das imagens, como convidam Didi-Huberman, Chéroux e Arnaldo (2013), a partir da imagem dialética. A busca por conteúdos *soterrados*, descartados ou negligenciados pela lógica evolucionista das mídias, acompanha a crítica de Zielinski (2006), quanto à ideia de progresso tecnológico contínuo, pois os historicistas deveriam ir em busca de variações, na direção contrária à tendência progressiva na história da mídia. O teórico ainda promove a associação com a evolução da Terra, já que foi um processo dinâmico com

---

<sup>1</sup> “Deep Time of Media - Toward an Archaeology of Hearing and Seeing by Technical Means.”



ciclo de variações e de erosões repetidas, aproximando-se da noção mais *anarqueológica* que recusa um ponto inicial fixo.

A passagem dos séculos apenas aprimora e aperfeiçoa as grandes ideias arcaicas. Esse ponto de vista constitui pedagogia primitiva, que é maçante, e suga a energia do trabalho relativo às mudanças tão desesperadamente necessárias. Então, se deliberadamente alterarmos a ênfase, virarmos de ponta-cabeça e experimentarmos, o resultado vale a pena: não procuremos o velho no novo, mas encontremos algo de novo no velho<sup>2</sup> (ZIELINSKI, 2006, p. 19, tradução nossa).

Concomitantemente, é importante salientarmos que reconhecemos que McLuhan (1964) já trazia a visão arqueológica dos meios, conforme explicitamos anteriormente nessa tese. A proposta ora formulada como leis das mídias, ora formulada como explorações, defende uma genealogia dos meios, já que cada “nova” mídia amplia alguma coisa e se recuperam relações. A interdependência total é o fato inicial, onde todas as coisas são interdependentes, ou seja, há ecologia em um movimento infinito. Nas palavras do pesquisador alemão Friedrich A. Kittler (2019, p. 22), em seu livro *Gramofone, filme typewriter*, o autor faz uma arqueologia desses três dispositivos tecnológicos, e afirma que “o saber absoluto sobre as mídias corre em *loop* infinito”. A arqueologia da mídia e sua provocação, em relação ao tempo, não apresenta um método fechado com regras indicativas de como operar nossos objetos, mas, conforme Fischer (2015, p. 84), traz uma variedade de apropriações, advertindo para “a ideia de método como invenção, mas também serve de alerta para não deixarmos nosso foco nas autenticações de audiovisualidades se perder”.

Paralelo a visão de tempo proposta pela arqueologia da mídia, o historiador francês Pierre Nora (1993, p. 21), questiona a perspectiva cronológica e linear dos fatos por trabalhar com a ideia de “[...] lugares de memória, uma ação registradora, que delega ao arquivo o cuidado de se lembrar por ela”. Nesse sentido, entendemos que as imagens são esses “lugares” e, algumas, até restos que carregam em seu devir diversas temporalidades anacrônicas mas que se atualizam em sua matéria. Nessa visão, há forte diálogo com o conceito de imagem dialética de Benjamin, conforme mencionam Santaella e Ribeiro (2017, p. 71):

A imagem dialética é aquela que surge pela percepção consciente (cognoscível) de um anacronismo. Ou, em outras palavras, ela surge quando um escavador da cultura (que poderia ser, por exemplo, um pesquisador da área de comunicação ou um

---

<sup>2</sup> “Past centuries were there only to polish and perfect the great archaic ideas. This view is primitive pedagogy that is boring and saps the energy to work for the changes that are so desperately needed. Now, if we deliberately alter the emphasis, turn it around, and experiment, the result is worthwhile: do not seek the old in the new, but find something new in the old.”

estudioso de história da arte) encontra marcas reveladoras de um passado adormecido em um fragmento residual inesperado. Esse encontro desconcertante é potencialmente capaz de ressignificar o próprio presente, conduzindo-o a novos patamares de conhecimento.

De maneira complementar à proposta arqueológica, conforme mencionado em outros momentos do texto, na exploração das materialidades realizamos uma *flânerie* pelo FB e pela *web*, não impondo limites, percurso pré-definido ou destino, mas, olhando a plataforma e recolhendo as imagens das capturas de telas da interface sem regras específicas. Fomos experimentando o *software* e deixando-o conduzir nosso percurso. Esse movimento de perambular pela plataforma foi responsável por nos permitir recolher diversas telas, ora aquelas que nos chamavam mais a atenção, seja pela lógica da rede social ao indicar um conteúdo atraente aos nossos interesses no momento, ora para imagens que fomos guardando no sentido de nada perder e deixar passar, sem seleção prévia ou hierarquia. Flanando pela plataforma fomos armazenando, em nosso computador pessoal, em um arquivo, somente as imagens, numa apresentação do programa Microsoft Power Point.

Ao colher essas telas, fomos olhando para nossas capturas em movimentos distintos, algumas, em determinado momento, achávamos que não estariam nos auxiliando em obter respostas para o questionamento da pesquisa, mas armazenamos mesmo assim, outras nos instigavam determinados aspectos sobre nossa tese e foram reorganizadas em outro arquivo de pré-seleção como “meu Facebook”, “do Facebook”. Esses cacos e fragmentos que encontramos e guardamos não foi um ato ingênuo, mas inspirado no movimento do *trapeiro* de Walter Benjamin (2018, p. 502), ao olhar para os resíduos, aqueles trapos que são deixados para trás e que são descartados nas ruas, “porém, os farrapos, os resíduos: não quero inventariá-los, e sim, fazer-lhes justiça da única maneira possível: utilizando-os”. Conforme descreve Kilpp (2010, p. 118, grifos da autora),

O *flâneur* foi personagem de Baudelaire, apropriado por Benjamin para pensar e referir um modo peculiar de agir de certos sujeitos modernos em relação às passagens parisienses do século XVIII. Esse modo de agir, hoje, vem sendo apropriado por pesquisadores contemporâneos para interpretar, por exemplo, os modos do usuário de internet vagar na *web*. A partir deles se criou, por exemplo, o conceito de *webflaneuria*.

Nos apropriamos da proposta do *flâneur*, de Benjamin, para percorrer as interfaces e coletar registros de nosso percurso tentando compreendê-los posteriormente ao criarmos possíveis **coleções** de imagens resgatadas da *web*. “A coleção é uma forma mais específica de

ajuntamento, por incluir itens que mantêm necessariamente uma relação entre si, dado que são objetos da mesma natureza ou de características afins” (MACIEL, 2009, p. 30).

Esse grupo de capturas de telas, que fomos tirando do fluxo da *web* para posterior análise, foi demandando, conforme o avanço de nossa tese em problematizar e exercitar nosso olhar sobre o objeto, agrupar ou classificar esses materiais conforme fomos percebendo algumas especificidades no material empírico. Portanto, sabemos que, ao optarmos por fazer essa espécie de agrupamento, exige algo que, por natureza, seja excluído. Assim, a proposta de Maria Esther Maciel (2009) pareceu-nos relevante para auxiliar nosso movimento de seleção das imagens, já que a autora mostra as ironias das lógicas de classificação e seleção em diversos atos, como, por exemplo, a escrita, a lista, a coleção e o inventário. Dessa maneira, mostraremos como ordenamos nossas coletas num critério provisório, “um modelo que não se presta, como o do dicionário, à impossível função de hierarquizar de modo único e incontroverso as marcas semânticas, as propriedades, os semas, mas incorpora o próprio formato incontrolável daquilo que busca mapear e catalogar” (MACIEL, 2009, p. 24).

Ao inserirmos o ato de colecionar em nosso *itinerário metodológico*, sabemos que estamos realizando uma atividade inspirada no próprio *flâneur* de Benjamin (2018), o colecionador, que enfrenta a dispersão, “visto que o colecionador ao registrar/catalogar as coisas, retira-as do estado dispersivo em que se encontram no mundo e as recontextualiza num outro espaço, regido por leis próprias” (MACIEL, 2009, p. 26). Compreendemos, a partir de Maciel (2009, p. 27), que o colecionismo “é um ato complexo”, pois tende a “criar suas próprias regras e princípios, de acordo com as inquietações e obsessões do colecionador, sobretudo quando o valor afetivo ou estético predomina”. E “Graças a sua potencialidade de recolher as coisas e salvá-las da dispersão através do deslocamento, ela assume inclusive uma função de arquivo, de dimensão memorialística, convertendo-se numa espécie de antídoto contra o esquecimento” (MACIEL, 2009, p. 28).

A criação das coleções, nos permite compreender que faz parte de nosso processo de operação do objeto criarmos uma espécie de mapa de nosso percurso, compreendermos o caminho para mapearmos os sentidos de segurança no FB. Já a cartografia, é a ciência dos mapas proveniente do termo grego composto pela junção da etimologia **mapa** + **grafia** e, conforme explicam Deleuze e Guattari (1995, p. 22), “o mapa é aberto, é conectável em todas as suas dimensões, desmontável, reversível, suscetível de receber modificações constantemente”. Com a intenção de reconhecer afinidades eletivas entre estrelas, através de um movimento como *flâneur*, para realizar assim uma constelação e para que, com isso, surja “[...] o senso luminoso do conhecimento” (CANEVACCI, 1997, p. 106).

Após agrupar nossa coleção de imagens que possibilitam cartografar nossa *flânerie*, é que acreditamos ser possível criar as constelações, novamente com inspiração benjaminiana, onde são conjuntos, agrupamentos de imagens, ou estrelas quando um traçado comum as reúne e a constelação cria construções aproximadas por afinidades eletivas. Ainda, com a metáfora das estrelas “[...] que brilharam mais do que as outras”, “Da constelação é possível deduzir a trama que liga os fatos empíricos [...]” (CANEVACCI, 1997, p. 113). Mas, para chegar a constelar, nosso itinerário metodológico demanda a dissecação das interfaces a partir da Metodologia das Molduras sob a proposta realizada por Suzana Kilpp (2010, p. 28) para

Matar o fluxo, desnaturalizar a espetação, intervir cirurgicamente nos materiais plásticos e narrativos, cartografar as molduras sobrepostas em cada panorama, e verificar quais são e como elas estão agindo umas sobre as outras, reforçando-se ou produzindo tensões no agenciamento de sentidos.

A metodologia das molduras, conforme Kilpp (2010, p. 26) trata de “um conjunto de procedimentos de análise das audiovisualidades, que são articulados por uma conjunção de referências teórico-metodológicas [...] articula intuição, cartografias, desconstrução e dissecação” para tentar **autenticar** as *ethicidades* atualizadas em molduras. A metodologia opera a partir de três eixos principais, sendo eles: as *ethicidades*; as molduras/moldurações e emolduramentos; e os imaginários. Dessa maneira, a metodologia, segundo sua autora, “ensaia procedimentos de três ordens: a técnica, a discursiva e a cultural, que são exatamente relativas às três dimensões das audiovisualidades” (KILPP, 2010, p. 26). Ao utilizar o verbo **autenticar**, ela comenta que são maneiras de legitimar características que o pesquisador percebe no objeto desde o movimento de investigação.

Já o movimento de dissecar as imagens, especificamente as interfaces, como no caso de nosso objeto, está inspirado no ato de dissecar cadáveres de Leonardo Da Vinci, e significa “um procedimento de ordem técnica que desdiscretiza digitalmente a imagem técnica audiovisual, que é sempre discreta em qualquer suporte” (KILPP, 2010, p. 29). Dessa forma, ao interceder na empiria, a dissecação auxilia a visualizar os diversos efeitos praticados que produzem sentidos a partir das molduras.

De maneira complementar, Fischer (2012) comenta sobre a prática da dissecação, inspirada na pesquisa de Kilpp, cuja materialidade originalmente são imagens de TV, mas adotada para outro suporte, as interfaces *web*. O autor encontra um diálogo com a proposta de Erkki Huhtamo e Parikka (2011) de como essa interferência nas interfaces se aproxima do movimento de escavação, inspirado na proposta da arqueologia da mídia:

Há, nitidamente, no nosso ver, uma forma de encontrar no papel de *dissecador* das interfaces *web* um movimento que vai ao encontro do que Huhtamo menciona como o objetivo da arqueologia da mídia de realizar a **escavação** das formas e formulações discursivas inscritas em determinados suportes. Quando falamos em ‘resgate de interfaces’, queremos avançar para pensar que esse procedimento se dá por esse binômio de escavação-dissecação, pois como coloca Huhtamo o que acompanha o movimento de escavação é a preocupação em encontrar características cíclicas, mas não cronológicas (FISCHER, 2012a, p. 10, grifo do autor).

Portanto, entendemos que atuar com a metodologia das molduras demanda compreendê-las, conforme Kilpp (2010, p. 29, grifo da autora), como um “território de experiência e significação qualquer. Nos mesmos termos que nos referimos às *ethicidades*”, essas sendo como os sentidos de *tecnosegurança* circunstanciadas na plataforma do FB. Kilpp (2010, p. 17, grifos da autora) esclarece o conceito especificamente ao tratar de sua pesquisa sobre imagens da televisão, o que dá suporte ao modo de pensar a respeito de nossa empiria e seu ambiente:

O eixo das *ethicidades*, entendidas como subjetividades virtuais – durações, *personas*, fatos e acontecimentos – que a televisão dá a ver como tais, mas que são, na verdade, construções televisivas. Subjetivo, nos termos de Bergson, é aquilo que muda de natureza ao de dividir. Subjetividade remete, assim, à sua virtualidade, que se atualiza, que está em vias de atualizar-se, que é inseparável do movimento de sua atualização, pois um ser não é o sujeito, mas a expressão da tendência, que é contrariada por outra tendência, outro ser.

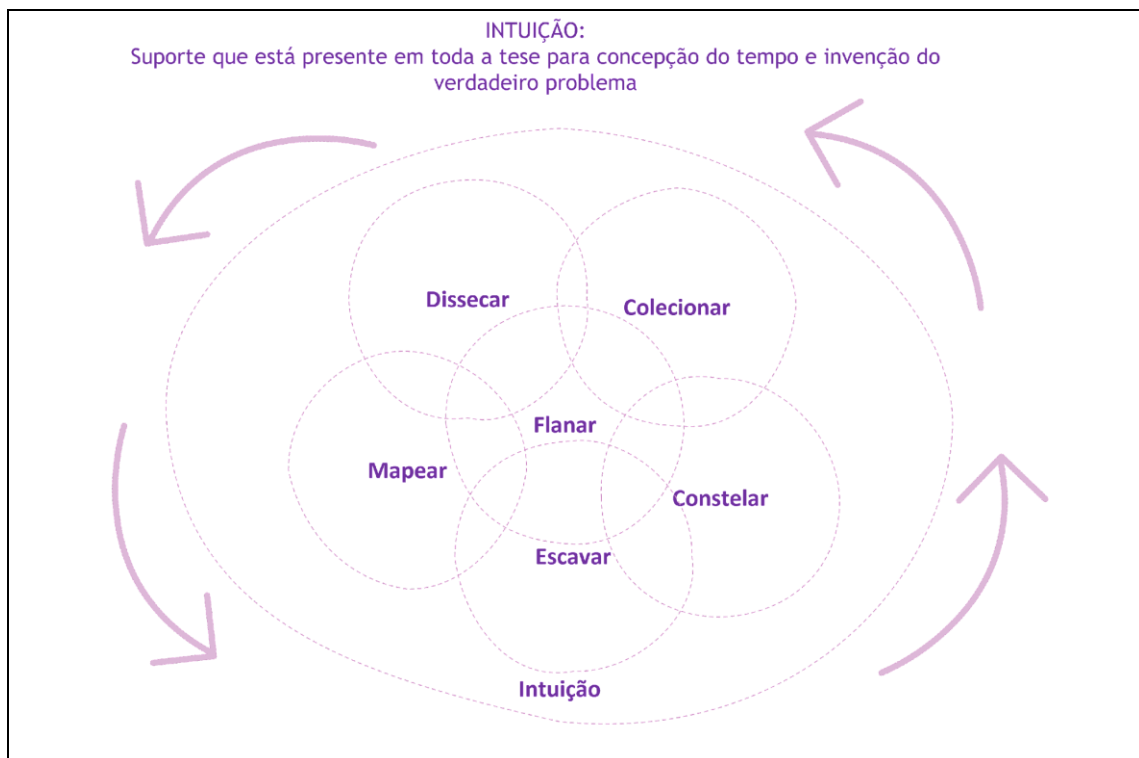
A partir do suporte de Kilpp (2010, p. 16, grifo da autora) e sua metodologia, acreditamos que, para identificarmos as moldurações realizadas pela plataforma FB para construirmos os sentidos de segurança em seu ambiente, é necessário primeiramente verificá-los atualizados na empiria, ou seja, encontrarmos as “*ethicidades*, virtualidades que só se atualizam desse modo [...]”. Concomitantemente, há o eixo dos imaginários na metodologia das molduras, que, em nossa pesquisa, dá suporte para encontrarmos as *ethicidades* em nosso objeto, pois precisamos pensar em imaginários que emergem desse ambiente, que são compartilhados entre emissor e receptor, conforme Kilpp (2003, p. 157) comenta: “cujos sentidos são gestados no ambiente da indústria da cultura e na relação que se estabelece entre os sujeitos do processo de produção e do consumo”. Por isso, entendemos que explorar nossa empiria em busca dos sentidos de *tecnosegurança*, que se atualizam nas interfaces, reforça o entendimento sobre imaginários que emergem nesses espaços já que

O eixo dos imaginários, que permitem a comunicação dos sentidos, entendendo-se imaginário como o conjunto de marcas de enunciação de culturas (identidades coletivas), manifestas e visíveis dos discursos, na arte, nos produtos culturais... ou que são por ela mediadas (KILPP, 2010, p. 18).

Portanto, chegamos ao fim (ou seria o início?) de nosso esboço de itinerário metodológico, que não pretendemos traçar como uma linha reta, uma rota de mão única, unilateral, mas entendendo que cada movimento proposto, dentro do arranjo metodológico, é capaz de influenciar avanços e retornos constantemente, visto que nosso objeto demanda refletirmos muito mais em função do tempo do que do espaço, ou seja, há um contágio constante em cada movimento realizado com o objeto.

Como diz Canevacci (1997, p. 111) “o objeto e o método se constroem reciprocamente”, a ideia inicial de chamar pela metáfora itinerário metodológico é reconhecer que necessitaremos fazer algumas paradas ao longo do caminho, voltar alguns quilômetros na estrada, para poder seguir no sentido que nosso objeto vai convocando, quando não estamos buscando a definição de uma única opção para chegada. Para auxiliar na compreensão de nosso itinerário, esboçamos a figura, a seguir, que ilustra o movimento que estamos desenvolvendo, onde cada fase contagia a outra, e, baseando-nos nessa lógica, identificamos que o conjunto de características de nosso objeto assume duas ordens: a da materialidade, referente ao percurso pela plataforma, dando suporte à *flânerie* e às **coleções**, e da ordem das virtualidades ou da duração, no nosso caso específico, entendida como as *ethicidades* e imaginários a partir dos **emolduramentos** agenciados dando a ver as **constelações**.

Figura 28 - Contágio do itinerário metodológico



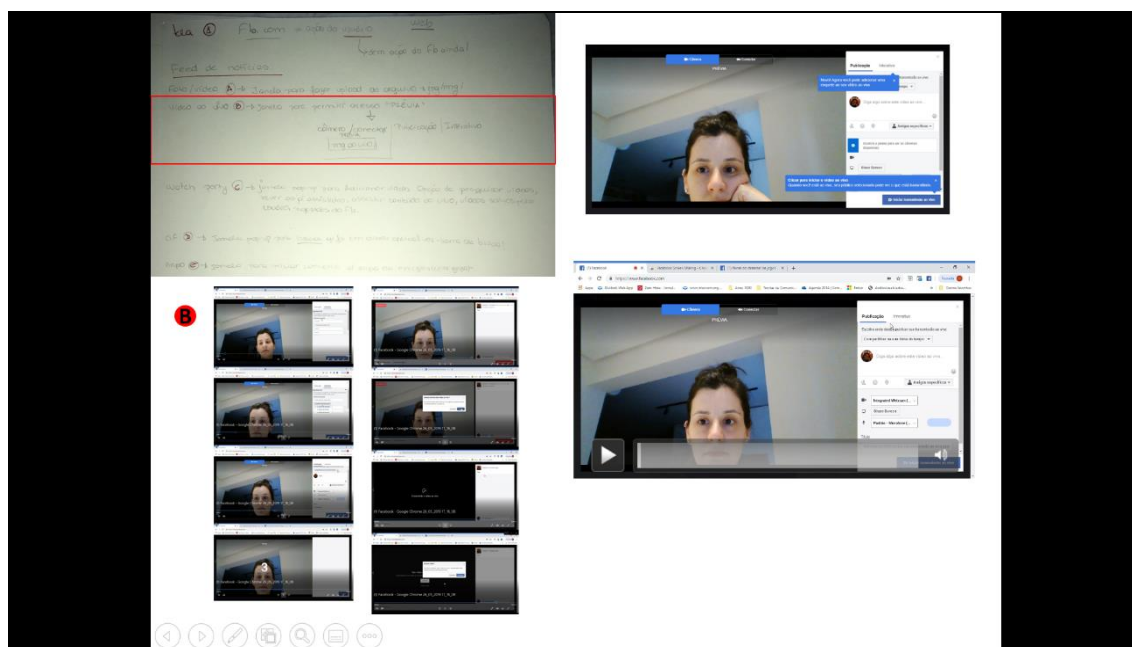
Fonte: Elaborado pela autora (2021).

Acreditamos, também, que não há resposta certa ou errada, mas talvez, àquelas mais coerentes com as exigências do objeto no momento, numa fusão constante de afetos entre os ambientes que circundam: pesquisadora, objeto e empiria.

### 3.2 Recolhendo e situando o *corpus* pela *tecnosegurança*

Esta seção de nossa tese é dedicada à apresentação das interfaces coletadas a partir de um movimento de *flânerie*, alicerçada numa prática de coleta de capturas de telas que vem sendo feita previamente ao ingresso no doutorado, em 2018, quando desenvolvemos o projeto para seleção no PPGCC UNISINOS. Em uma série de movimentos “descompromissados” em encontrar algo específico no objeto, fomos caminhando pelas interfaces da plataforma sem filtrar o que seria sugerido, permitindo que o *software* nos conduzisse durante todo o percurso. Fizemos algumas tentativas de mapear ou organizar o trajeto e levamos esses registros de “caminhos” em reuniões do LAR, conforme registro no acervo de imagens a seguir:

Figura 29 - Exemplo do exercício de recolher interfaces para análise do *player* de vídeos do FB - LAR (maio 2019)

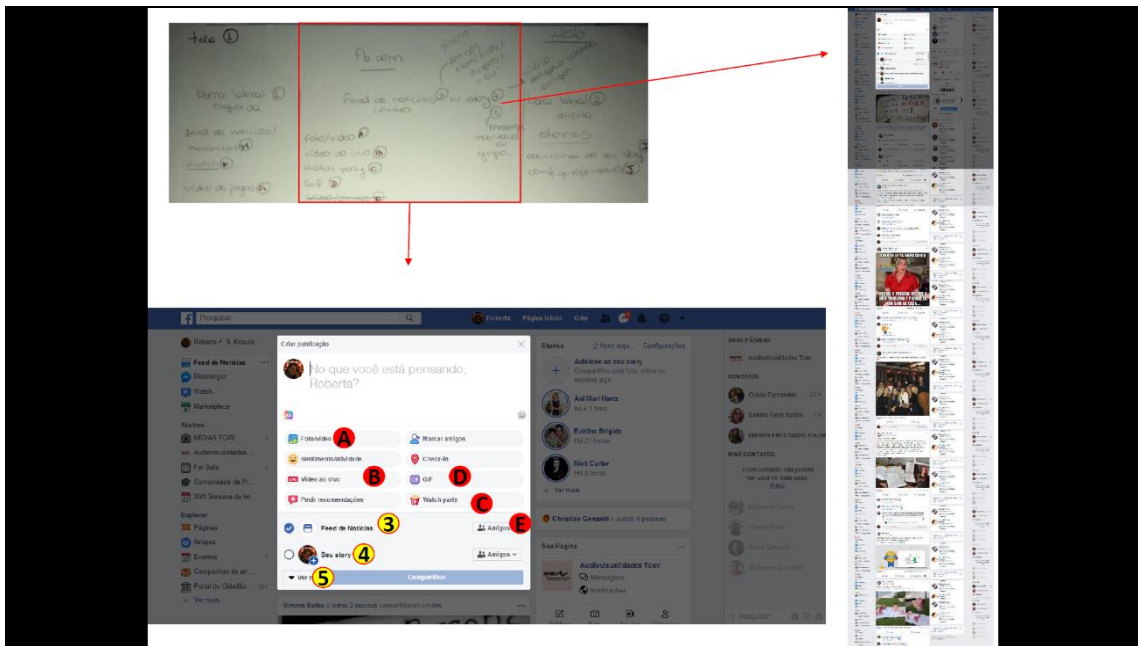


Fonte: Elaborado pela autora (2019).

Durante os exercícios de coleta, que são inspirados na figura do *flâneur*, de Walter Benjamin (2006), fomos coletando todas as interfaces durante os movimentos de exploração do objeto, sem a intencionalidade de ver algo, pelo contrário, de recolher tudo, não deixar de

registrar nada que pudesse ficar para trás ou descartado. Esses movimentos foram sendo armazenados, alguns em formato de vídeo, pela gravação da tela do *notebook* no programa Microsoft Game, outros em capturas de telas pela extensão Go Full Page-*screenshot*, no navegador Google Chrome para versão *desktop/web*, outras no formato *screenshot* com o comando simultâneo do botão lateral + volume) da tela do *smartphone* Iphone SE (período de 2018 até maio 2020) e Iphone 11 (a partir de junho de 2020 até julho de 2022).

Figura 30 - Tentativa de inventariar as capturas de telas e compreender a arquitetura da interface (jul. 2019)



Fonte: Elaborado pela autora (2019).

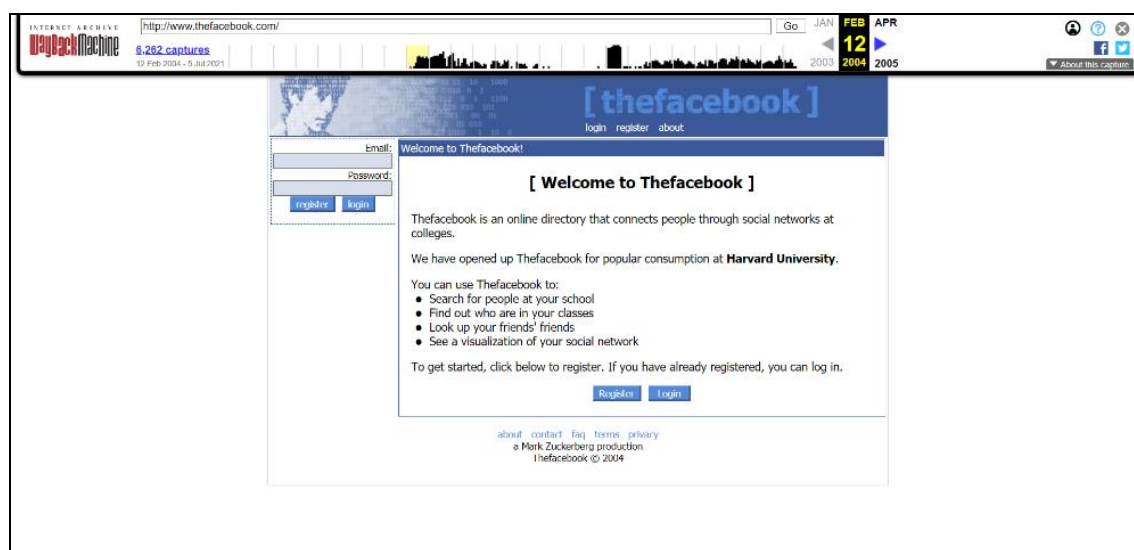
O exercício de recolher telas fez parte de nosso hábito de navegar pelas funcionalidades da plataforma, onde fomos guardando imagens das interfaces por motivos específicos e outros por simplesmente tentar registrar a nossa passagem por aquela seção ou interação com o conteúdo ofertado. Iremos detalhar melhor os processos e percursos, pois acreditamos ser uma parte importante de nosso itinerário metodológico, necessário para “preparar o terreno”, no FB, a ser explorado e contextualizá-lo como plataforma, compreender seu surgimento, a partir de um breve relato de sua história, até chegar na relação polêmica sobre uso e segurança de dados e a privacidade de seus usuários. Conforme debate realizado no capítulo dois, vimos que a *tecnosegurança* na contemporaneidade carrega aspectos extremamente alicerçados em privacidade, monitoramento, controle, vigilância e banco de dados.



Fundado no outono de 2003 por um grupo de estudantes da Universidade de Harvard, nos Estados Unidos, a primeira versão da rede social que deu origem ao FB se chamava FaceMash, onde eram exibidas imagens de estudantes de Harvard, numa espécie de comparador entre eles e animais, para avaliar quem seria o mais atraente. As imagens eram exclusivas de estudantes do sexo feminino e eram expostas lado a lado, na interface do FaceMash onde o visitante poderia escolher entre duas opções de alunas. Para coletar essas fotografias, Mark Zuckerberg, aluno de Harvard, *hackeou* o banco de dados da universidade, relatou todo o passo a passo de sua façanha em seu *blog* pessoal e programou o *site* que atingiu 22 mil visualizações nas primeiras quatro horas de publicação, e, em poucos dias, praticamente todos os estudantes já haviam acessado ou tinham recebido o convite para conhecer. A diretoria de Harvard puniu Zuckerberg com 6 meses de afastamento acadêmico por violação de segurança e coleta indevida de informação (ROTHAERMEL, 2015).

Conforme uma série de relatos sobre a migração do FaceMash para o The Facebook, onde outros estudantes ingressam no grupo de desenvolvedores, Zuckerberg atuava como programador terceirizado em diversos projetos, tanto de estudantes quanto de empreendedores locais, a partir da fama gerada com o FaceMash. Conforme matéria investigativa publicada pela revista *The Rolling Stone* (HOFFMAN, 2010), a concepção de criar um *site* para conectar pessoas da comunidade acadêmica foi inicialmente criada por Divya Narendra, que nomeou a página na internet como *Harvard Connection*. Zuckerberg havia sido contratado para programar o *site*, o que nunca aconteceu. Poucos meses após, registrou e lançou, em 4 de fevereiro de 2004, junto com outro colega de dormitório de Harvard, Eduardo Saverin, o The Facebook.

Figura 31 - Captura de tela da primeira versão do *site* The Facebook (publicada em 12 fev. 2004)<sup>3</sup>



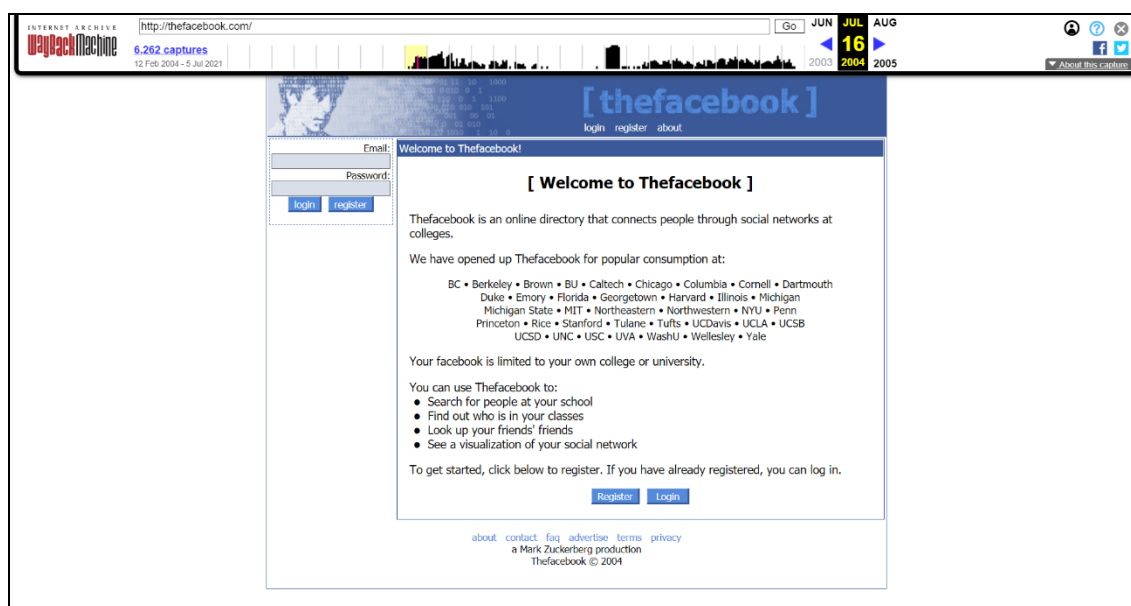
Fonte: Internet Archive (2004)<sup>4</sup>.

O *site* foi um sucesso entre os estudantes universitários, pois em apenas duas semanas de lançamento atingiu o número de 4 mil usuários (para criar uma conta gratuita na rede social era necessário fazer o *upload* de uma fotografia de perfil e cadastrar um endereço de *e-mail* com final *.edu* – o que caracteriza uma conta universitária nos Estados Unidos). Prevendo o sucesso da rede, Saverin e Zuckerberg convidaram outro colega, Dustin Muskovitz, para auxiliar na divulgação e lançamento em outras grandes comunidades universitárias como Yale, Stanford e Columbia. Nessa época, o percentual do negócio era 65% de Zuckerberg, 30% para Saverin e 5% para Muskovitz. Posteriormente, outro colega, Chris Hughes, incorporou o grupo assumindo como porta-voz da empresa. E, no final de maio do mesmo ano, ou seja, no encerramento do semestre, o *site* já havia atingido o número impressionante de duzentos mil usuários cadastrados (HOFFMAN, 2010).

<sup>3</sup> Captura de tela realizada a partir da ferramenta WaybackMachine, onde buscamos a URL <http://www.thefacebook.com> no *site* Internet Archive, “que cataloga e disponibiliza de forma *online* versões de páginas *web* através do tempo” (FISCHER, 2008, p. 46).

<sup>4</sup> Maiores informações em <https://web.archive.org/web/20040212031928/http://www.thefacebook.com/>.

Figura 32 - Captura de tela da página inicial do The Facebook aberto para as demais comunidades acadêmicas (16 jul. 2004)



Fonte: Internet Archive (2004).<sup>5</sup>

Uma das questões que garantia a identidade dos usuários da rede social, naquela época, era justamente o seu *login*, que obrigatoriamente deveria pertencer a uma das universidades de elite cadastradas, garantindo um alto padrão de entrada, diferentemente de outros *sites* de redes sociais como MySpace, por exemplo. Ainda em 2004, Mark Zuckerberg trancou a faculdade de Harvard, foi para o Vale do Silício e lá deu início aos investimentos e estrutura que culminam com a realidade da empresa hoje, inclusive retirando o “The”, mantendo apenas Facebook no nome da rede social. Em 2005 o FB recebeu seu primeiro grande investimento de uma *venture capital*, a Accel Partners, de US\$ 12,7 milhões, e abriu seu cadastro para estudantes de ensino médio e demais universidades, fechando o ano com 6 milhões de usuários ativos por mês e receita de US\$ 9 milhões (ROTHAERMEL, 2015).

<sup>5</sup> Maiores informações em <https://web.archive.org/web/20040716021640/http://thefacebook.com/>.

Figura 33 - Excerto de tela da página inicial do FB quando restrito ao uso da comunidade escolar (19 abr. 2006)



Fonte: Internet Archive (2006).<sup>6</sup>

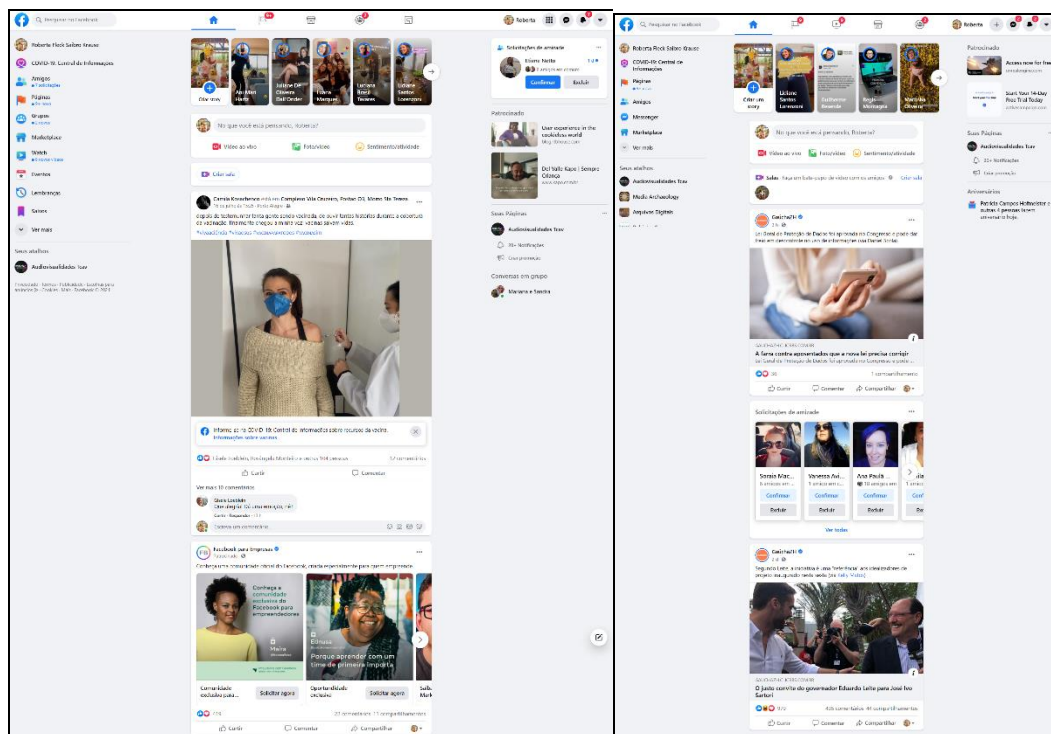
No segundo semestre de 2006, a rede social foi aberta para cadastro de qualquer indivíduo com mais de 13 anos, não mais restringindo a participação à relação com alguma instituição de educação. Em 2007, o FB lançou a possibilidade de integração com aplicativos e demais funcionalidades de terceiros, o que permitiu o surgimento do *game* Farmville, importante sucesso na época e responsável por manter altas taxas de engajamento com o conteúdo e tempo de permanência na página. Além disso, foi o ano em que o FB criou uma nova ferramenta de publicidade, o Beacon Ads, que iremos detalhar mais à frente no texto. No ano seguinte, 2008, foi lançada a ferramenta de bate-papo e, também, a versão do aplicativo para ser utilizado no mais novo *smartphone* da época, o Iphone. Até então os usuários que acessavam via celular entravam no FB via versão *desktop*, o que deixava a desejar no quesito usabilidade e tempo de carregamento de página, que fora desenhado originalmente para acesso via computador e não dispositivos móveis. Foi em 2009 que o FB criou o botão *like* ou “curtir”, para incentivar o engajamento e interação dos usuários com as publicações de suas conexões, e registrou, pela primeira vez, o lucro para a empresa (G1, 2014). Com a possibilidade de monetização, a partir de terceiros, o FB deixou de ser uma rede social para operar no modelo de plataforma, conforme vimos no capítulo anterior dessa tese, onde Van Dijck, Poel e Waal (2018) comentam sobre o modelo de negócio que envolve monetização, processamento algorítmico e circulação de dados, não restringindo mais a conexão entre usuários finais do *site*, mas, entre parceiros interessados em anunciar seus produtos, marcas e serviços aos indivíduos cadastrados.

<sup>6</sup> Maiores informações em <https://web.archive.org/web/20060419184949/https://www.facebook.com/>.

Conforme a empresa afirma, sua missão atualmente é “Dar às pessoas o poder de criar comunidades e aproximar o mundo” (FACEBOOK, 2021); já em outra página da plataforma, ao buscar a seção “central de segurança” encontramos: “Nossa missão é proporcionar às pessoas o poder de compartilhar e tornar o mundo mais aberto e conectado. Desejamos que as pessoas se sintam seguras quando usam o Facebook” (FACEBOOK, 2021).

Quando o assunto é modelo de negócios, escavamos o FB para verificar como se organiza para o mercado. É possível inferir que opera com base em três pilares principais em sua plataforma, ou seja, são áreas específicas dentro de sua interface que são destinadas à interação com seus usuários e monetização: o *newsfeed* – ou “alimentação de notícias”, lançado em 2006 e é onde se encontram as principais atualizações da rede de contatos de um usuário, uma espécie de *homepage* logo após fazer login. Nesse ambiente, é onde há acesso a todas as áreas e recursos da plataforma, e, ao mesmo tempo, é onde o algoritmo do FB opera de maneira extremamente complexa, selecionando, ocultando e priorizando a exibição de conteúdo para os usuários a partir de métricas como volume de comentários, taxas de engajamento, avaliação de usuário que originalmente postou e capacidade de adequação desse conteúdo aos interesses do “proprietário” do *feed* (ROTHAERMEL, 2015).

Figura 34 - Excertos de capturas de telas da *newsfeed* para versão *desktop* (jul. 2021/set. 2020)



Fonte: Krause (2021; 2020).

De acordo com a declaração do FB, a maneira como os conteúdos são oferecidos na *newsfeed* é única para cada usuário, onde se cria por dedução a personalização das notícias levando em consideração 3 pontos principais, como quem publicou, qual o tipo de conteúdo postado e as interações no histórico dessa publicação específica;

Um: Como avaliamos as histórias mais relevantes para você. Levamos em conta três sinais principais para deduzir a relevância de uma publicação:

- Quem publicou: amigos, familiares, fontes de notícias, empresas e figuras públicas com os quais você mais interage têm prioridade no seu Feed de Notícias.
- Tipo de conteúdo: priorizamos o tipo de conteúdo com o qual você interage com mais frequência, sejam fotos, vídeos ou links de preferência.
- Interações com a publicação: publicações com muitas curtidas, reações, comentários e compartilhamentos (principalmente de pessoas com as quais você mais interage). As publicações com as histórias mais relevantes para as pessoas são exibidas em primeiro lugar.

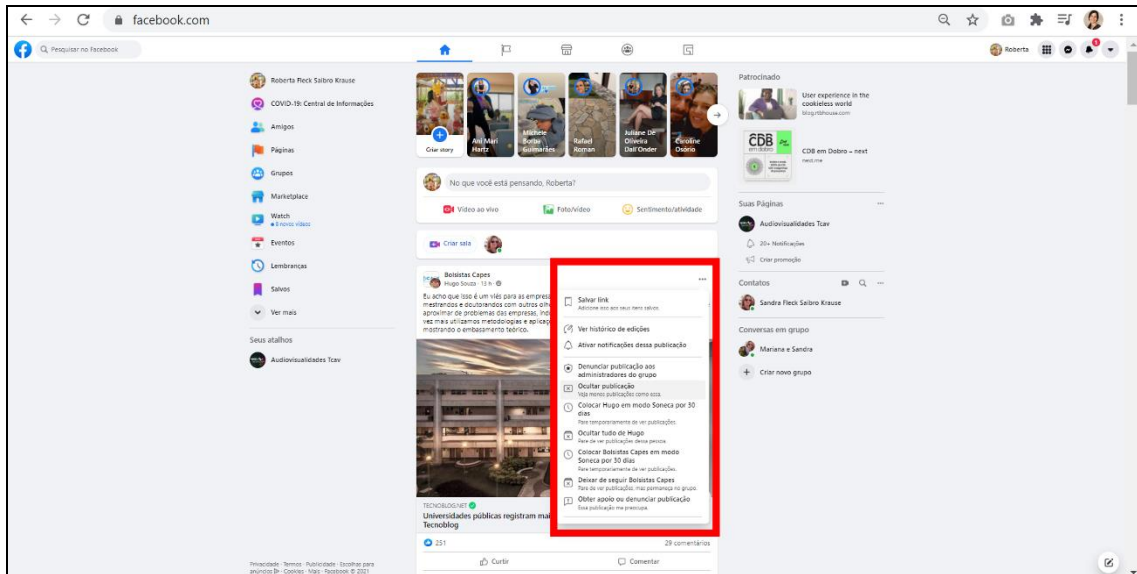
Com base nesses três sinais, cada publicação recebe uma classificação para determinar onde ela aparecerá no seu Feed de Notícias e quais histórias aparecerão primeiro (FACEBOOK, 2021).

Além disso, o FB auxilia o usuário a obter certa possibilidade de selecionar, ou melhor, ensinar o algoritmo a compreender, cada vez melhor, qual o tipo de conteúdo é interessante para ele, permitindo que as pessoas possam moldar o seu espaço com poucas funcionalidades:

Nem sempre é possível acertar. No fim das contas, é você quem sabe o que mais importa. Por isso, disponibilizamos controles específicos para que sua experiência seja personalizada.

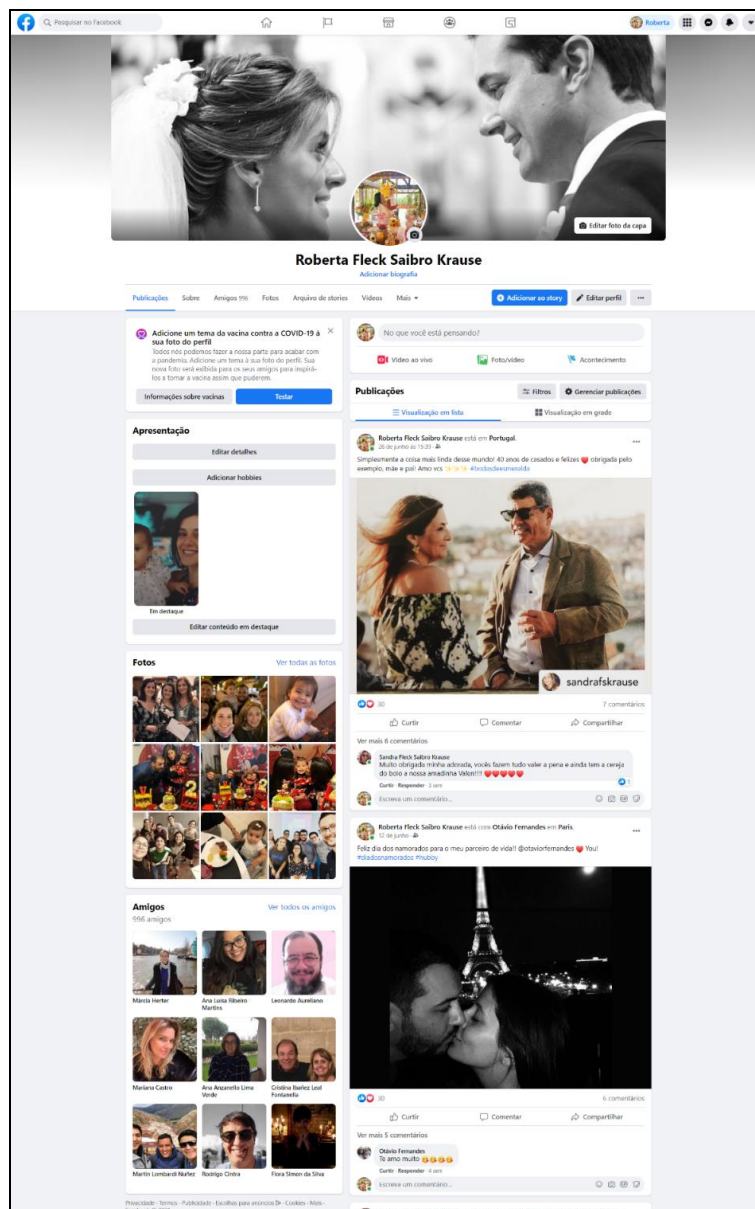
- Preferências do Feed de Notícias: toque em qualquer uma das Preferências do Feed de Notícias para ver como elas funcionam.
- Personalize diretamente no Feed de Notícias: além disso, com um simples toque, você pode melhorar seu Feed de Notícias diretamente em qualquer publicação. O menu suspenso oferece opções de personalização como Ocultar ou Deixar de seguir (FACEBOOK, 2021).

Figura 35 - Excerto de tela - *newsfeed* - personalização a partir do usuário



Fonte: Krause (2021).

O segundo pilar para sustentação do produto FB e seu modelo de negócios, de acordo com Rothaermel (2015), corresponde à *Timeline* (linha do tempo), lançado em 2011, espaço destinado ao conteúdo próprio do usuário da conta, uma espécie de perfil contendo em arquivo o acervo com as publicações e histórico de interações da conta. Somente o usuário detentor daquele *login* possui acesso completo àquela linha do tempo, ou seja, ela é restrita ao proprietário da conta pela qual se está acessando o FB. É possível selecionar o que se deseja omitir ou exibir e para quais contatos tornar visíveis as informações sobre perfil, tais como nome, localização, estado civil, profissão, dentre outros dados que podem ser compartilhados como as próprias publicações.

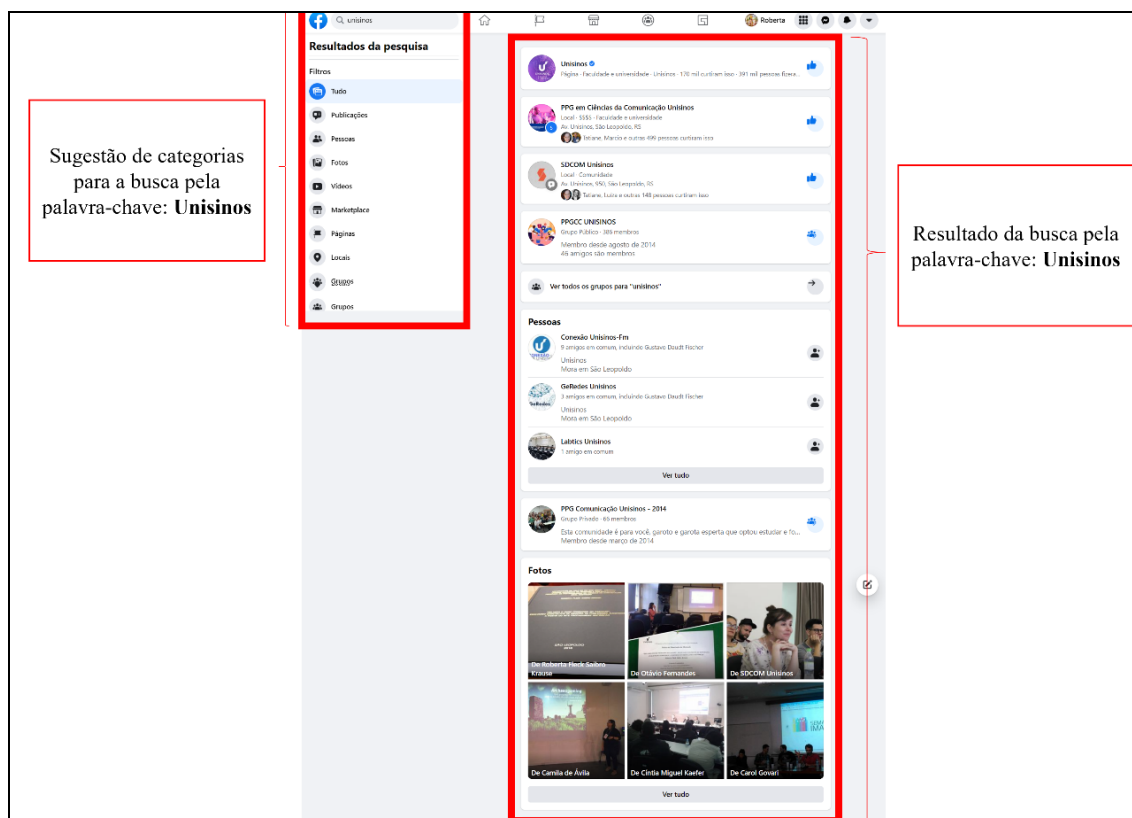
Figura 36 - Excerto de tela - *timeline* do usuário

Fonte: Krause (2021).

O último pilar que faz parte do modelo de negócios, fundamentado na análise de Rothaermel (2015), é a capacidade de realizar buscas a partir de gráficos em bancos de dados, o que permite que a plataforma tenha a capacidade de encontrar pessoas, fotografias, lugares, empreendimentos e conteúdos, através de uma barra de pesquisa localizada no topo da interface do usuário. Simbolizada por uma lupa, essa ferramenta agrega a capacidade do FB em concorrer diretamente com outras ferramentas de busca na *web*, como o próprio Google, mas, com um agregador importante pois realiza a pesquisa dentro de sua própria plataforma, entre seus usuários, grupos, páginas, eventos e demais funcionalidades do FB, tornando um diferencial competitivo entre os demais buscadores disponíveis na rede.



Figura 37 - Barra de busca do FB e suas categorias de indexação de resultados



Fonte: Facebook (2021).<sup>7</sup>

Além de obter esses três pilares principais como modelo de negócios, o FB trabalha com a monetização de publicidade desde 2007, mas atualmente, a partir de seu sistema chamado Gerenciador de Anúncios, o Facebook Ads, que integra no mesmo ambiente investimentos em publicidade nos outros produtos da empresa Meta (antiga Facebook Inc.), como a rede social Instagram (no portfólio da empresa desde 2012). Além disso, no mesmo ano o FB atinge a marca de mais de 1 bilhão de usuários ativos ao redor do mundo. E, em 2014, o aplicativo de troca de mensagens instantâneas, WhatsApp, foi adquirido pela empresa Facebook Inc.; junto com essa aquisição a plataforma FB lança o *check-in* de segurança para seus usuários. Em 2015 atinge a marca de 1 bilhão de usuários diários e lança, no mercado, a opção de transmissão de conteúdo ao vivo por vídeo, o Facebook Live.

Em 2016 é anunciada a criptografia de ponta a ponta para o aplicativo WhatsApp, assim como, sua versão para uso de aplicativo no desktop (FACEBOOK, 2021). Atualmente, a plataforma FB possui 2,93 bilhões de usuários ativos mensalmente no mundo (STATISTA, 2022), sendo que, no Brasil, o total foi de 148,57 milhões em 2021. A receita da empresa Facebook Inc., no ano de 2021, foi de US\$ 117 bilhões conforme relatado por Statista (2022).

<sup>7</sup> Maiores informações em <https://www.facebook.com/search/top?q=unisinos>.

De acordo com o Professor da Universidade de Nova Iorque (NYU), Scott Galloway (2020, p. 8), o ranking é “FB (em 1º lugar), o Messenger do FB (2º lugar) e o Instagram (8º lugar) são os aplicativos móveis mais populares nos EUA”. Na atualidade, a Meta possui o total de 3,69 bilhões de usuários ativos em todos os seus produtos (Facebook, Instagram, Messenger e Oculus – empresa produtora de *hardware* para realidade virtual) (STATISTA, 2022).

Entendendo a demanda do mercado anunciante por investimentos em sua plataforma, atualmente, o FB promete entregar relevância em seu conteúdo, assim como alto alcance com seus usuários, engajamento e contexto social ao serem inseridos a publicidade ou conteúdo pago. Os itens patrocinados são expostos em áreas específicas da interface, incluindo *newsfeed*, com vídeos tanto nas barras laterais da página da *timeline*, quanto da *newsfeed*.

Porém, desde o ano de 2004, a rede social opera com conteúdo patrocinado, ou *flyers*, originalmente chamados, onde eram oferecidos espaços publicitários em formatos de *banners* e exibidos exclusivamente na lateral esquerda da tela, abaixo da barra de busca, já na área logada do usuário. A precificação das campanhas era feita por diárias, variando de US\$ 12 até US\$ 50, a depender para qual comunidade escolar o anunciante desejasse exibir a peça, conforme explicita a descrição na seção do *The Facebook Announcements* de 2005, onde simulamos uma operação de campanha a seguir:

Figura 38 - Página dentro do The Facebook dedicada a conteúdo publicitário - *Announcements* (ago. 2005)



Fonte: Internet Archive (2021).<sup>8</sup>

<sup>8</sup> Informações em <https://web.archive.org/web/20051127050746/http://www.facebook.com/announce.php>.

Figura 39 - Detalhamento da operação publicitária dentro do Facebook - sob nova nomenclatura (nov. 2005)

The screenshot shows the 'Facebook Announcements' page. At the top, there is a navigation bar with 'facebook' and links for 'login', 'register', 'about', and 'help'. Below this, the page is divided into several sections:

- What are Facebook Announcements?**: A section explaining the concept of Facebook Announcements, including 'The Dilemma' (three scenarios for a local restaurant, property manager, and athletics staff) and 'The Solution' (Facebook Announcements as text-only advertisements).
- Who will see them? How many times?**: A section explaining that users choose the school(s) to advertise to, and the announcement will be seen by thousands of target students multiple times each day.
- Test it out:**: A section encouraging users to preview their ad and calculate the number of views.
- Questions?**: A link to the 'Announcement FAQ'.
- What should your announcement say?**: A form with fields for 'Title' (ROBERTA), 'Link' (https://www.facebook.com/rober), and 'Body' (olá, meu nome é roberta e gostaria de testar esse espaço publicitário para divulgar minha pesquisa!). A 'Preview' window shows the ad as it would appear on a Facebook page.
- Which schools should get your announcement?**: A section with a dropdown menu set to 'NYU (\$50/day)' and an 'Add school' button.
- When should your announcement start?**: A section with radio buttons for 'Right now' (selected) and 'On this date: (mm/dd/yyyy) 11/27/2005'.
- Contact Information**: A section with fields for 'Name' and 'Email'.

At the bottom of the page, there is a 'Continue' button and a footer with links for 'about', 'jobs', 'announce', 'advertise', 'terms', and 'privacy', along with the text 'a Mark Zuckerberg production' and 'Facebook © 2005'.

Fonte: Internet Archive (2021).<sup>9</sup>

<sup>9</sup> Mais Informações em <https://web.archive.org/web/20051127050746/http://www.facebook.com/announce.php>.

Figura 40 - Evolução da opção *Annoucement*s para Facebook Flyers (fev. 2007)

Fonte: Internet Archive (2021).<sup>10</sup>

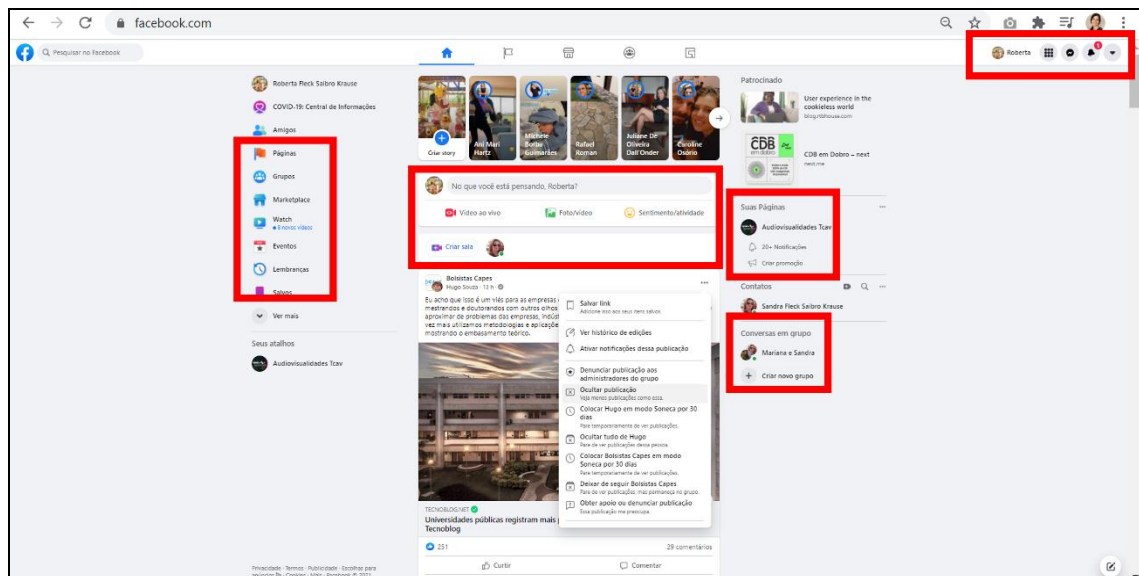
Já em relação aos produtos destinados aos usuários do FB, a plataforma oferece uma série de formatos e funcionalidades capazes de entreter, engajar e, principalmente, conectar pessoas por meio da internet, como iremos citar alguns exemplos:

- a) envio de mensagens - os usuários podem enviar mensagens via *e-mail* (com o @facebook.com gratuitamente), via Messenger no chat e via *newsfeed*;
- b) grupos - os usuários podem criar comunidades para debater assuntos específicos em comum, como esportes, culinária, política etc. O recurso Grupos foi lançado em 2004, logo no início da rede social;
- c) eventos - permite que os usuários criem eventos e encaminhem convites para outras pessoas na rede social, contendo horário, endereço e demais informações sobre a atividade. Além disso, proporciona uma espécie de página como uma *timeline* para arquivar conversas e informações trocadas exclusivamente entre os convidados do evento no mesmo ambiente *online*;

<sup>10</sup> Mais informações em <https://web.archive.org/web/20070204071003/http://www.facebook.com:80/adfaq.php>.

- d) *check-in* - possibilita aos usuários sinalizarem em sua *timeline* que estão em determinado ponto físico. O serviço de localização surgiu como uma extensão da rede social FourSquare em 2010. Permite que os usuários troquem informações sobre a localização e proporciona avaliação sobre o local;
- e) notificações - serviço de sinalização que envia um alerta ao usuário sobre atualizações de amigos ou notícias em sua *newsfeed*, como avisos de amigos, convite para eventos e demais atividades de interações. As notificações ficam visíveis para os usuários com um sistema de quantificação, mostrando em números quantas notificações possui;
- f) fotos e vídeos - uma das funcionalidades mais populares do FB é o compartilhamento de fotos. Em média, os usuários fazem o *upload* de 250 milhões de fotografias diariamente na plataforma, além de poder compartilhar com quem quiser, marcar amigos e localização. O serviço é ilimitado e gratuito, e há a possibilidade de capturar fotos e vídeos direto pela câmera do dispositivo de acesso, facilitando ao usuário não precisar fazer *upload* de arquivo para publicar na plataforma;
- g) páginas - qualquer usuário pode criar uma página de conteúdo de maneira gratuita, funcionalidade que permite que vários usuários gerenciem a mesma página, e possibilita um número ilimitado de conexões, diferentemente do perfil de pessoa física que limita a 5 mil a conexão com “amigos” ou com outros usuários. Além disso, as páginas ou perfis comerciais têm acesso ao Facebook Ads, recurso para gerenciar publicidade no Instagram e no FB (ROTHAERMEL, 2015, p. 5-6);
- h) *watch* - espaço destinado ao consumo de conteúdo em vídeo dentro da plataforma, sendo possível assistir ao mesmo conteúdo com um amigo, agendar uma “*watch party*”, e consumir vídeos oferecidos pelo *software* conforme interesses demonstrados pelo usuário;
- i) Marketplace - área que tem como objetivo conectar pessoas que desejam vender/comprar algo específico. O FB não opera como uma loja virtual, mas como um ponto de contato entre consumidores e vendedores.

Figura 41 - Excerto de tela sinalizando na *newsfeed* os produtos destinados aos usuários do FB



Fonte: Facebook (2021).

Conforme citado anteriormente, é gigantesco o volume de dados coletados pelo FB em apenas alguns segundos de uso de seus usuários, e, como já vimos, a empresa foi alvo diversas vezes de críticas referentes ao mau uso de informação “privada” e vigilância de seus usuários cadastrados. A primeira vez foi em 2007, quando o FB lançou a ferramenta de publicidade Beacon Ads, que rastreava os usuários em *sites* comerciais parceiros da empresa, e, posteriormente, divulgava essa informação aos “amigos” do usuário numa espécie de recomendação dentro do FB.

Se, por exemplo, um membro compra um filme num site associado ao Facebook, a sua rede de amigos pode receber uma notificação sobre a compra que fez, links para o produto, preços etc. O mecanismo publicitário permite, ainda, que empresas parceiras do Facebook tenham um perfil similar aos dos demais membros e façam destes seus “amigos”, ofertando produtos condizentes com seus perfis pessoais (BRUNO, 2008, p. 10).

A plataforma mencionava o sistema do Beacon Ads como algo revolucionário: “um novo modo de distribuir socialmente a informação [...] possibilitava aos anunciantes do FB rastrear usuários através da internet, revelando suas compras por meio de suas redes pessoais sem ter permissão para tanto” (ZUBOFF, 2020, p. 63). O serviço estava descrito nos “acordos de termos de serviço” que são ofertados aos usuários como contratos de adesão, ou seja, é a única opção de utilizar o serviço, caso contrário não é possível abrir uma conta no FB. Logo após o escândalo, a empresa descontinuou esse sistema de publicidade e reformulou suas políticas de uso de dados, alertando para questões envolvendo privacidade e segurança das

informações cedidas gratuitamente e voluntariamente por usuários da plataforma. O primeiro alerta havia sido dado para chamar a atenção de questões éticas envolvendo informações na internet, que também se expande entre “os quatro” gigantes da tecnologia e economia atualmente: Google, Facebook, Amazon e Apple (GALLOWAY, 2020).

As plataformas coletam automaticamente grandes quantidades de dados - tanto dados de conteúdo quanto dados do usuário (Driscoll 2012; Mayer-Schönberger e Cukier 2013; Turow 2012; Van Dijck 2014). A coleta de dados é ativada e moldada por hardware e software; os dispositivos que as pessoas usam para acessar os serviços da plataforma geralmente vêm equipados com software e aplicativos que podem coletar dados automaticamente. Com cada clique do mouse e movimento do cursor, os dados do usuário são gerados, armazenados, analisados automaticamente e processados - não apenas endereços de protocolo da Internet e geolocalização, mas informações detalhadas sobre interesses, preferências e gostos<sup>11</sup> (VAN DIJCK; POEL; WAAL, 2018, p. 9, tradução nossa).

No ano de 2012, a matéria publicada no *The Wall Street Journal*, realizada por Julia Angwin e Jeremy Singer-Vine, revelou que diversas informações confidenciais de usuários do FB e de sua lista de amigos estavam sendo compartilhadas com empresas de *softwares* a partir do desenvolvimento de aplicativos populares para a própria plataforma. Além de ter acesso aos dados sensíveis desses indivíduos, a matéria alertava para a dificuldade de compreensão sobre os termos de uso do serviço, o que fazia com que os usuários acabassem dando consentimento a contratos mascarados ou muito mal explicados.

Agora existem “aplicativos” - pedaços discretos e elegantes de software que ficam online ou em seu smartphone. Para “comprar” um aplicativo, basta clicar em um botão. Às vezes, eles custam alguns dólares, mas muitos aplicativos são gratuitos, pelo menos em termos monetários. Você costuma pagar de outra forma. Aplicativos são portas de entrada e, quando você compra um aplicativo, há uma grande chance de você estar fornecendo a seus desenvolvedores uma das mercadorias mais cobiçadas da economia atual: a dos dados pessoais<sup>12</sup> (ANGWIN; SINGER-VINE, 2012, tradução nossa).

Em 2014, o FB voltou a se envolver em questões polêmicas envolvendo dados, ao informar que iria compartilhar inclinações políticas e tendências de interesses de seus usuários

---

<sup>11</sup> “Platforms automatically collect large amounts of data - both content data and user data (Driscoll 2012; Mayer-Schönberger and Cukier 2013; Turow 2012; Van Dijck 2014). The collection of data is enabled and shaped by hardware and software; devices people use to access platform services often come equipped with software and apps that can automatically collect data. With each mouse click and cursor movement user data are generated, stored, automatically analyzed, and processed— not just Internet protocol addresses and geolocations but detailed information about interests, preferences, and tastes.”

<sup>12</sup> “Now there are ‘apps’—stylish, discrete chunks of software that live online or in your smartphone. To ‘buy’ an app, all you have to do is click a button. Sometimes they cost a few dollars, but many apps are free, at least in monetary terms. You often pay in another way. Apps are gateways, and when you buy an app, there is a strong chance that you are supplying its developers with one of the most coveted commodities in today’s economy: personal data.”

para auxiliar na cobertura das eleições presidenciais dos Estados Unidos, de 2016, para algumas empresas de jornalismo.

Como parte do experimento, o Facebook categorizará as atualizações de status sobre políticos e questões políticas por usuários adultos do Facebook nos EUA como positivas, negativas ou neutras. Os dados guiarão os relatórios da ABC e do BuzzFeed sobre as tendências políticas de certos grupos demográficos<sup>13</sup> (FLYNN, 2014, tradução nossa).

Alguns anos mais tarde, em 2018, o FB foi acusado por vazamento de informação “privada” de usuários para a empresa de tecnologia, Cambridge Analytica, conforme relatado no livro recente de Brittany Kaiser<sup>14</sup> (2020) sobre um dos maiores escândalos envolvendo as redes sociais. Nesse ponto, é necessário trazeremos o conceito de capitalismo de vigilância proposto por Shoshana Zuboff (2020), ao afirmar que hoje o colonialismo de dados é o novo capitalismo, partindo do uso de informação de usuários para aprimoramento de produtos e serviços, mas, também, para realizar análise preditiva de comportamento humano para fins financeiros. Nas palavras da autora “o capitalismo de vigilância reivindica unilateralmente a experiência humana como matéria-prima gratuita para tradução em dados comportamentais” (ZUBOFF, 2020, p. 27).

Nesse episódio extremamente danoso para a sociedade em geral, tanto os 87 milhões de usuários do FB que tiveram suas informações manipuladas sem o seu consentimento, quanto a sociedade como vítima do resultado dessa manipulação, o próprio CEO<sup>15</sup> Mark Zuckerberg enfrentou um depoimento ao Senado americano de aproximadamente 5 horas de duração, explicando as políticas de dados da empresa, regulamentação dos dados e parceiros, e como a Cambridge Analytica conseguiu violar os termos de uso da plataforma ao recolher e analisar informações de usuários a partir do próprio FB. Devido ao episódio, a empresa perdeu US\$ 35 bilhões em valor de mercado. “A audiência conjunta foi realizada entre os comitês de Justiça e do Comércio, Ciência e Transportes, ambas do Senado dos EUA. [...] questionado por 44 senadores em uma sessão [...] Na quarta, será a vez da Câmara dos Deputados” (SIMÕES, 2018).

---

<sup>13</sup> “As part of the experiment, Facebook will categorize status updates about politicians and policy issues by adult Facebook users in the US as positive, negative or neutral. The company also stressed that it will anonymize the aggregated data reports before they hand them over to ABC and BuzzFeed.”

<sup>14</sup> Ex-diretora de desenvolvimento de negócios da Cambridge Analytica, no livro *Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque*.

<sup>15</sup> Chief Executive Officer – termo em inglês para designar o mais alto cargo em uma empresa.



A Cambridge Analytica teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu prever e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais The Guardian e The New York Times (BBC NEWS, 2018).

Durante a sessão, Mark Zuckerberg assumiu o erro de não proteger os dados dos usuários de sua plataforma, e de ter falhado ao não impedir que informações falsas circulassem na rede social, além de deixar que uma empresa terceirizada tivesse acesso às informações sem o consentimento dos seus proprietários para uso na corrida presidencial americana, de 2016, e na campanha de saída do Reino Unido da Comunidade Europeia, o chamado Brexit. Com relação à eleição americana, há fortes suspeitas de que esse fato tenha auxiliado iniciativas russas em favorecer a eleição do então candidato à presidência Donald Trump, “Proteger nossa comunidade é mais importante que maximizar nossos lucros [...] nós temos agora muito trabalho para reconstruir uma confiança” (SIMÕES, 2018). Durante o depoimento do CEO. no Senado americano, as ações do FB subiram 4,5%, a maior alta da empresa em quatro anos.

Como forma de limitar e proteger o uso de dados de usuários para fins comerciais ou desenvolvimento de produtos nas plataformas, o conceito de *privacy by design*, que falamos anteriormente na tese, defende que a arquitetura de informação, a estrutura de banco de dados de um *site*, sua interface e *software* devem ser projetados com uma preocupação inicial desde a concepção do projeto em manter e resguardar a privacidade e segurança dos seus visitantes e usuários como um requisito padrão. O Internet Lab<sup>16</sup> define o conceito de alguns princípios, como objetivo central de manter *privacy by design* como elemento fundamental para a proteção e privacidade, sendo incluído em diretrizes oficiais como regulamentações do setor, como aqui no Brasil, dando origem à LGPD.

Privacidade desde o projeto significa que a proteção de dados deve ser integrada desde o início ao projetar um sistema e, portanto, as salvaguardas acima mencionadas devem ser fornecidas desde o início também. A obrigação de cumprir recai sobre o controlador de dados e o processador de dados. Esta abordagem reduz a dependência de salvaguardas políticas, mas, em vez disso, regula o processamento de dados pessoais através da própria tecnologia. Deve-se notar que a adoção tem sido lenta, visto que empresas e governos resistem a limitar o futuro capacidades ou aspirações de minerar dados pessoais, mesmo que sejam legalmente supostos para

---

<sup>16</sup> Centro independente de pesquisa multidisciplinar que promove o debate acadêmico e a produção de conhecimento nas áreas do Direito e tecnologia, sobretudo no campo da internet. Constituído como uma entidade sem fins lucrativos, o InternetLab atua como ponto de articulação entre acadêmicos e representantes dos setores público, privado e da sociedade civil, incentivando o desenvolvimento de projetos que abordem os desafios de elaboração e implementação de políticas públicas em novas tecnologias, como privacidade, liberdade de expressão e questões ligadas a gênero e identidade (INTERNETLAB, 2021).

limitar o “deslocamento” de propósito<sup>17</sup> (INTERNET LAB, 2018, p. 77, tradução nossa).

Ao encontro da premissa do *privacy by design*, diversas iniciativas ao redor do mundo estão inclinadas a exigir melhores políticas de privacidade e segurança para os usuários de dispositivos conectados à internet, como a própria LGPD. Em resposta ao movimento e a todos os escândalos envolvendo coleta e mau uso de dados privados de usuários, principalmente do FB, a empresa Google lançou a chamada Privacy Sandbox, cartilha que prega como deixará de utilizar os chamados *third party cookies*, ou *cookies* de terceiros, para segmentação de campanhas publicitárias em seu produto Google Ads. Intitulada como *Building a more private web*, a cartilha defende o uso de dados corretamente, sem o cruzamento ou troca de informações entre parceiros comerciais, por exemplo, sem recolher informações pessoais sobre os usuários a partir da implementação de arquivos de texto em seus navegadores (os *trackers*, rastreadores, arquivos de *cache*, *cookies* ou *pixel*, no caso do FB).

As identidades individuais por site podem se unir entre os primeiros, devido a ações do usuário como “Pagar com PayPal”, “Fazer login com o Facebook” ou “Usar seu endereço de e-mail como nome da sua conta”. Os navegadores devem ajudar seus usuários a entender as implicações de permitir essa associação e devem oferecer suporte a maneiras de acessar sites que não exigem essa associação entre sites<sup>18</sup> (MICHAELKLEBER, 2022).

Nesse sentido, recorreremos à afirmação de Shoshana Zuboff (2020, p. 26) quando menciona a lógica do capitalismo de vigilância não estar diretamente relacionada a uma tecnologia específica, ou um tipo de *modus operandi* de todas as empresas e iniciativas que trabalham com dados, mas “é uma forma de mercado que é inimaginável fora do meio digital, mas não é a mesma coisa que o digital [...] é o capitalismo o responsável por atribuir a etiqueta de subjugação e impotência, não a tecnologia”. E ao encontro dessa visão, há muitas especulações no mercado referentes às grandes empresas líderes quando o assunto é receita e investimento em tecnologia, e o que, de fato, elas fazem com todas as informações coletadas

---

<sup>17</sup> “Privacy by design means that data protection must be integrated from the outset when designing a system and so the aforementioned safeguards must be provided from the inception too. The obligation to comply falls on both the data controller and the data processor. This approach reduces reliance on policy safeguards, but instead regulates processing of personal data through the technology itself. It must be noted that adoption has been slow, as companies and governments are resistant to limit future capabilities or aspirations to mine personal data, even as they are legally supposed to limit ‘purpose creep’.”

<sup>18</sup> “Per-site identities can become joined across first parties, due to user actions like ‘Pay with PayPal’, ‘Log In with Facebook’ or ‘Use your email address as your account name’. Browsers should help their users understand the implications of allowing that joining, and should be supportive of ways to access sites that do not require that cross-site joining.”

sobre os indivíduos que utilizam dessas plataformas. A lógica do capitalismo de vigilância mantém a informação nas mãos de iniciativas que detém o poder, ou seja, o conhecimento sobre interesses, gostos e qualquer outro material que possa ser utilizado para monetização ou moldar conceitos, ideias e comportamentos da população.

E, justamente sobre esse aspecto, é que novamente o FB, em 2019, foi alvo de críticas sobre a possível prática velada de coleta de dados para testar uma nova ferramenta de reconhecimento facial, com a *#10yearschallenge*, que supostamente iniciou como uma brincadeira estimulando os usuários a publicar duas fotos lado a lado com a diferença de 10 anos para comparação. Novas especulações surgiram questionando a veracidade do conteúdo, sondando se a verdadeira razão para o lançamento da “brincadeira” seria o teste e alimentação de *software* com dados sobre envelhecimento da população. Essa questão vai ao encontro de aspectos tidos como direito e garantia dos usuários de Internet no Brasil, a partir do MCI desde 2014, que afirma como direito e garantia do usuário o expresso consentimento sobre o uso de suas informações coletadas, porém, muitos desses dados constam em termos e contratos de uso de aplicativos ou plataformas, que os usuários são obrigados a aceitar sob pena de não usufruir do serviço, como os contratos por adesão.

Nesse sentido, alguns aspectos engendram o que David Lyon (2018, p. 151) denomina como “cultura da vigilância”, cuja “característica-chave é que as pessoas participam ativamente em uma tentativa de regular sua própria vigilância e a vigilância sobre outros”, ou seja, estamos mais alertas sobre questões que envolvem nossa privacidade, como coletam e utilizam nossas informações, mas, também, colaboramos com nosso livre envolvimento em mídias sociais, por exemplo, ou monitorando câmeras domiciliares de segurança. A cultura da vigilância é um “produto das condições contemporâneas de modernidade tardia, ou simplesmente, da modernidade digital” (LYON, 2018, p. 153), pois também alimenta uma grande indústria capitalista e governamental.

Portanto, para avançarmos na perspectiva de exploração de nosso objeto empírico, e buscarmos os sentidos de *tecnosegurança* nas interfaces do FB, primeiramente, apresentamos nossa *flânerie* na plataforma desde seu lançamento na *web*, e, posteriormente, escavamos suas principais funcionalidades e polêmicas envolvendo o *big data* e a monetização a partir de informações cedidas por seus usuários. Além disso, verificamos como aspectos relacionados à privacidade e à segurança dos dados são preocupações do modelo de sociedade em que vivemos atualmente, conforme debate desenvolvido no Capítulo 2, e que, de certa maneira, conferem ao FB um *status* de confiabilidade. Seus usuários aceitam ceder suas informações para os *data centers* do FB, mas, de algum modo, não confiam com sua distribuição à

terceiros, parceiros comerciais e governos. Assim, pretendemos explorar como se cria a arquitetura da confiança na plataforma que promete a eficiência do segredo aos seus quase 5 bilhões de usuários ativos mensalmente, que entregam a “chave” para o acesso à sua intimidade, rotina, interesses e comportamentos para o FB. No Capítulo 4, a seguir, iremos apresentar a exploração e análise do objeto, iniciando pela *flâneria* e apresentando as constelações que compõem a galáxia da *tecnosegurança* pela ambiência FB.

## 4 CONSTELAÇÕES

Com o objetivo de apresentar ao leitor(a) como a etapa de realização da análise e operação de nossa empiria se deu, em direção a compreender como se atualizam sentidos durante de *tecnosegurança* pela ambiência FB, o presente capítulo foi organizado em algumas etapas. A primeira delas contextualiza o processo metodológico da *flâneria* e apresenta uma característica muito forte de deixar “ser olhado” pelo objeto de pesquisa, pois foi a partir de intensa e constante revisita às imagens da empiria é que percebemos o que nos olha nas materialidades, certamente em duplo contágio pesquisadora *versus* objeto.

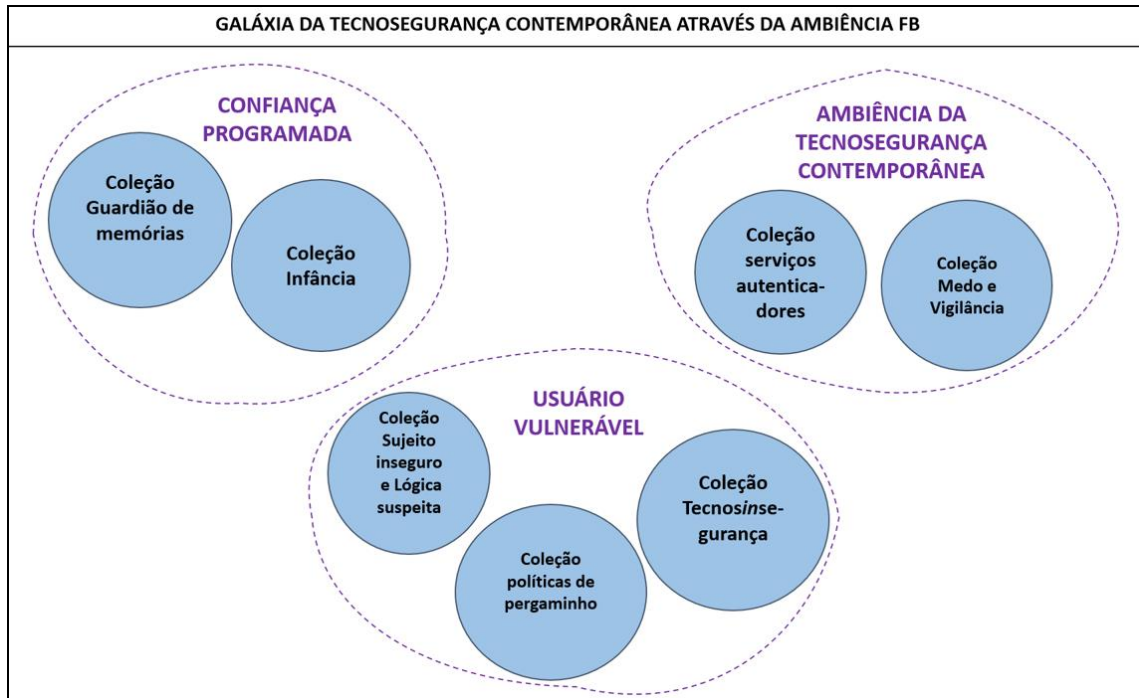
Após evidenciar o processo de *flâneria*, apresentamos como a coleta aconteceu – seleção, escolha e organização de imagens das interfaces – respondendo ao critério de criar 7 coleções, organizando as capturas de tela a partir de *ethicidades*, imaginários que fomos percebendo num processo de dissecação, inspirados em Kilpp (2002a). A organização das coleções demonstra que, em alguns casos, as interfaces podem se repetir em mais de uma coleção, portanto, não são excludentes, mas optamos por evidenciar determinados aspectos do que outros, esse critério ficará mais claro quando as coleções forem apresentadas e contextualizadas.

Após a navegação pelas interfaces já organizadas em coleções, estabelecemos conexões entre elas, ou afinidades eletivas, que deram origem a união de quatro constelações. A partir delas é que compreendemos a cartografia da *tecnosegurança* pela ambiência FB, pois através do método de criar mapas que

A metáfora da constelação certamente foi uma das inspirações mais importantes de Walter Benjamin. É nas ‘Questões introdutórias de crítica do conhecimento’ de sua tese de Livre-Docência, publicada, no Brasil, sob o título de Origem do drama barroco alemão, que o filósofo alemão, em meio a reflexões bastante abstratas, alivia o trabalho de compreensão do leitor recorrendo a imagens de estrelas: ‘As ideias se relacionam com as coisas como as constelações com as estrelas’ (OTTE; VOLPE, 2000, p. 37).

Portanto, por meio das três constelações é que verificamos como os sentidos de *tecnosegurança* se atualizam nas materialidades analisadas. Para fins de compreensão do(a) leitor(a), desenvolvemos a composição, a seguir, que sintetiza as coleções e as respectivas constelações criadas a partir da cartografia:

Figura 42 - Galáxia das constelações



Fonte: Elaborado pela autora (2022).

A primeira constelação, Confiança Programada, reside na construção de *ethicidades* ancoradas no apelo constante criado pela plataforma FB em criar uma programação de laço de confiança com o usuário, seja pela construção de um imaginário fundamentado em um universo infantil, colorido e divertido, seja pela relevância em criar um ambiente de aconchego e cuidado, embasado na força de uma comunidade segura, ou, então, em fortalecer um imaginário de constantes lembranças felizes, memórias e nostalgia.

A segunda constelação, Usuário Vulnerável, apresenta três coleções, que compõem imagens das interfaces do FB que promovem constante tensão com o usuário a partir da provocação de uma presença suspeita, de um suposto inimigo ou ameaça externa àquele ambiente. Portanto, são imaginários identificados nas imagens que corroboram com a construção do sujeito inseguro de Lemos (2009) e da construção de *tecnosinsegurança* constante em alguns ambientes dentro da FB. Isso fica mais evidente quando fizemos o exercício de escavação das seções associadas a sua Privacidade e Segurança, assim como Configurações da Conta, e, também, quando verificamos as Políticas e Termos de uso das plataformas.

Por fim, a terceira constelação, Ambiente da *Tecnosegurança* Contemporânea, contém capturas de interfaces de ambientes paralelos ao FB, ou seja, mapeamos construções *tecnoculturais* em interfaces que retroalimentam (e são alimentadas) pela *tecnosegurança* do

FB. Isso nos conduz à reflexão de que o FB é reflexo, mas, também, produtor dessa *tecnosegurança* que convive na nossa relação com as tecnologias digitais, sejam elas associadas aos sistemas de pagamento, câmeras de monitoramento, vigilância urbana, reconhecimento facial, e outros aspectos que já debatemos no Capítulo 2 dessa tese. Encerramos o capítulo de exploração da empiria com nossas considerações a respeito da forma como cada uma das três constelações constroem a *tecnosegurança* pela ambiência FB.

#### 4.1 *Flâneur* e colecionadora

Conforme sinalizamos algumas vezes ao longo desse trabalho, nossa *flânerie* pelas interfaces do FB vem acontecendo desde o ingresso no PPGCC da UNISINOS, quando o objeto da tese ainda estava em uma configuração anterior, mas com foco na mesma empiria. Portanto, temos um vasto volume de capturas de telas da interface da plataforma FB via acesso na *web*, ou seja, dentro do endereço eletrônico <https://www.facebook.com> e também na versão do aplicativo para o sistema IOS.

Para a operacionalização de nossa análise, nosso movimento inicial foi partir, então, do navegador para internet via *desktop* Google Chrome, onde fomos ao endereço eletrônico <http://www.facebook.com>, onde “aterrizamos” na página inicial de *login*, área dedicada ao usuário acessar sua conta específica e das páginas as quais gerencia, ou, então, cadastrar uma nova conta. Somos usuários no FB há 11 anos<sup>1</sup>, acompanhamos diversas atualizações do *layout* da plataforma e guardamos alguns registros, mais especificamente desde 2018 (e algumas telas desde 2014-2015 – período em que o FB fez parte de nossa empiria na dissertação do mestrado, conforme comentamos na introdução dessa tese). Portanto, algumas capturas que serão analisadas aqui foram retiradas “do fluxo” da *web*, ou seja, fazem parte de um ato de recolher e colecionar imagens, num constante tensionamento de tempos e versões de atualizações (de *layout*) da interface gráfica oferecida ao usuário final.

Em síntese, o movimento aconteceu operacionalmente da seguinte maneira; a *flânerie* pela plataforma nos levou a perceber a presença de algumas características do FB envolvendo diversos tipos de manifestações a partir das imagens, conforme já mencionamos na introdução dessa tese. A primeira delas foi uma espécie de demonstração de “cuidado” com o usuário através de referências à infância e ao uso do desenho. Por exemplo, logo após o *login*, ao acessar nossa área “privada”, ou *homepage* dentro do FB, chegamos no *newsfeed*, ou *feed* de

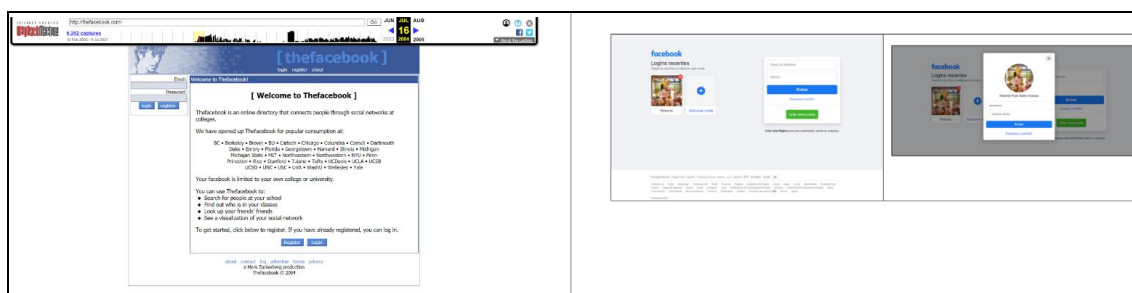
---

<sup>1</sup> Criamos nosso perfil de usuário no FB em 2011 quando atuávamos em agência de publicidade que gerenciava páginas comerciais de clientes na plataforma FB.

notícias. Lá, encontramos a pergunta: “No que você está pensando, Roberta?” e um espaço dedicado ao preenchimento da resposta, acompanhado de sugestões de figurinhas e *emojis* que também perguntavam “Como você está se sentindo?”.

Começamos a refletir sobre esses espaços “próprios nossos” dentro do FB, o que de nosso tinha ali? E se contássemos de verdade ao FB o que estávamos sentindo naquele momento, será que algum *emoji* iria nos abraçar virtualmente? Além disso, toda a construção da interface colorida, repleta de gente feliz, de balões e bandeirinhas nos remeteu diretamente à festa de aniversário infantil<sup>2</sup>, onde a celebração tem como ambiência principal em “volta da mesa do parabéns”, bolo, balões e velas coloridas.

Figura 43 - Montagem comparação de *layout* para a presença da *ethicidade* infância na página de *login* da primeira versão da plataforma The Facebook em 2004 *versus* versão 2022



Fonte: Adaptado de Internet Archive (2004; 2022)<sup>3</sup>.

Concomitantemente, a plataforma mostrava coisas muito relacionadas a outros aspectos tidos como “sérios” na nossa rotina, como lembranças de eventos que participamos, atividades anteriores, previsão do tempo, ambiente profissional, histórico de trabalho, anúncios que remetiam a nossa possibilidade de consumo, pagar contas. Por outro lado, também remetia fortemente a um clima aconchegante, onde imaginávamos ter a semelhança com uma brisa de verão, temperatura constante de 24° e um lindo sol, com estética limpa, organizada e cheia de limites, linhas e demarcações para onde deveríamos seguir o caminho.

Todas essas manifestações foram nos provocando a coletar essas imagens da interface, chamando a atenção para possíveis sentidos associados às temáticas citadas anteriormente. Dessa maneira, outro movimento metodológico influenciado pela prática do recolhimento das imagens foi justamente juntar, agrupar, criar coleções a partir dessas possíveis similaridades encontradas em um processo de dissecação. Esse arranjo de capturas foi realizado ao longo da

<sup>2</sup> No momento que refletimos sobre a festa infantil, estávamos realizando – fora do FB, uma celebração de aniversário de 2 anos da Valentina, muito restrita devido à pandemia, mas que continha balões em volta de uma mesa com bolo, enfeites da personagem Minnie Mouse/Disney e alguns docinhos. A data se aproximava de setembro de 2020.

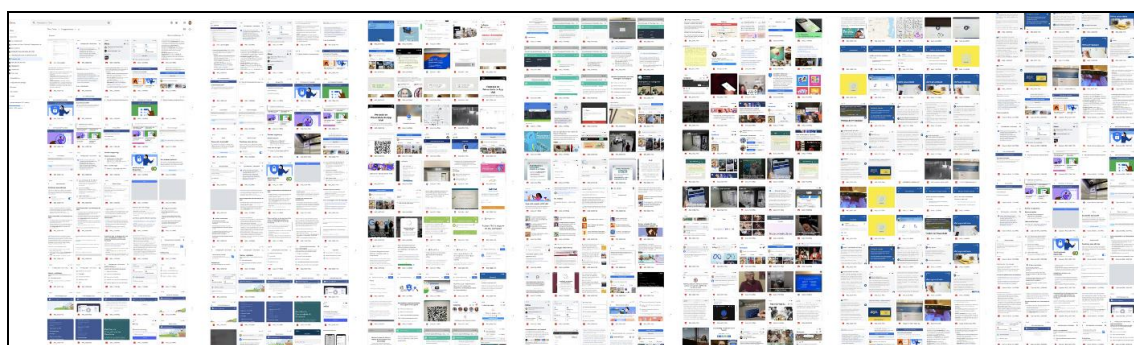
<sup>3</sup> Maiores informações em <https://web.archive.org/web/20040212031928/http://www.thefacebook.com>.



*flâneria* e não necessariamente foi algo sequencial, mas que durante o processo de refletir sobre os sentidos de *tecnosegurança* que *duram* ali é que essas coleções foram emergindo e nos dando apoio para compreendermos que elas poderiam ser nossas primeiras impressões sobre o objeto de pesquisa.

Nossas práticas de coleta foram armazenadas em três ambientes diferentes, um deles foi a ferramenta Google Drive, onde fomos fazendo *upload* das capturas de tela em nosso *smartphone* e também funciona como um *backup* de nossas imagens salvas em outros dispositivos, como o *notebook*. Lá criamos uma pasta que contém aproximadamente 400 imagens de interfaces, conforme registro a seguir. Além disso, armazenamos arquivos do Microsoft Power Point com demais capturas realizadas, não apenas do FB, mas de outros ambientes na *web* e em aplicativos que encontramos manifestações associadas ao que estávamos coletando dentro do FB. Optamos por essa maneira de operar pois o nosso *notebook* não possui capacidade de armazenamento e tampouco carregamento para grandes volumes de imagens, o que nos provocou diversos “sustos” ao longo do doutoramento, justamente por não carregar corretamente os arquivos em sua memória. Ao irmos salvando em arquivos menores, como o Power Point, otimizamos velocidade e armazenamento com o *hardware* que dispomos. Além disso, a capacidade de uso gratuito do Google Drive também foi extrapolada devido ao tamanho dos arquivos guardados.

Figura 44 - Armazenamento das interfaces no Google Drive

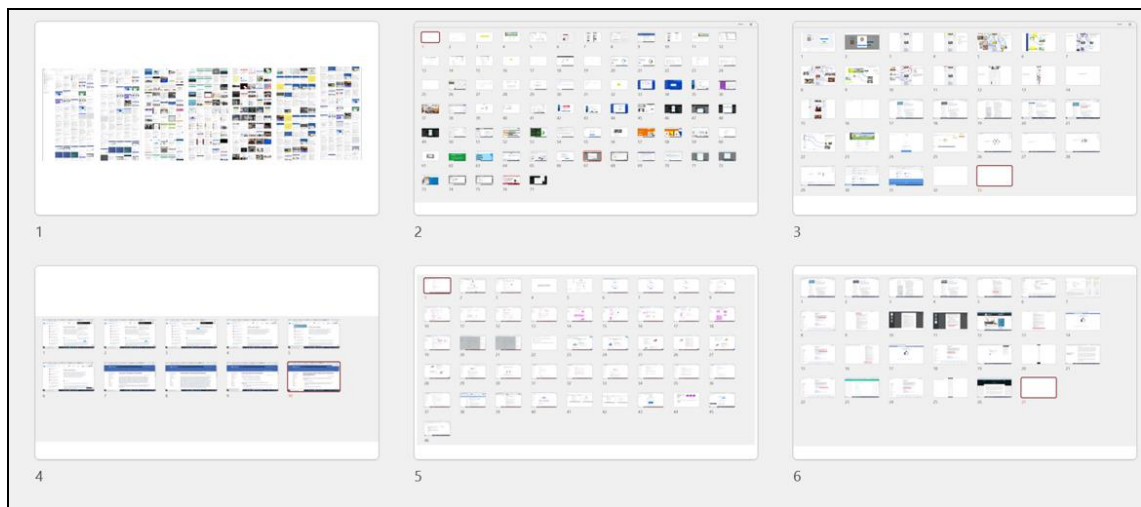


Fonte: Elaborado pela autora (2021).

Os arquivos em Power Point totalizam aproximadamente 150 capturas, conforme as imagens, a seguir, também demonstram o armazenamento. Estamos mencionando a quantificação apenas para fins de informação, não temos intenção de utilizar a mensuração como algum critério ou método para auxílio na análise. Na verdade, o ato de recolhermos interfaces aconteceu inicialmente sem um motivo específico, conforme mencionamos acerca da figura do trapeiro, recolhemos do fluxo aquelas imagens que foram oferecidas pelo

*software*. Porém, o ato de colecionar foi intencional, a partir da dissecação de algumas interfaces que demandou elencar para as demandas do objeto e da pesquisadora respondendo aos critérios que intitulam as coleções que foram emergindo. Além disso, outras coleções, conforme apresentaremos mais adiante no texto, foram criadas com a intenção clara da pesquisadora em escavar partes específicas da plataforma, como Privacidade e Segurança no FB, por exemplo.

Figura 45 - Armazenamento das interfaces no Microsoft Power Point



Fonte: Elaborado pela autora (2021).

Retomando as palavras de Maciel (2009), lembramos que o ato de criar coleções como um processo metodológico responde à forma de ajuntamento, incluindo itens que apresentam alguma característica afim. Dessa maneira, nossa prática representa claramente uma tentativa de “matar o fluxo” dessas imagens, conforme Kilpp (2010), para refletirmos sobre os sentidos ali enunciados, caracterizando uma das etapas da metodologia das molduras, proposta pela mesma autora.

Portanto, o movimento de dissecar essas imagens foi para compreendermos a interface como um espaço em que há *ethicidades*, enunciações circunstanciadas ao ambiente FB. Compreendemos que diversos imaginários são convocados nas imagens tendo a interface como um espaço onde comparecem tendências de *software*, dados e imaginários sociais e que também, por essas razões, deram origem às nossas constelações. A “mesa operatória” da dissecação de nossas materialidades se deu a partir das imagens das interfaces, que deram origem às coleções, quando agrupamos conjuntos de imagens recolhidas da *web* e do aplicativo do FB por meio de determinados critérios de agrupamento. Esse agrupamento nos

auxiliou a criar uma cartografia, ou mapa das constelações, com inspiração em Benjamin (2006), conforme nos apresenta Canevacci (1997, p. 111):

O verdadeiro método benjaminiano, portanto, não é ‘o’ método, mas sim o reconhecimento de que a criação de novos objetos de estudo, campos de pesquisa, esferas de interesse implica, mais do que a aplicação escolástica de fórmulas ‘eternamente’ tiradas dos cânones, a paralela (e isomórfica) elaboração de novos métodos.

Para avançarmos em direção ao procedimento realizado de escavação e dissecação das interfaces, apresentaremos, a seguir, cada uma das constelações e suas coleções, ou estrelas, que são os corpos celestes que carregam luz própria iluminando a compreensão da galáxia da *tecnosegurança* pela ambiência FB.

## 4.2 Primeira constelação - Confiança Programada

Como diz Canevacci (1997, p. 106), dar o “[...] o senso luminoso do conhecimento” a partir das estrelas que compõem a primeira constelação, intitulada Confiança Programada, vamos apresentar cada uma das coleções, agrupamentos criados com as dissecações de interfaces do FB. Essa constelação é composta por 2 coleções, sendo elas a) infância e b) guardião de memórias. Percebemos que, em cada uma das coleções, há **imaginários** e que dão origem às *ethicidades*, que são agenciados por **emolduramentos** no FB. Compreendemos que a constelação Confiança Programada opera com foco nessas duas *ethicidades* construídas a seguir.

### 4.2.1 Coleção Infância

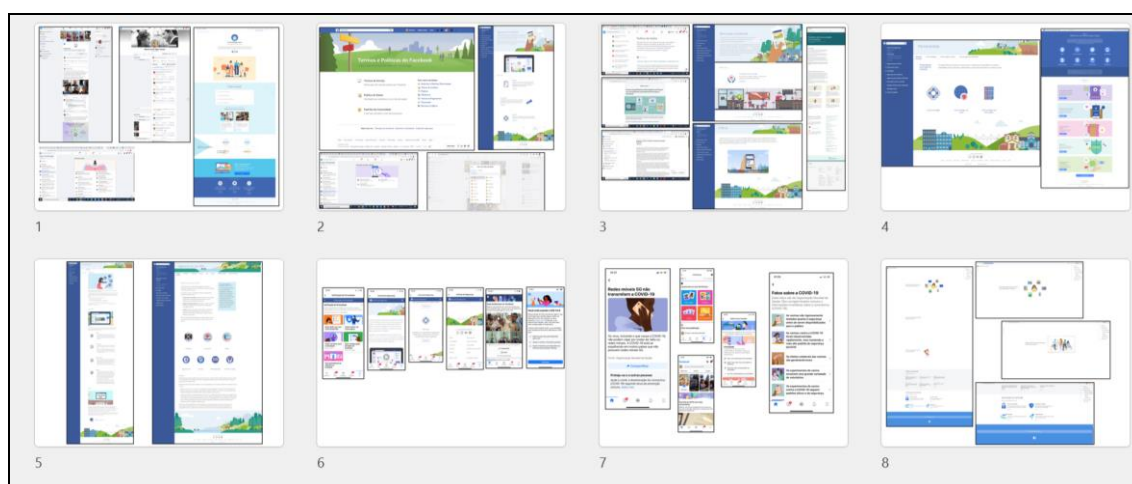
A coleção que nomeamos como **Infância** caracteriza-se por um agrupamento onde encontramos sentidos durante de um universo marcado fortemente pelo uso da ilustração e do desenho nas interfaces que coletamos. Nesse conjunto, percebemos a manifestação da “infância” nas interfaces da plataforma que também se anunciam como áreas “particulares” dos usuários, como aquelas onde o *software* procura personalizar o conteúdo a partir dos dados interpretados pelos interesses de cada indivíduo por sua manifestação através do FB, conforme vimos no capítulo anterior. Também são espaços que demandam acesso somente via senha, e que são extremamente relevantes para a lógica de monetização: **newsfeed** e **timeline**. São áreas onde são inseridos os anúncios e conteúdos patrocinados de parceiros comerciais do FB. Sem dúvida são espaços onde os usuários são retidos por muito tempo,

pois, ao propor entrega de impressões de anúncios, conseqüentemente, há acessos e visualizações de usuários carregando esses conteúdos pagos. Em termos publicitários, poderíamos dizer que remete à lembrança do “horário nobre” (KILPP, 2010) da TV aberta.

Partimos para o exercício de dissecação dessas interfaces, que nos indicou algumas *ethicidades*, que são agenciadas por imaginários construídos entre os agentes comunicacionais envolvidos. Portanto, realizamos a dissecação dessas interfaces ao criarmos associações com imaginários e memórias contidas nas imagens. Utilizamos como referência a proposta das imagens dialéticas de Didi-Huberman a partir de Walter Benjamin:

Benjamin associou conhecimento a imagens dialéticas, ou seja, à presença de imagens relativas a diferentes experiências históricas presentes num mesmo momento, numa mesma constelação, em conflito. A partir de tensões aparentes no imaginário do presente, seria possível a busca de um passado perdido. O que é fundamental no conceito de imagens dialéticas para o estudo da memória é que o confronto de diferentes formas de experiência humana, advindas de diferentes condições históricas, seria capaz de possibilitar o passado a intervir no presente trazendo conhecimento. Este conhecimento, no entanto, não se dá sob a forma de razão, que tem por fundamento a ‘verdade’, mas sob a possibilidade de uma prática libertária em relação ao passado, a redenção (SANTOS, 2003, p. 149).

Figura 46 - Coleção Infância



Fonte: Elaborado pela autora (2021).

Apoiados na proposta de Benjamin, o agrupamento da coleção nomeada como **Infância** contém imagens oriundas de um processo de recolhimento pela *web* e aplicativo, e da dissecação, e apresentam sentidos associados fortemente à uma temática colorida, feliz, alegre e divertida do universo de criança. Com predomínio da ilustração, animação (em formato .gif) e desenho, a coleção conta com interfaces encontradas na seção **Newsfeed**, **Timeline**, **Segurança e Privacidade no FB**. Porém, não temos a pretensão de retirar uma quantidade específica ou a totalidade das interfaces, não faz sentido para o questionamento da

pesquisa, para nossa metodologia, nosso prazo de finalização dessa tese e tampouco a capacidade de nosso equipamento disponível para realização da pesquisa. A maneira que organizamos as capturas na coleção não segue uma ordem específica, apenas foram organizadas da melhor maneira para auxiliar na visualização do(a) leitor(a) na versão impressa ou digitalizada de nossa tese. Mas, se desejar explorar melhor cada captura, sugerimos então, que aponte a câmera do celular para o QRCode (já assumindo aqui a audiovisualização da pesquisa) para acessar a coleção composta de interfaces agrupadas<sup>4</sup>.

Figura 47 - Código QR para acessar imagens das interfaces que compõem a coleção Infância



Fonte: Elaborado pela autora (2021).

Tendo o “bisturi” nas mãos para intervir na imagem, começamos a nos questionar sobre os imaginários, que mundos haviam sido reconvocados a partir da interface? Não estamos nos referindo especificamente às mídias ou ao suporte, mas, na verdade, a quais imaginários são construídos aqui na interface? Quais memórias são evocadas? Como se atualizam sentidos *tecnoculturais* nesse ambiente? Portanto, para a dissecação, utilizamos um esquema de cores que indica as referências que a interface faz à algumas *ethicidades*, com base nesses imaginários reconvocados. Entendemos que há muitos indicativos da construção de um ambiente feliz, colorido, alegre, povoado de amigos reunidos numa mesma celebração. Por isso, entendemos que há sentidos de um universo infantil sendo construído, não apenas pelas cores e formas, mas, justamente, por associações que carregam imaginários contidos nas imagens apresentadas ao usuário.

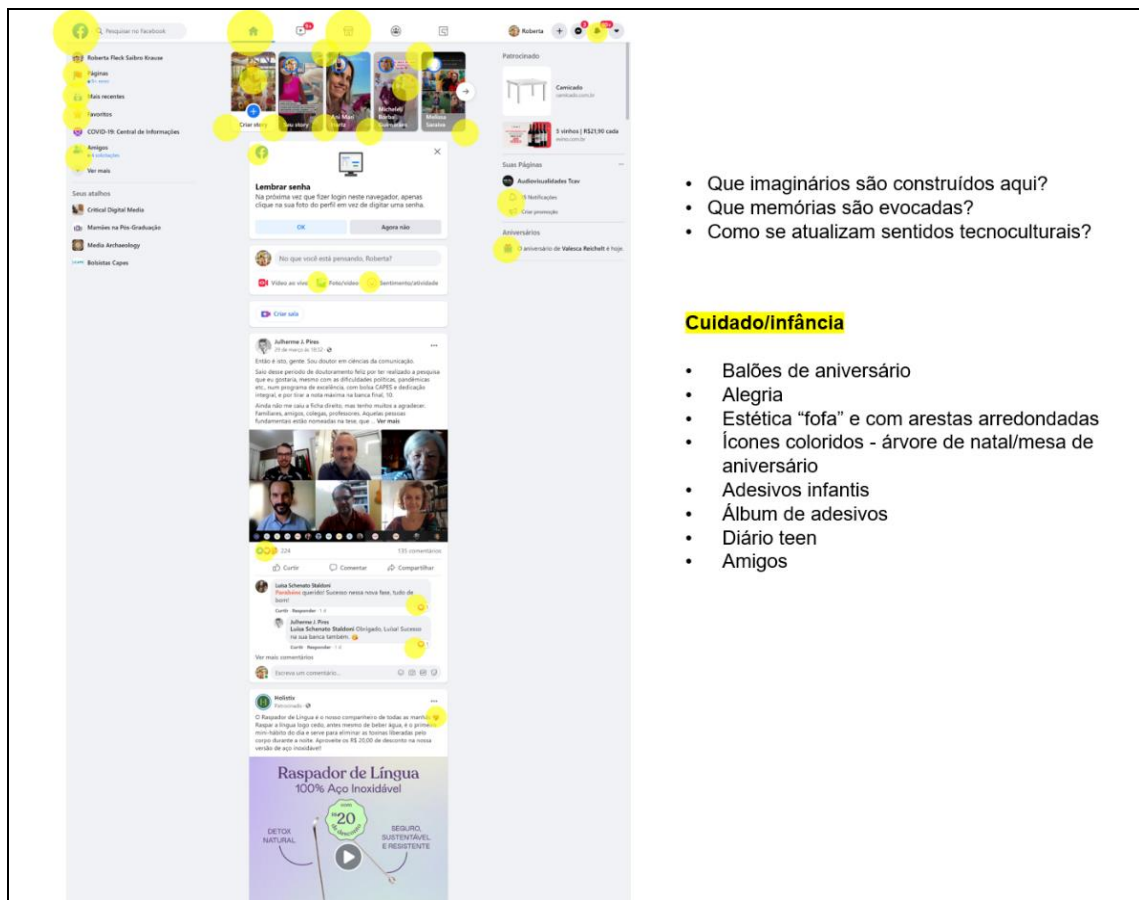
Para “sujar” as mãos com o objeto e, de fato, intervir na imagem, dissecamos algumas das interfaces da coleção criando inúmeras indicações com associações a imaginários atualizados nesse ambiente. Optamos por selecionar determinadas interfaces que entendemos como aspectos complementares ou que tensionam nosso objeto de encontro e ao encontro de nossa problematização, e estas foram selecionadas para serem expostas no presente capítulo. O caráter fofo e alegre tende a montar uma construção positiva que nos remete à infância, ou, até mesmo, uma festa de aniversário, conforme mencionamos anteriormente. O imaginário do

---

<sup>4</sup> Basta acessar a funcionalidade do aplicativo da câmera fotográfica no celular, apontar para o código do texto e abrir a página na *web* que contém o arquivo das imagens, gerando um arquivo com extensão pdf.

*software*, da máquina, ou do dispositivo que coleta, armazena e monetiza nossas informações, a partir da geração de dados (conforme vimos anteriormente no Capítulo 2), desaparece da “festa de aniversário”, propositalmente, visto que, é de interesse da plataforma conduzir o usuário ao maior tempo de consumo dentro de seu ambiente, sendo essa uma das métricas de monetização do FB – tempo de permanência na página para entregar impressões a seus parceiros comerciais/anunciantes. Vejamos as indicações do processo a seguir:

Figura 48 - Indicação da dissecação da interface *newsfeed* - coleção Infância



- Que imaginários são construídos aqui?
- Que memórias são evocadas?
- Como se atualizam sentidos tecnoculturais?

#### Cuidado/Infância

- Balões de aniversário
- Alegria
- Estética “fofa” e com arestas arredondadas
- Ícones coloridos - árvore de natal/mesa de aniversário
- Adesivos infantis
- Álbum de adesivos
- Diário teen
- Amigos

Fonte: Elaborado pela autora (2021).

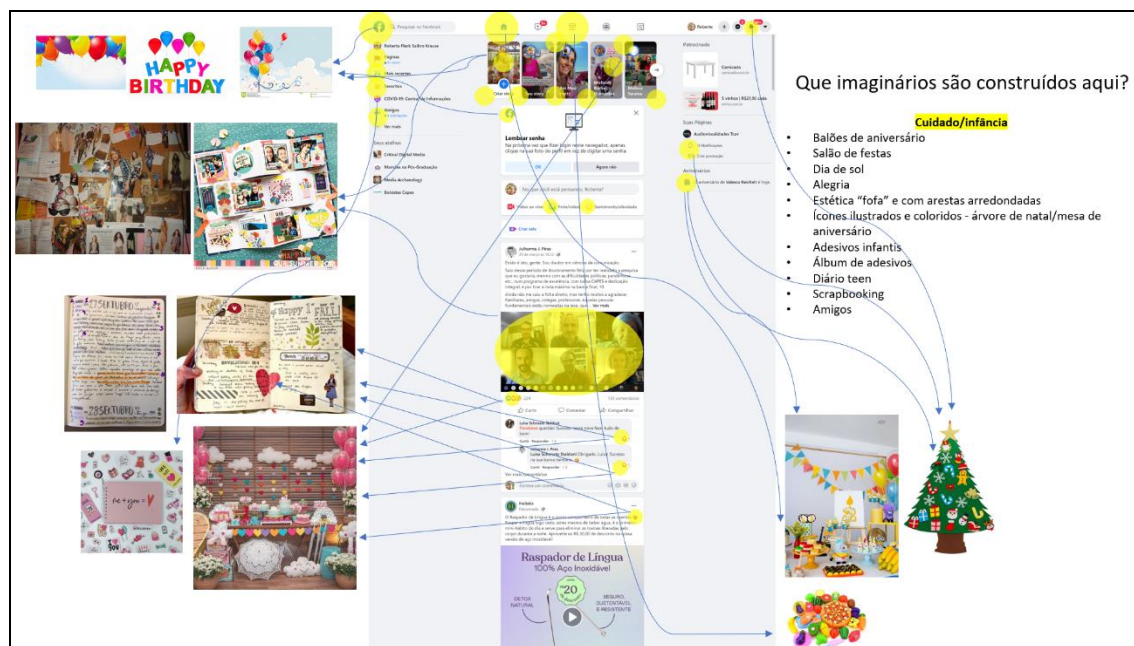
Além disso, qual a razão para “ir embora da festa?”. Parece-nos que esse ambiente se faz de uma estética infantil, divertida e de cuidado, provando ao usuário que o mundo feliz acontece, na verdade, dentro da *newsfeed* do FB. E, justamente, sobre o papel da imagem nessa construção do mundo, Flusser (2002, p. 9) comenta que “o homem, ao invés de se servir das imagens em função do mundo, passa a viver em função de imagens. Não mais decifra as cenas da imagem como significado do mundo, mas o próprio mundo vai sendo vivenciado como um conjunto de cenas”. Nesse sentido, podemos inferir que a intenção de criar essa associação de resgate à infância carrega aspectos como pureza, diversão e alegria, o que



auxilia a proposta de se viver fora de perigo, conforme viver em comunidade a partir de Bauman (2003).

Recorremos à Convenção dos Direitos da Criança, organizado pelo Fundo das Nações Unidas para a Infância (UNICEF, 2022), ao afirmar que “reconhecendo que a criança, para o pleno e harmonioso desenvolvimento de sua personalidade, deve crescer no seio da família, em um ambiente de felicidade, amor e compreensão”. Portanto, percebemos na dissecação das interfaces a marcação da infância em diversos momentos, visando criar um ambiente de proteção e cuidado, seja recorrendo ao uso da ilustração e do desenho, mas também pelo texto, a disposição de conteúdo e as associações imagéticas ofertadas por palavras-chave que buscamos na própria ferramenta de busca, dentro do FB e no Google imagens, conforme a seguir:

Figura 49 - Dissecação da coleção Infância - *newsfeed*



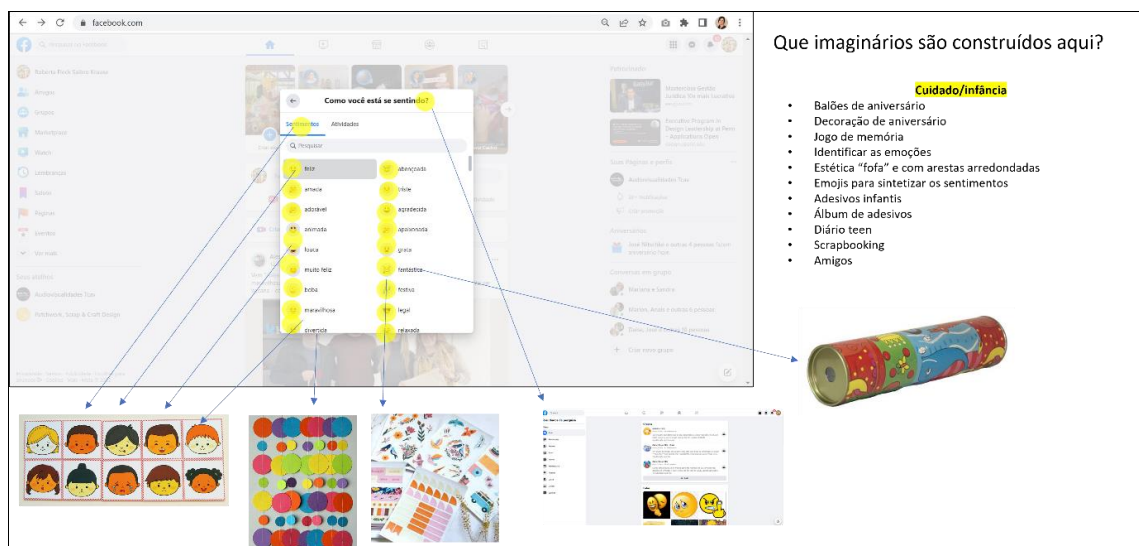
Fonte: Elaborado pela autora.

Também compreendemos que os imaginários reconvocados aqui remetem a construção infantil e outras associações imagéticas que fizemos. A dissecação como processo metodológico, que intervém nas imagens, demonstra que há diferentes imaginários contidos e que, ao fazermos o exercício de associá-los com palavras-chave, e de buscarmos outros imaginários (dentro e fora do FB), é possível compormos essa *ethicidade* pela ambiência FB mas que não é restrita a ela, e se manifesta em zonas paralelas ao FB.

Nesse sentido, recorremos à Kilpp (2002a, p. 4) quando propõe “o imaginário como o conjunto de marcas de enunciação das culturas (identidades coletivas), manifestas e visíveis

nos discursos, na arte, nos produtos culturais..., ou que são por eles mediadas”. Encontramos, na visão da autora, uma maneira de compreendermos a relação de imaginários e sentidos que constroem as *ethicidades* como “subjetividades virtuais” (KILPP, 2002a, p. 4) que residem circunstanciadas à determinadas ambiências. Em nossa empiria, permanecemos dissecando outras interfaces de territórios próprios aos usuários, ou seja, seções dentro da plataforma que são moldadas conforme a interação do usuário logado e seu histórico de uso do *software*, como a *timeline* a seguir:

Figura 50 - Dissecção da coleção Infância - *timeline*



Fonte: Elaborado pela autora (2021).

A dissecção demonstrada previamente indica a construção dos imaginários associados à infância, mas com muitas similaridades à dissecção da *newsfeed*, já que fizemos o mesmo exercício de buscar palavras-chave e associações com os *emojis* ofertados na interface. A plataforma provoca o questionamento “Como você está se sentindo?” e oferta como caminhos para a resposta mais de 100 opções de emoções (já sinalizadas com o gênero feminino, conforme cadastro realizado no banco de dados do perfil do FB) acompanhadas de expressões faciais específicas dos *emojis* (“calma, relaxada, inspirada, preocupada”, etc.). As classificações de emoções sugeridas pelo FB, a partir da ilustração, carregam o tom de diversão e inocência da infância pelo uso do desenho para demonstrar as emoções conforme a criança vai aprendendo a identificar o que está sentindo. Parece-nos que mesmo a opção “maldosa” ou “p... da vida” traz o *emoji* como recurso de alívio e comédia para algo sério sendo demonstrado no FB. O que nos auxilia a refletirmos sobre mesmo estando triste, para os “padrões” incentivados dentro do FB, a tristeza permitida é associada a um imaginário de leveza e diversão por meio do *emoji*. Inferimos que a única melancolia permitida, no FB, é



bem-vinda e estimulada se vier acompanhada de algo colorido e “fofo”, mascarando o real sentimento de quem está publicando o conteúdo para os demais usuários da rede.

Essa espécie de utopia criada em torno da promessa da internet é contextualizada por Chun (2016, p. 106, tradução nossa) desde seu surgimento, “embora essa ideia pareça incrivelmente ingênua para nós agora e parecesse mesmo naquela época (foi criticada fortemente em meados dos anos 1990 como *hype*<sup>5</sup>)”. Segundo a autora, a promessa reside claramente em:

Esta versão utópica do ciberespaço prometia soluções tecnológicas para problemas. Através de sua popularização, o ciberespaço estranhamente mudou de prever um futuro sombrio para sinalizar um futuro feliz, e a posição liberal sobre a tecnologia passou de protesto (por exemplo, os anos 1980 o movimento antinuclear que informou a visão cyberpunk de Gibson) para uma abordagem entusiasta. [...]<sup>6</sup> (CHUN, 2016, p. 106, tradução nossa).

Essa provocação ao constante escapismo do “mundo real” e pandêmico, estimulada nas interfaces do FB, permanece em outras seções na plataforma ainda em territórios “próprios” do usuário, mas também em territórios “do FB”, ou seja, nas interfaces das seções que não apresentam interesse comercial, personalização de conteúdo ou intenção/incentivo à interação do usuário com a plataforma. São informações mais “institucionais”, sem o convite para o usuário publicar algo.

Nesse sentido, já alertas para a seção Segurança, fizemos um movimento intencional de escavarmos a plataforma para verificarmos se em espaços, mesmo quando relacionados à privacidade, segurança e configurações da conta eram apresentados os aspectos associados à infância. Por isso, escavamos o percurso traçado para chegarmos até esses territórios ali dentro; seguimos a interface conforme ela vai indicando: encontramos na nossa página inicial, uma espécie de “home” (no sentido de *homepage* de um *website*), onde são ofertadas as informações principais sobre nossas preferências e opções de navegação pela plataforma. Por fim, buscamos o ícone de engrenagem, que simboliza, muitas vezes, as configurações de aplicativos e *softwares* na *tecnocultura*. Lá, praticamente escondido do restante da “festa da *newsfeed*”, estava a seta com menu *dropdown* para abrir as 5 opções de configurações da conta, estruturando, portanto, os conteúdos de Privacidade.

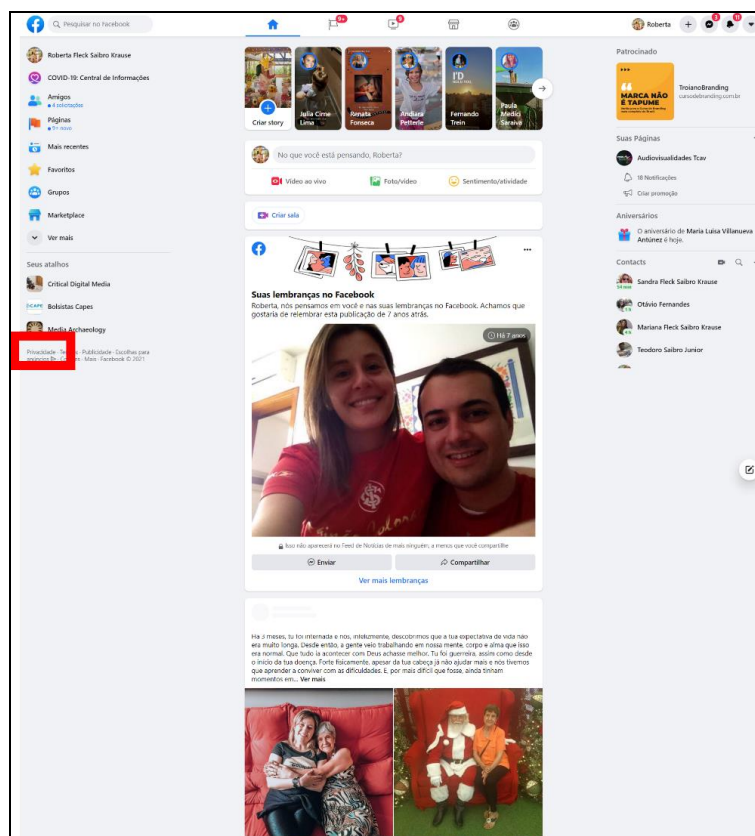
---

<sup>5</sup> “Although this idea seems incredibly naïve to us now and seemed so even then (it was criticized heavily in the mid 1990s as hype).”

<sup>6</sup> “This utopian version of cyberspace promised technological solutions to political problems. Through its popularization, cyberspace bizarrely moved from foretelling a dark future to signaling a happy one, and the liberal position on technology moved from one of protest (for example, the 1980s anti nuclear movement that informed Gibson’s cyberpunk vision) to one of enthusiastic embrace.”

No arranjo de telas capturadas na coleção, podemos verificar que a interface teve atualizações durante o período de realização dessa tese, ou seja, desde 2018 até 2022 (no sentido do espaço que se determina a realização da pesquisa). Vejamos na imagem, a seguir, que demonstra a sinalização onde é possível encontrar demais conteúdos que direcionam o usuário para além das seções que são comercialmente interessantes para o FB. É claro o entendimento que não há qualquer interesse em “tirar” o usuário dos ambientes *newsfeed* e *timeline*, já que as indicações para estar “fora da festa” ou em conteúdos como “Privacidade · Termos · Publicidade · Escolhas para anúncios · Cookies · Meta © 2022”, através de uma minúscula indicação na barra lateral inferior, sem qualquer destaque para estimular a atenção do usuário.

Figura 51 - Indicação da seção Privacidade na *newsfeed* do FB (abr. 2021)



Fonte: Elaborado pela autora (2021).

Ao clicarmos no *hyperlink* que direciona ao conteúdo sinalizado como *privacidade*, somos direcionados a um outro ambiente completamente diferente, sem nenhum artifício para manter o usuário na página. Na verdade, podemos inferir que é propositalmente hostil chegarmos em assuntos como “privacidade” dentro do FB, já que a maneira que a plataforma oferece esse aspecto ao usuário é com uma seção contendo 116.798 caracteres, o que

corresponde a um documento de oitenta e cinco páginas<sup>7</sup> de texto sem nenhuma referência “à festa” personalizada que acontecia na *timeline* e *newsfeed*, conforme a captura da tela a seguir demonstra:

Figura 52 - Captura da seção Privacidade dentro do FB



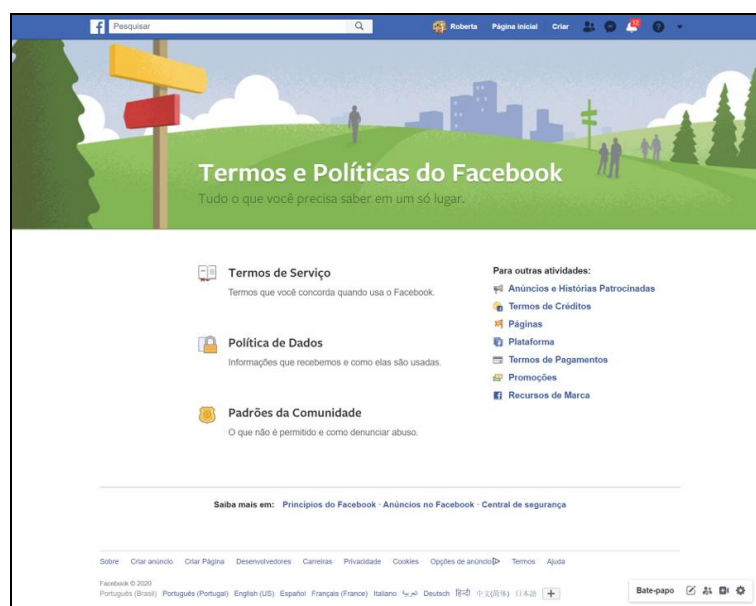
---

<sup>7</sup> Padrão no software Microsoft Word, fonte tamanho 12, espaçamento simples, 85 páginas de documento.

Fonte: Facebook (2021).<sup>8</sup>

Esse conteúdo está sendo ofertado por meio de uma extensa subdivisão, que iremos nos deter em outra coleção, com outros imaginários sendo reconvocados nas interfaces. Porém, com o intuito de apresentarmos ao(à) leitor(a) o percurso realizado a partir do mergulho na escavação dessas interfaces, iremos apresentar a seção que está “dentro” da “Central de Privacidade” do FB, chamada de Termos e Políticas do FB. Essa interface que iremos dissecar a seguir, foi capturada no ano de 2020, quando ainda preparávamos o texto da pesquisa para o seminário de tese da linha *Mídias e Processos Audiovisuais*. É relevante situarmos o(a) leitor(a) nesse recorte de tempo, pois recentemente, no ano de 2022, a empresa Facebook Inc, alterou seu nome para Meta, fazendo referência ao projeto Metaverso, que iremos detalhar em outra coleção, mas, devido à importante alteração de nomenclatura e dando maior atenção ao tema Privacidade, o FB (produto então que faz parte do portfólio da Meta), também atualizou seus Termos e Políticas de Uso<sup>9</sup>, em julho de 2022.

Figura 53 - Termos e Políticas do Facebook



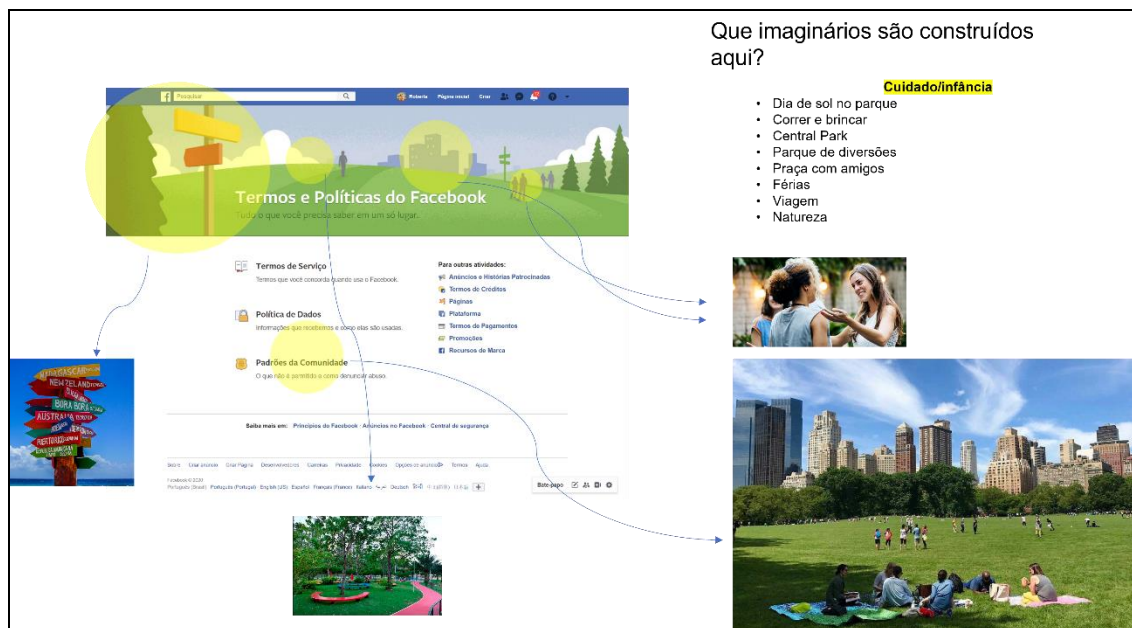
Fonte: Facebook (2020).<sup>10</sup>

<sup>8</sup> Maiores informações em <https://www.facebook.com/privacy/explanation>.

<sup>9</sup> Iremos detalhar melhor todo esse processo na coleção Políticas de Pergaminho.

<sup>10</sup> Maiores informações em [www.facebook.com/policies](http://www.facebook.com/policies).

Figura 54 - Dissecação da coleção Infância - Termos e Políticas do Facebook



Fonte: Elaborado pela autora (2021).

Ao dissecar a interface na seção Termos e Políticas, apesar de ser um espaço sem nenhuma possibilidade de publicação de conteúdo pelo usuário, curiosamente encontramos sentidos relacionados à liberdade, espaço para brincadeiras, um lindo parque em um dia ensolarado, como o imaginário associado ao Central Park em Nova Iorque, ou, até mesmo, placas indicando diversas direções para outros destinos. Mesmo sendo uma interface que não permite que o usuário publique algo para sua rede de “amigos”, a construção de uma utopia onde os Termos e Políticas do FB são um espaço livre e ensolarado como um gramado disponível para diversão de crianças, se faz presente a partir das ilustrações. Há, ainda, o texto que apoia com a pretensão “Tudo o que você precisa saber em um só lugar” reforça a restringir o interesse em buscar mais informações sobre a plataforma além desse parque ensolarado. Parece-nos que a plataforma nos sinaliza, de uma maneira sarcástica, “não avance, fique nesse parque que aqui está tudo bem”. Essa construção da *ethicidade* infância com a junção de liberdade e natureza, carrega aspectos da promessa da criação da internet nos anos 1990, conforme Chun (2006, p. 24, tradução nossa) compara com McLuhan e o conceito de *global village*, “a internet era uma aldeia global, embora mais feliz do que a de McLuhan”<sup>11</sup>.

Essa construção de um ambiente feliz e aconchegante, se estende mesmo para tratar de assuntos mais sérios, como a regulamentação da plataforma através dos “Termos e Políticas

<sup>11</sup> “the internet was a global village, albeit a happy one than McLuhan’s.”

do FB”, e o uso da ilustração, dos dias ensolarados e da utopia da tranquilidade, serve como suporte para a construção de um imaginário associado às referências da falta de seriedade, rigidez e, até mesmo, responsabilidade. Apoiados em Castoriadis (2004, p. 127), podemos dizer que “a história da humanidade é a história do imaginário humano e de suas obras”, para compreendermos a construção de sentidos a partir dessas interfaces. Em outra obra anterior, o autor contextualiza a construção do imaginário social, como algo que carrega sentidos,

consiste em ligar símbolos (significantes) a significados (representações, ordens, injunções ou incitações para fazer ou não fazer, consequências e significações, no sentido amplo do termo) e fazê-los valer como tais, ou seja, a tornar esta ligação mais ou menos forçosa para a sociedade ou o grupo considerado (CASTORIADIS, 1982, p. 150).

Portanto, compreendemos que a representação da ilustração na interface, apoiada a outras formas de imagem, como fotografias pela associação na *web*, a partir das palavras-chave utilizadas nos buscadores, formam um imaginário que carrega sentidos e densidade imagética para a interface. Entendemos que é claramente intencional a construção que o FB quer fazer de um imaginário alegre e feliz, mesmo quando o usuário busca pela rigidez das políticas da plataforma. Além disso, percebemos o uso da *imageria* já associada a sentidos tidos como “seguros” em outros espaços, como cadeados, escudos e regulamentações, sendo indicadas em desenho. Ou seja, inferimos que assim como na *timeline*, o uso do *emoji* visa reduzir a seriedade das emoções e sentimentos negativos, e aqui a ilustração do parque em grande proporção em relação às indicações associadas à “segurança” do mundo *offline*, incita o usuário a compreender que os “Termos e Políticas” dentro do FB também são divertidos e felizes como numa brincadeira de criança.

É possível percebermos essa construção de sentido nas demais interfaces capturadas da seção Segurança da Conta, que encontramos dentro dos Termos e Políticas, mais precisamente na url: <https://www.facebook.com/safety>. Essa seção chamada de Central de Segurança no Facebook, nos apresenta uma série de conteúdos em subseções, dedicados a “manter as pessoas seguras quando usam o Facebook”. Assim como a página inicial, que iremos dissecar logo a seguir, todas as páginas que fazem parte dessa Central de Segurança, são completamente tomadas pela ilustração de um lindo céu azul, com balões sobrevoando montanhas, lindos jardins, bonequinhos felizes numa linda comunidade alegre, colorida, divertida e tranquila.

Essa perfeita construção de um “mundo ideal” idealizado por uma criança, com brinquedos, amigos, animais e carrinhos coloridos, reforça nossa compreensão de que os

imaginários que emergem dessas interfaces reforçam o mundo idealizado da infância e retira a seriedade e gravidade das informações lá contidas. Alguns dos imaginários encontrados foram parque de diversões, brinquedos, amigos, tons serenos de cores que praticamente mascaram a relevância do conteúdo que está sendo apresentado. Verificamos que na Central de Segurança, no FB, o medo e a angústia não fazem parte nem das subseções como “Prevenção contra o *bullying*”, “Segurança das mulheres”, “Vítimas de abuso”, “Prevenção contra o suicídio” ou “Imagens íntimas não consensuais”, ou seja, há claramente muitos conteúdos de lógica suspeita e comportamento criminoso acontecendo dentro do FB, mas a maneira como a plataforma apresenta as temáticas carrega *ethicidade* infantil em toda sua extensão. O imaginário construído é propositalmente imaturo para lidar com temas tão graves e sérios, o que inferimos ser reflexo do mesmo comportamento de Mark Zuckerberg quando interrogado no Senado americano em 2018, demonstrando despreparo e descaso nas respostas dadas sobre a acusação.

Compreendemos que essa postura da plataforma em lidar com diversão e destreza aos aspectos tão graves e criminosos, a partir dos emolduramentos criados por uma *ethicidade* alicerçada na infância nesses ambientes, refletem negativamente na sociedade, aparentemente menosprezando a seriedade desses crimes. Vejamos na reflexão de Castoriadis (2004, p. 130) a relevância desses sentidos perpetuados na sociedade:

Uma vez criadas, tanto as significações imaginárias sociais quanto as instituições se cristalizam ou se solidificam, e é isso que chamo de imaginário social instituído, o qual assegura a continuidade da sociedade, a reprodução e a repetição das mesmas formas que a partir daí regulam a vida dos homens e que permanecem o tempo necessário para que uma mudança histórica lenta ou uma nova criação maciça venha transformá-las ou substituí-las radicalmente por outras.

A *ethicidade* que reconvoca infância pela Central de Segurança no FB não utiliza recursos da *imageria* da segurança tradicional, como chaves ou fechaduras, mas cria pelo acolhimento, aconchego e sensação de conforto aspectos associados à segurança do usuário nesse ambiente. Como pode ser visualizado, na captura a seguir, a segurança também está sendo representada por outros indicativos que fogem de aspectos associados ao medo e preocupação, mas ao imaginário de socorro, como a própria boia salva-vidas, que é fornecida pela plataforma para “retirar o usuário do perigo do afogamento”, ou a lanterna oferecida que ilumina o que está na escuridão do usuário:

Figura 55 - Dissecação da *ethicidade* infância - Central de Segurança no Facebook



Fonte: Facebook (2021).<sup>12</sup>

Na dissecação realizada, é possível verificarmos imaginários contidos na interface a partir de uma série de sentidos relacionados ao cuidado, infância, carinho, acolhimento e salvamento. Claramente, a ilustração torna o conteúdo intencionalmente mais “leve”, já que os aspectos da Central de Segurança evidenciam a ocorrência de possíveis atos criminosos dentro do FB, e o texto de apoio, na página inicial, demonstra a construção da ingenuidade infantil da plataforma em encarar esses temas:

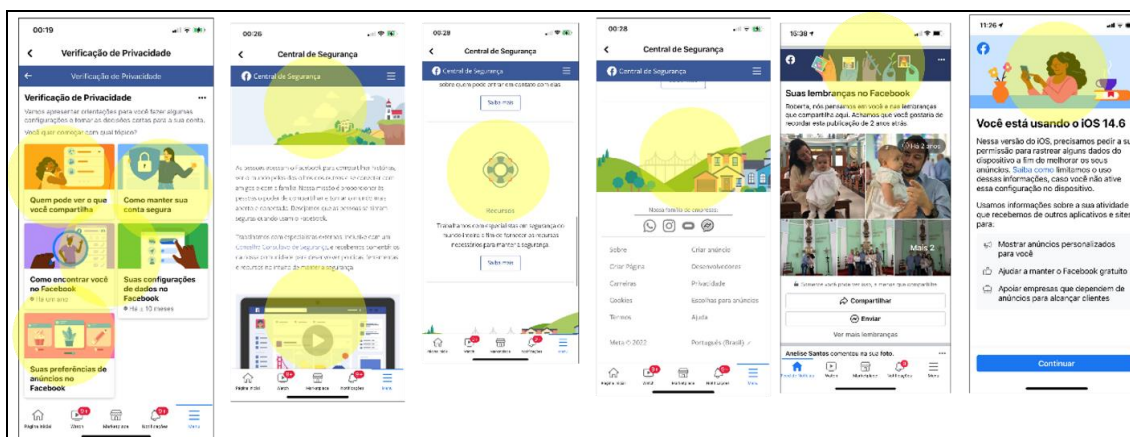
As pessoas acessam o Facebook para compartilhar histórias, ver o mundo pelos olhos dos outros e se conectar com amigos e com a família. Nossa missão é proporcionar às pessoas o poder de compartilhar e tornar o mundo mais aberto e conectado. Desejamos que as pessoas se sintam seguras quando usam o Facebook. Trabalhamos com especialistas externos, inclusive com um Conselho Consultivo de Segurança, e recebemos comentários da nossa comunidade para desenvolver políticas, ferramentas e recursos no intuito de manter a segurança (FACEBOOK, 2021).

Esse imaginário associado à infância, com sentidos que constroem a *ethicidade* por meio do desenho, da ilustração, da ingenuidade e da isenção do FB, em relação aos “perigos” e ameaças que ocorrem dentro da plataforma, também é replicado nas versões do aplicativo FB para dispositivos móveis, conforme o arranjo, a seguir, demonstra a partir dos emolduramentos agenciados com a adaptação da interface gráfica à medida reduzida da tela do *smartphone*:

<sup>12</sup> Maiores informações em <https://www.facebook.com/safety>.



Figura 56 - Indicação da coleção Infância na reprodução da interface gráfica, versão aplicativo do FB



Fonte: Elaborado pela autora (2021).

Finalizamos a compreensão da coleção Infância pelas interfaces do FB. Para dar seguimento ao processo de cartografar os sentidos de segurança pela ambiência, iremos apresentar a coleção intitulada por Guardiã de Memórias, um conjunto de capturas de telas que possuem um significado associado a lembranças, recordações e cuidado que presentificam o sentidos de o FB ser um grande protetor a partir da vigia.

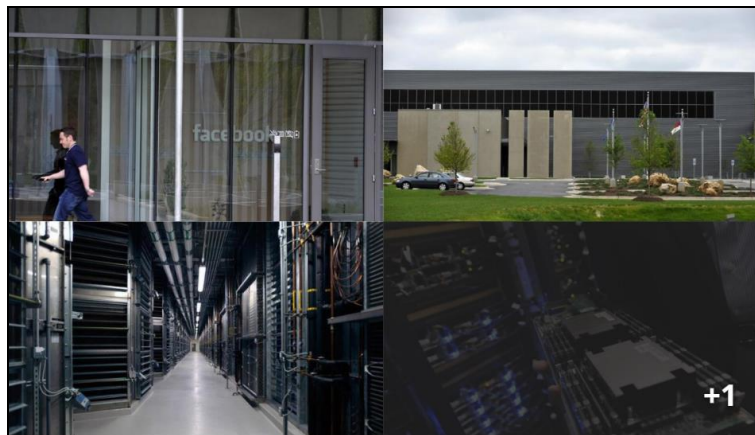
#### 4.2.2 Coleção Guardiã de Memórias

Ao continuarmos a dissecação de nossas materialidades, encontramos outros territórios de identificação que dão a ver imaginários convocados nas interfaces comunicando sentidos, pois não é somente a partir de uma construção baseada no alicerce infantil que os usuários – todos com idade acima de 13 anos, conforme políticas de uso da plataforma, aceitam as condições do FB e, também, dedicam muitas horas do dia em acessar a plataforma. Percebemos que a construção do imaginário de comunidade e zelo, fortemente enunciado no FB, como explicitamente em suas práticas de segurança, mas também na própria *newsfeed* e *timeline*, tensionam um papel de Guardiã que protege e acolhe o usuário.

Paralelamente, já que cuidar também remete ao controle e segurança, começamos a investigar como o FB diz que seu ambiente é um lugar seguro, e como ele diz que nossos dados estão seguros ali dentro (em nenhum momento no nosso flunar pela plataforma encontramos informações, de fato, onde o FB guarda nossas fotos, vídeos e todos dados coletados – que, na verdade, estão em *datacenters* localizados nos EUA, bem longe desse mundo colorido e fofo que a interface faz questão de construir e demonstrar, mas num

território enorme contendo *hardwares*, cabos e *softwares* fechados em um ambiente totalmente climatizado artificialmente) (OLHAR DIGITAL, 2018).

Figura 57 - Fotografia do *datacenter* do FB na Carolina do Norte



Fonte: CanalTech (2012).

Mas, encontramos diversas associações com o conceito de comunidade, amizade e estar em grupo que são reconvocados a partir das imagens. O constante estímulo e lembrança da roda de amigos, de celebrarmos, darmos um abraço (tão raros em tempos de pandemia que estamos vivendo) que acabam por despertar o senso de pertencimento, de coletividade, sociabilidade e interação social. Ao mesmo tempo, conforme relata Bauman (2003), há ambivalência ao se querer viver em comunidade, já que para haver o bem-estar e a tão desejada segurança, devemos renunciar à liberdade. A comunidade imaginária do autor, que produz a sensação de aconchego e carinho é utópica, pois, para aceitarmos viver em comunidade é concordarmos com limites, regras e uma constante vigilância, já que aquele membro que não respeita as condições de permanência, é excluído por expor os demais à falta de proteção, portanto, a insegurança. Conforme Bauman (2003, p. 111), esse movimento “natural” de exclusão dá origem ao gueto, maneira de se viver às margens da sociedade comum idealizada:

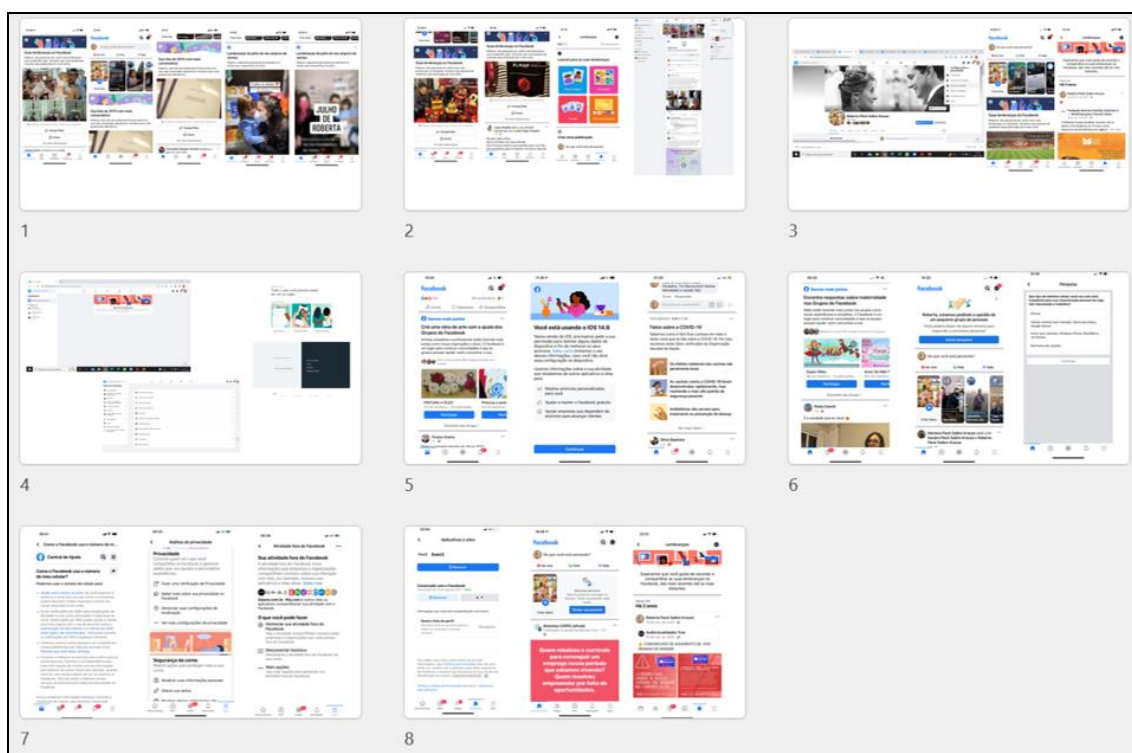
[...] gueto quer dizer impossibilidade de comunidade. Essa característica do gueto torna a política de exclusão incorporada na segregação espacial e na imobilização uma escolha duplamente segura e a prova de riscos numa sociedade que não pode mais manter todos os seus membros participando do jogo, mas deseja manter todos os que podem jogar ocupados e felizes, e acima de tudo obedientes.

Outro sentido identitário, que encontramos nas interfaces, está associado à prática da memorização, de lembranças, recordações e culto ao que já foi postado em outro momento na linha do tempo do usuário ou quando ele foi *tagueado* por outro usuário. A postura que o FB

assume ao propor que o usuário retorne suas lembranças “passadas” em “novas” postagens na *timeline*, sugere um grande protetor de acontecimentos, pois é o próprio *software* que faz o papel de recordar ao usuário o que ele estava fazendo há 1 ano ou mais, ou de sinalizar quais dos “amigos” do FB estão fazendo aniversário na semana. Inferimos essa espécie de controle como uma das formas de vigiar os “passos” dos usuários ao longo da sua interação com a plataforma, mas apresentado a ele como um grande aliado nessa memorização.

Para dar a ver esses sentidos, nossa coleção contém a captura de interfaces de diversas seções dentro do FB, como *timeline*, Configurações da Conta, *newsfeed* e Central de Ajuda, conforme o arranjo, a seguir, demonstra:

Figura 58 - Arranjo de interfaces da coleção Guardiã de Memórias



Fonte: Elaborado pela autora (2021).

A maneira que agrupamos as capturas na coleção está seguindo uma espécie de organização para exemplificar a dissecação a seguir. Se o(a) leitor(a) desejar explorar melhor cada captura, assim como na coleção anterior, sugerimos direcionar a câmera do celular para o QRCode a seguir:

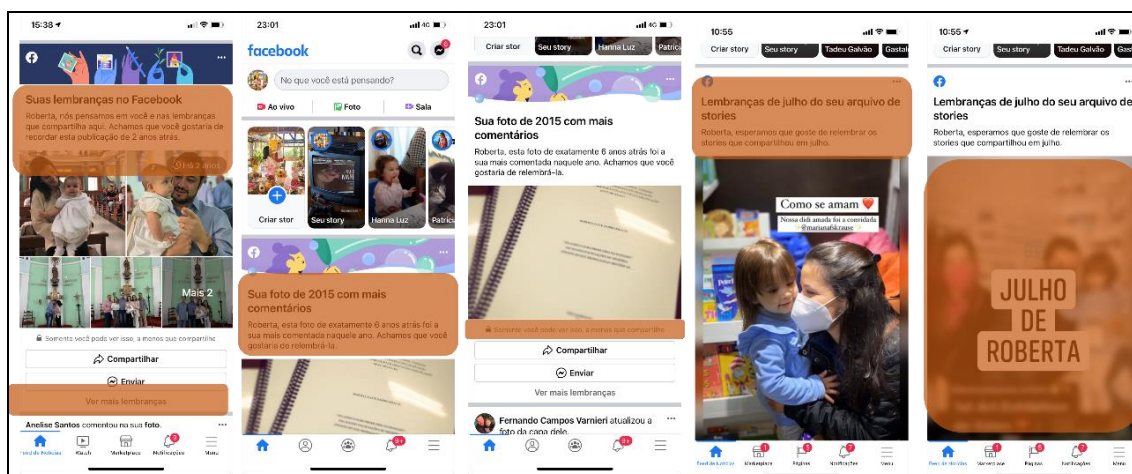
Figura 59 - Código QR para acessar imagens das interfaces que compõem a coleção Guardião de Memórias



Fonte: Elaborado pela autora (2021).

A operação da dissecação das interfaces, a seguir, está sendo indicada pela cor marrom, onde intervimos na imagem para esmiuçarmos determinados aspectos que enunciam os sentidos de guardião, associado ao imaginário daquele que guarda e protege sua comunidade, conforme explicaremos:

Figura 60 - Dissecação da *ethicidade* - Guardião de Memórias



Fonte: Elaborado pela autora (2021).

Encontramos, nas indicações sinalizadas no arranjo de capturas de interface do aplicativo FB, algumas enunciações que circunscritas ao ambiente, que dão a ver sentidos de um grande amigo, de alguém para quem o usuário confia suas lembranças e recordações. Quando o FB diz “Roberta, nós pensamos em você e nas lembranças que compartilha aqui”, entendemos que a plataforma assume um lugar de fala de cuidado, que pensa no melhor para seus usuários, que analisa criteriosamente o que nós gostaríamos e *como* gostaríamos de ser tratados. “Achamos que você gostaria de recordar esta publicação de 2 anos atrás” realiza e expõe, pelas imagens, uma sugestão de álbum de fotografias com memórias que, pelo viés da plataforma, recebem o *status* de um momento feliz que mereceria ser rememorado numa roda de amigos íntimos. A plataforma, ainda, realiza o convite para “ver mais lembranças”, dando

a oportunidade para “reviver” outras postagens “anteriores”. Há uma espécie de *ranking* das lembranças mais “curtidas” ou comentadas, ou seja, aquelas que tiveram maior aceitação junto às conexões da plataforma. Provavelmente, o controle das publicações de “maior sucesso” ou engajamento como comentários e *likes*, são aquelas dignas do FB sugerir como nova oportunidade para serem recordadas, e gerar novamente engajamento, envolvimento, tempo de permanência na página e demais métricas para monetização de anúncios.

Encontramos um outro sentido nessas mensagens “de memórias”, em textos como “Somente você pode ver isso a menos que compartilhe”, criando um segredo, algo oculto que acontece exclusivamente no “privado” entre a intimidade do FB e do usuário, como uma conversa particular entre amigos. O FB então está “nos bastidores”, cuidando e vigiando o que, de fato, pode se tornar “público” ou acessível aos demais usuários, criando a conexão “nós *versus* eles”. É como se a plataforma fosse um grande guardião, que oferece o segredo ao usuário e estimula que vaze aos demais participantes da roda. Wendy Chun (2016, p. 103, tradução nossa) comenta sobre a característica das redes e como cria a relação de sentir-se seguro:

Essa segurança, baseada na transformação de usuários em ‘amigos’ recíprocos e reciprocidade, era e não é segurança, pois amigos online são uma tecnologia extremamente vazada. Amizade online – um conceito que turva a nítida fronteira entre o público e o privado, trabalho e lazer – encapsula a promessa e a ameaça das redes: a promessa de uma intimidade que, por mais banal que seja, transcende a localização física e permite que laços feitos por si mesmos aliviem a solidão do neoliberalismo; a ameaça de uma segurança baseada em “comunidades” mal protegidas.<sup>13</sup>

Quando a autora diz que a tecnologia é “vazada” significa que uma das lógicas de sustentação dessa rede “de relacionamentos”, a internet, que surgiu na década de 1990, contrasta com a ideologia de liberdade e certo empoderamento que acompanhavam o “nascimento” da internet comercial, com a atualidade da rede que lida com a busca por autenticidade constante.

O frequente estímulo ao tipo de relacionamento superficial, que quantifica o sucesso, controla e vigia o outro não configura em amizade “real”, que se dá entre humanos, mas, perpetua socialmente o perigo de um modelo simulado entre *software* e usuário. Chun (2016,

---

<sup>13</sup> “This safety, based on the transformation of users into reciprocal and reciprocating ‘friends,’ was and is no safety, for online friends are an extremely leaky technology. Online friendship – a concept that muddies the neat boundary between public and private, work and leisure – encapsulates the promise and threat of networks: the promise of an intimacy that, however banal, transcends physical location and enables self-made bonds to ease the loneliness of neoliberalism; the threat of a security based on poorly gated ‘neighborhoods.’”

p. 104, tradução nossa) complementa chamando por uma amizade autenticadora que “[...] perverte conceitos tradicionais de amizade transformando-a de uma ação essencialmente difundida (e privada) – a uma ação não recíproca para amar/gostar de alguém – para um comportamento banal, recíproco de ‘relação-curtida’”<sup>14</sup>.

Nas dissecação das interfaces, a seguir, é possível perceber esse guardião estimulando a amizade autenticadora de Chun (2016), acrescido da característica de um controlador, onde armazena, classifica, organiza e oferece ao usuário o que julgar mais relevante. Ao informarmos na seção específica que escavamos clicando em “ver mais lembranças”, fomos direcionados a uma espécie de hipocampo cerebral, onde residem as memórias conscientes do usuário, ou seja, um banco ou acervo de conteúdos que o *software* elege como “memoráveis” e que poderiam ser visíveis. Nessa seção do FB não encontramos lembranças, mas a mensagem “Hoje não há lembranças. Hoje não há lembranças para ver ou compartilhar, mas avisaremos quando houver algo para recordar”, ou seja, além de assumir a potência de elencar o que vale a pena ser lembrado, o FB declara que o usuário será notificado por ele quando houver algo relevante a ser postado. Para a plataforma, não houve nada de interessante que valesse a pena de ser rememorado na *timeline*. Mas e se nós, como usuários do FB, quiséssemos acessar memórias, interações ou conteúdos realizados no “mesmo dia” há 1 ou 5 anos? Pelo critério do que deve ser guardado pelo FB, não fizemos nada de interessante, e consequentemente, não é elegível para ser lembrado?

Além disso, ao escavarmos a seção “Lembranças”, chegamos na página intitulada como Registro de Atividades, onde a interface oferecida é pouco estimulante ao usuário, com um relatório de nossa movimentação pelo FB. Porém, é interessante verificar que o lugar de fala da plataforma vai mudando conforme a *ethicidade* circunstanciada pela interface. Conforme vimos anteriormente, o cuidado e atenção eram característicos do FB ao “conversar” diretamente com o usuário, se posicionando como um amigo. Agora, nesse ambiente pouco estimulante para publicação, onde não há presença de amigos ou álbum de fotografia, a interface coloca o usuário como responsável pela navegação, numa espécie de abandono. Por exemplo, “vídeos que *você* curtiu”, “vídeos que *você* procurou”, ou seja, o usuário parece estar sozinho agora, aquele companheiro cuidadoso que se pronunciava “Nós pensamos em você”, agora não se faz mais presente. Chun (2016, p. 104, tradução nossa)

---

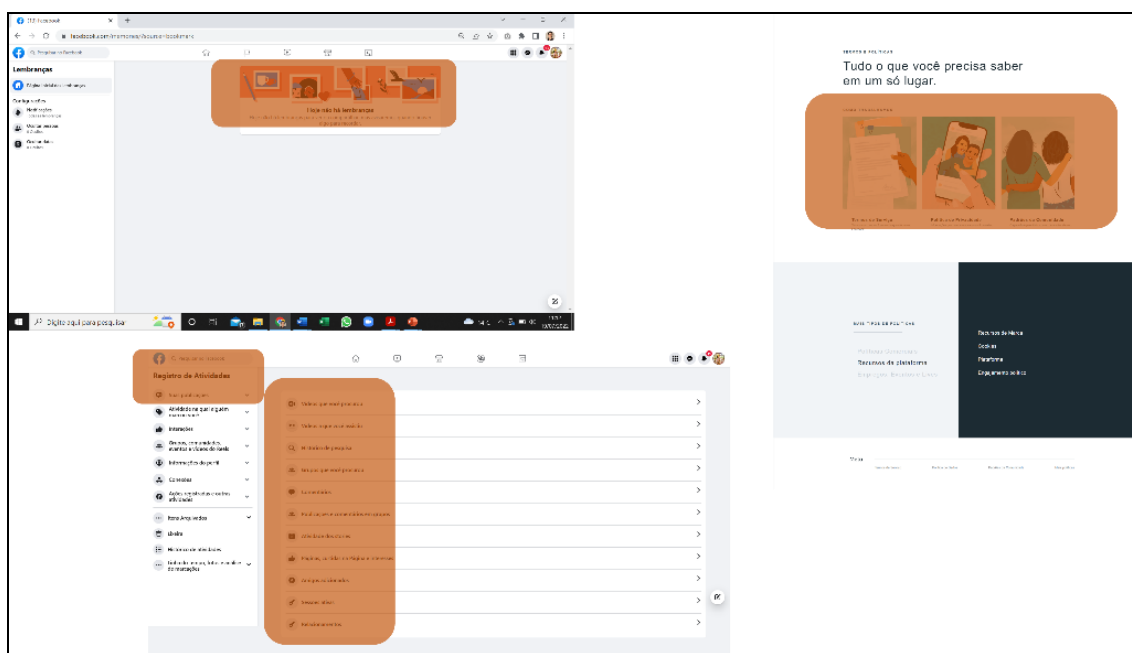
<sup>14</sup> “This authenticating friendship, this chapter also emphasizes, perverts traditional concepts of friendship by transforming it from an essentially broadcast (and private) action – an unreciprocated act to love/like someone – to a banal, reciprocal, and ‘authentic like’ relation.”



contextualiza essa característica, dizendo que se trata de algo manipulado, vigiado que foi calculado para agir dessa maneira,

Através dessa amizade empobrecida, as relações são mapeadas e extrapoladas: ações habituais – curtir, retweetar, postar etc. – usadas para criar perfis para rastrear cuidadosamente, antecipar e criar o consumo. Que diz respeito menos de suas próprias ações individuais, VOCÊ é constantemente traído por pessoas que ‘gostam de VOCÊ’ e que são determinados algorítmicamente para serem ‘como VOCÊS’.<sup>15</sup>

Figura 61 - Dissecação da coleção Guardiã de Memórias



Fonte: Elaborado pela autora (2021).

Na dissecação do arranjo das interfaces anteriores, encontramos sentidos alicerçados em amizade, carinho e cuidado. Já no arranjo dissecado na Figura 61, esse zelo é substituído pelo abandono e registro de quantificações em um histórico frio e distante. Mas, percebemos que o imaginário do carinho retorna às interfaces quando dissecamos o arranjo, a seguir, que contém capturas de interfaces da *newsfeed*. Ou seja, a *ethicidade* do guardião que protege se enuncia claramente a partir de emolduramentos e uso da linguagem “Somos mais juntos”, reconvocando o usuário para dialogar com o FB novamente.

<sup>15</sup> “Through this impoverished friendship, relations are mapped and extrapolated: habitual actions – liking, retweeting, posting, etc. – used to create profiles to carefully track, preempt and craft consumption. Regardless of your own individual actions, YOU are constantly betrayed by people who ‘like YOU’ and who are algorithmically determined to be ‘like YOU’.”

Figura 62 - Dissecção da coleção Guardiã de Memórias - *newsfeed*



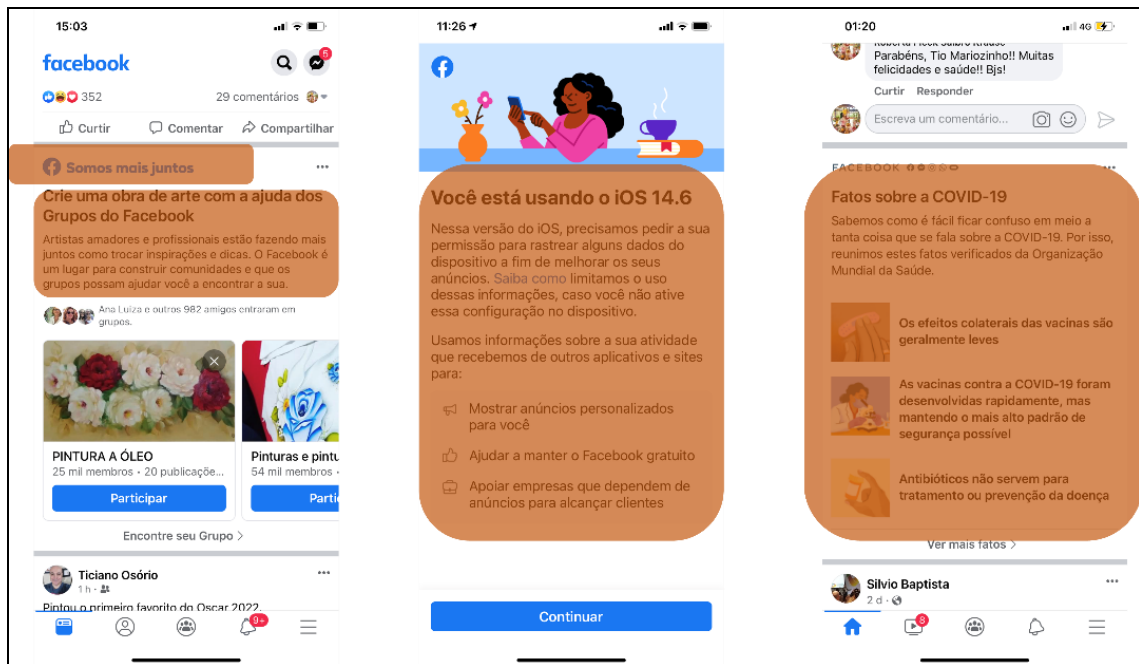
Fonte: Elaborado pela autora (2021).

Compreendemos que os sentidos que se enunciam na interface constroem um imaginário de comunidade, socialização, amizade e pertencimento. Além disso, na dissecção do arranjo a seguir, é possível identificarmos esses sentidos a partir de conteúdos ofertados como “Nessa versão do iOS, precisamos pedir a sua permissão para rastrear alguns dados do dispositivo, a fim de melhorar os seus anúncios”; novamente o lugar de fala retoma um posicionamento que, apesar de estar monitorando o usuário do FB, faz vigia mas “pede permissão” para ter acesso aos dados, é cortês, como um cavalheiro, sob a justificativa de melhorar a “experiência” na oferta de anúncios, que na verdade só é positiva pelo viés da monetização publicitária, tanto para a plataforma quanto para o anunciante que pagou pelo conteúdo patrocinado.

O guardião que protege e cuida, reaparece ao ofertar conteúdos associados ao bem-estar da saúde do usuário, sugerindo informações sobre a prevenção da Covid-19: “Sabemos como é fácil ficar confuso em meio a tanta coisa que se fala sobre a COVID-19. Por isso, reunimos estes fatos verificados da Organização Mundial da Saúde”. Nesse sentido, as interfaces que coletamos demonstram a troca de guardião protetor para um guarda que monitora os passos dos seus vigiados, abandonando-os sozinhos.



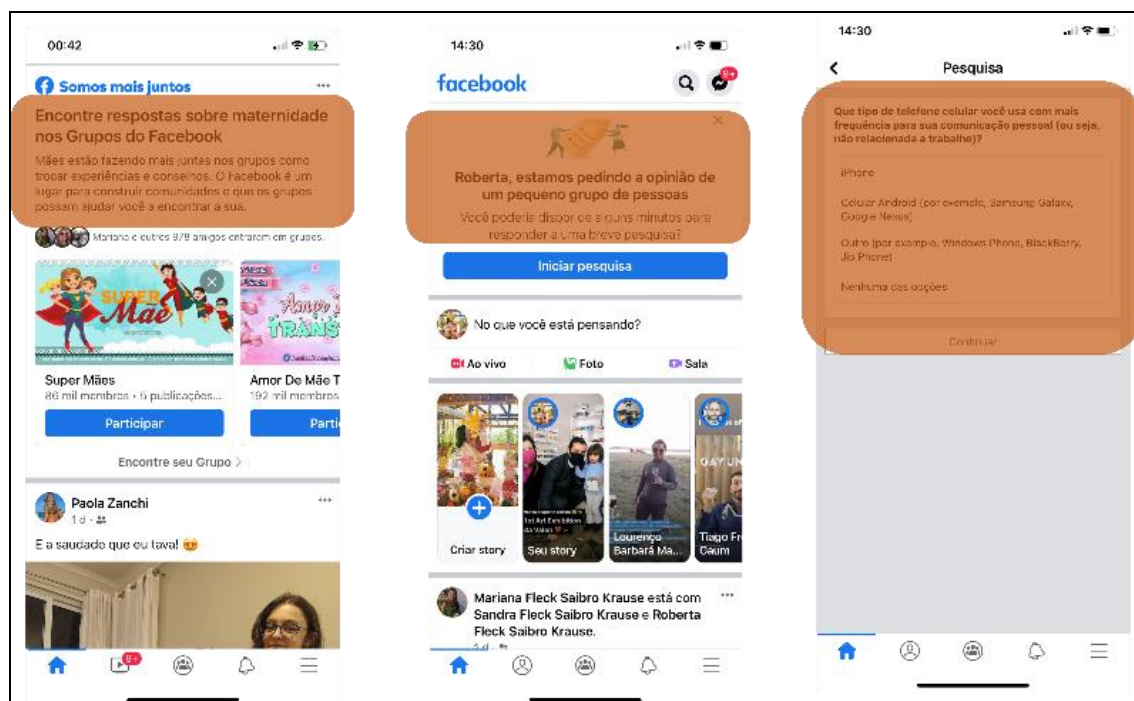
Figura 63 - Dissecção da coleção Guardiã de Memórias



Fonte: Elaborado pela autora (2021).

Para finalizar a coleção Guardiã de Memórias, apresentamos o arranjo, a seguir, que carrega sentidos extremamente alicerçados em cuidado. Na verdade, podemos inferir como o maior deles, o cuidado materno. A plataforma compreende, pelo histórico de publicações, interesses demonstrados e interações realizadas por nosso perfil, que conteúdos relacionados a maternidade estão alinhados a nosso usuário. Portanto, ao sugerir “Encontre respostas sobre maternidade nos grupos do Facebook”, está produzindo sentidos muito carregados de prudência e capricho, agenciando construções muito fortes no imaginário da família e da maternidade.

Figura 64 - Dissecção da coleção Guardiã de Memórias



Fonte: Elaborado pela autora (2021).

O zelo permanece na postura do conteúdo ao questionar “Roberta, estamos pedindo a opinião de um pequeno grupo de pessoas. Você poderia dispor de alguns minutos para responder a uma breve pergunta?”, correspondendo à valorização do usuário como um ente querido e muito próximo, já que apenas um seletivo grupo (dos bilhões de usuários ativos), fomos selecionados como relevantes (!). Apoiamos novamente na visão de Chun (2016, p. 12, tradução nossa) sobre haver uma grande mistura e confusão nas mídias sociais sobre a construção dos limites entre o que é público e o que seria privado. Conforme a autora, as nossas referências para “a própria noção de ‘amigo’, inicialmente vista como uma maneira de restringir as comunicações em *sites* de mídia social como Friendster.com, levou a várias “crises” que decorrem de brechas nas fronteiras entre privado e público, amigo/chefe/mãe”<sup>16</sup>.

Compreendemos que a constelação **Confiança Programada** reúne imaginários sociais, que, conforme Castoriadis (1985, p. 103), representa a significação das coisas

A instituição imaginária da sociedade é instituição das significações imaginárias sociais que deve, por princípio, conferir sentido a tudo que pode se apresentar, ‘dentro’ da sociedade como ‘fora’ dela. A significação imaginária social faz ser as coisas como tais coisas, coloca-as como sendo aquilo que são – o aquilo que sendo posto pela significação, que é indissociavelmente princípio de existência, princípio de valor, princípio de ação.

<sup>16</sup> “The very notion of a ‘friend’, initially viewed as a way to restrict communications in social media sites such as Friendster.com, has led to various ‘crises’ that stem from breaches in the boundaries between private and public, friend/boss/mother.”

Inferimos que os imaginários construídos, a partir da comunicação dos sentidos agenciados pelas interfaces dissecadas, produzem molduras e moldurações de **Confiança Programada**, carregam, então, as *ethicidades de guardião* como o responsável ora por defender, cuidar e proteger, ora por vigiar, abandonar e controlar. Assim como a *ethicidade infantil* produz um eixo do imaginário permitindo enunciar sentidos que estão alicerçados em um universo colorido, ingênuo, livre de responsabilidade, onde impera a diversão e a liberdade.

Para dar continuidade ao exercício de análise, a seguir, apresentaremos a segunda constelação, **Usuário Vulnerável**, composta por coleções de interfaces que autenticam em nossa pesquisa algumas *ethicidades*, a partir das coleções Sujeito inseguro e Lógica Suspeita, *Tecnoinsegurança*, e Políticas de Pergaminho.

### 4.3 Segunda constelação - Usuário Vulnerável

Para dar início à apresentação da segunda constelação que compõe a galáxia da *tecnosegurança* pela ambiência FB, iremos demonstrar as três coleções que fazem parte dessa construção de sentidos a partir do agrupamento das imagens da interface. Porém, é importante situarmos o leitor na construção do nome da constelação. Nos fundamentamos da reflexão realizada por Chun (2006), para nomear como Usuário Vulnerável, porque percebemos que a promessa da criação da internet comercial nos anos 1990 como um ciberespaço livre para seus “astronautas” sobrevoarem, caiu por terra principalmente por causa da possível ameaça a esse ambiente “livre”. Isso se deu, basicamente, pela falta de proteção dos dados de cidadãos americanos, e pela suposta invasão de segurança em informações tidas como sigilosas para o governo dos EUA que podem ter auxiliado o planejamento dos atos terroristas de 11 de setembro de 2001. Em razão dos atos, o governo, à época, optou por retirar informações públicas de seus *sites* institucionais, encorajando a criar, no senado, as 12 novas medidas de vigilância eletrônica, dando origem ao *Eletronic Pearl Harbor* (CHUN, 2006).

Essas assim chamadas reavaliações críticas da Internet, que se reduzem a “pessoas ruins fazem coisas ruins com tecnologia” e “pessoas boas fazem coisas boas”, ofuscam **acidentes e vulnerabilidades**, aquele que usa a tecnologia - ou mais apropriadamente, suas intenções - determina o resultado<sup>17</sup> (CHUN, 2006, p. 257, grifo da autora, tradução nossa).

---

<sup>17</sup> “These so-called critical reassessments of the Internet, which reduce to ‘bad people do bad things with technology’ and ‘good people do good things’, obfuscate accidents and vulnerability, the one using the technology - or more properly, one’s intentions - determines the result.”

Sua ênfase em quem, portanto, no usuário da internet que estamos compreendendo, acaba por provocar a construção paranoica da ameaça associada à tecnologia e, principalmente, quem faz o uso dela. Conforme diz Chun (2006, p. 257, tradução nossa), essa construção do medo social se apoia na falta de lucidez dos sujeitos, já que “a paranoia não pode ser dissipada pela explicação racional, porque a paranoia tem tudo a ver com explicação racional e significado: para o sujeito paranoico, sempre há significado”<sup>18</sup>. Ainda, embasados na defesa da autora, consideramos que essa paranoia constrói sentidos, e se reproduz a partir das molduras, autenticadas pelas *ethicidades* que são dadas por sentidos identitários que iremos indicar na dissecação das interfaces.

Para isso, na primeira coleção denominada por **Sujeito Inseguro e Lógica Suspeita**, autenticamos algumas *ethicidades* que se atualizam em molduras e moldurações de significação associadas à imaginários que comunicam sentidos de vigilância como um modo de ser na contemporaneidade, aliado a cultura do medo constante, de agir em anonimato e da confiança pela construção da comunicação somente pelo íntimo e pelo segredo.

Já a segunda coleção, nomeada como **Tecnoinsegurança**, demonstra como o suposto “zelar” pela proteção no FB acontece alicerçado em práticas de molduras e moldurações que produzem sentidos comunicados por uma *imageria* da comunicação “segura”, a partir do uso de cadeados, chaves, escudos e conteúdos explicitamente dedicados a contar como aquele espaço se caracteriza por uma comunidade.

E a terceira coleção, **Políticas de Pergaminho**, indica, a partir da dissecação, os imaginários de defesa associados a uma judicialização, questões legais e termos de consentimento que alertam o usuário para os “perigos” da plataforma, mas, metaforicamente, são utilizados como a mais explícita maneira de defesa do próprio FB contra acusações e vazamento de dados coletados.

#### 4.3.1 Coleção Sujeito Inseguro e Lógica Suspeita

Nossa coleção conta com capturas de diversas seções dentro do FB, *timeline*, *newsfeed*, Configurações da Conta, Central de Privacidade e Segurança, assim como formatos para *web (desktop)* e aplicativo.

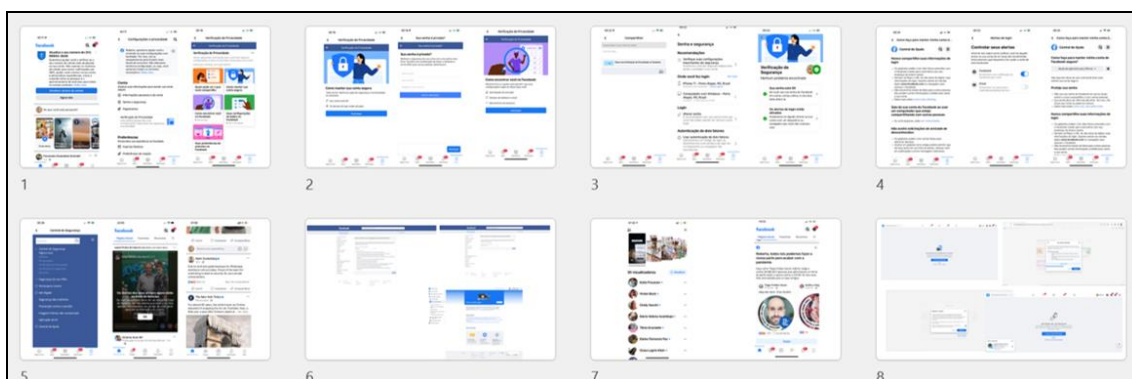
A forma que as interfaces estão agrupadas na coleção está seguindo um tensionamento de itens (opostos ou complementares) que encontramos a partir da realização da intervenção

---

<sup>18</sup> “Paranoia cannot be dispelled by rational explanation because paranoia is all about rational explanation and meaning: for the paranoid subject, there is always meaning.”

nas imagens, ou seja, durante a dissecação. A seguir, também estamos dispondo do código QR para visualizarmos as interfaces no *smartphone*, assumindo aqui a própria *ethicidade* que estamos autenticando na pesquisa, com o uso de códigos e cifras para acessarmos um documento dessa tese, algo em “segredo” entre você leitor(a), nós (pesquisadora, orientadores e referencial teórico), e o próprio serviço de armazenamento de dados, Google Drive, nada privado, na *tecnocultura* contemporânea.

Figura 65 - Coleção Sujeito Inseguro e Lógica Suspeita



Fonte: Elaborado pela autora (2021).

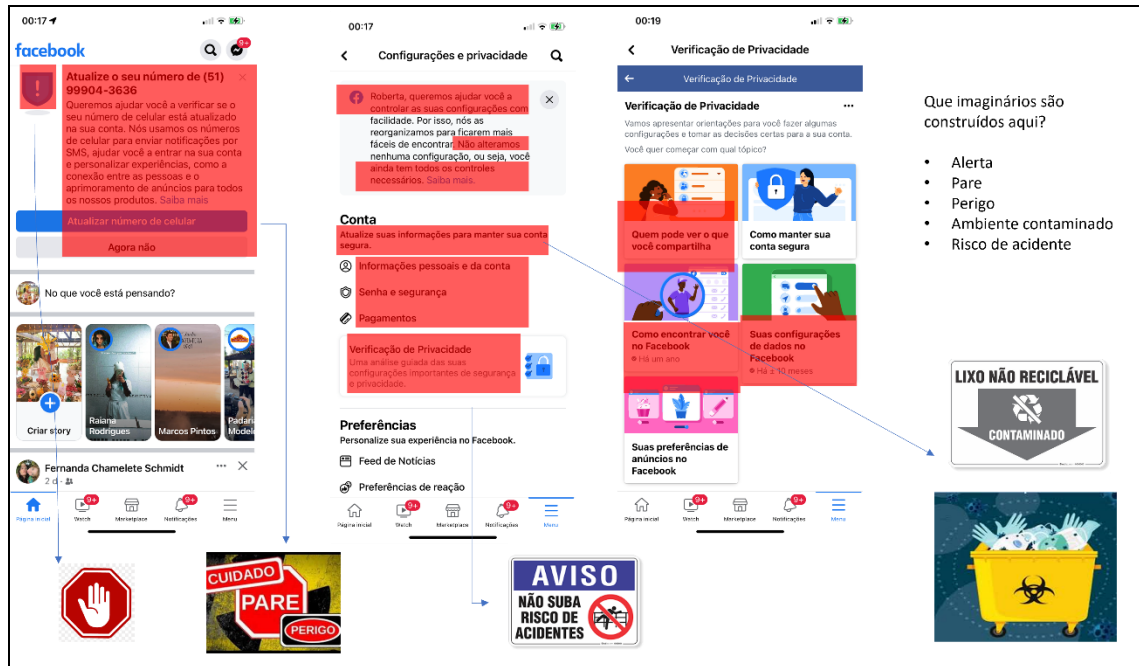
Figura 66 - Código QR para acessar a coleção Usuário Inseguro e Lógica Suspeita



Fonte: Elaborado pela autora (2021).

O primeiro arranjo de interfaces, que realizamos a dissecação, apresenta uma forte preocupação com o usuário, demonstrando intimidade em alguns momentos, contando segredos e promovendo confiança para aquele usuário que, claramente para o FB, se sente suscetível naquele espaço. Entendemos que pela vulnerabilidade construída naquele ambiente, o usuário encara o FB como “alguém” em quem confiar, conforme dissecação, a seguir, indica na cor vermelha esses sentidos de paranoia e contaminação:

Figura 67 - Dissecção da coleção Sujeito Inseguro e Lógica Suspeita



Fonte: Elaborado pela autora (2021).

A primeira captura da interface, no arranjo, demonstra um alerta do FB para o nosso usuário logo ao acessar a *timeline*. Uma mensagem que toma conta de grande parte da tela sinalizando que o FB admite haver um possível perigo acontecendo “lá dentro”:

Atualize o seu número de (51) 99904-3636. Queremos ajudar você a verificar se o seu número de celular está atualizado na sua conta. Nós usamos os números de celular para enviar notificações por SMS, ajudar você a entrar na sua conta e personalizar experiências, como a conexão entre as pessoas e o aprimoramento de anúncios para todos os nossos produtos. Saiba Mais (FACEBOOK, 2021).

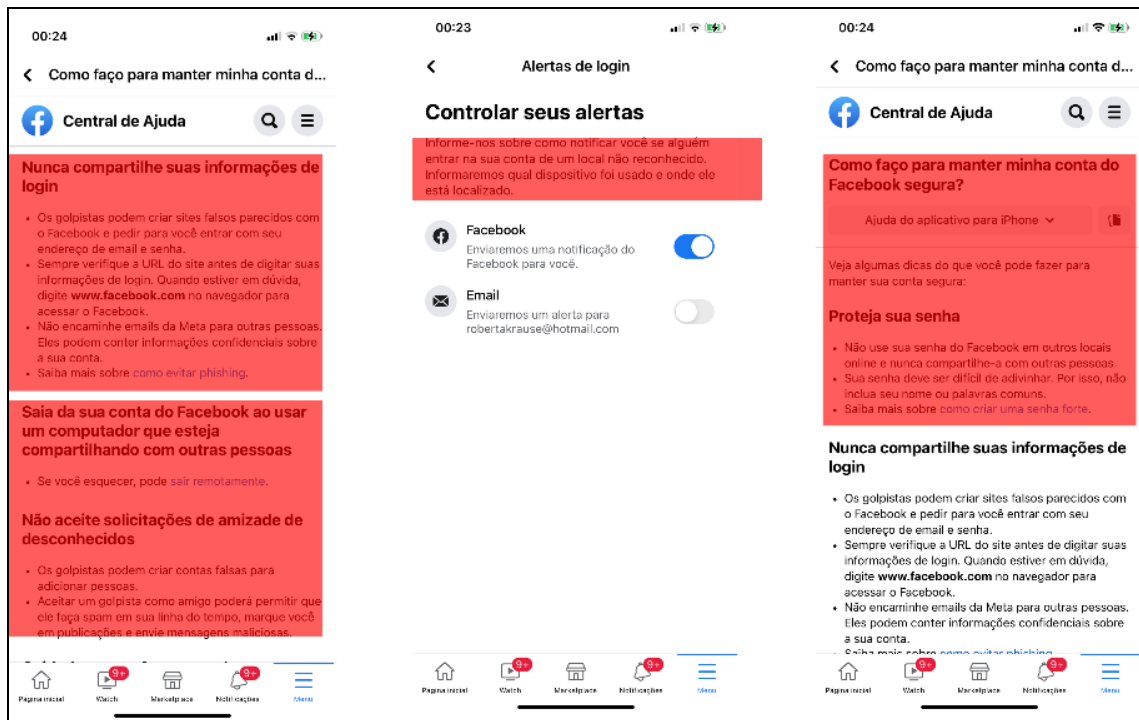
É possível perceber que esse alerta da plataforma carrega sentido de perigo e infiltração por parte de terceiros, sendo o FB o responsável por fazer a segurança do usuário, desde que este ceda informações sinalizadas para “personalizar experiências”, inclusive “aprimorar anúncios para todos os nossos produtos”. Essas características representam o que Lemos (2009) chama por construção de um sujeito inseguro, atitudes que alimentam a cultura da insegurança nas pessoas. Uma dessas iniciativas é justamente o constante alerta para segurança, ou seja, quanto mais se garante que aquele ambiente é seguro, mais se reforça o tema na cultura em geral. Lemos (2009) resgata a fala de Rosello (2008), ao refletir sobre o discurso da segurança que cria concomitantemente a cultura da *insegurança*. Entendemos que assim como o medo alimenta a cultura da insegurança, a paranoia de Chun (2006) é resultado da fobia social.

Pela etapa metodológica da dissecação e a indicação dos imaginários (e das imagens associadas às palavras-chave), é possível inferirmos que todos esses avisos e sinalizações, que buscam proteger a conta do usuário, na verdade, corroboram com o sentido do pavor. Em outra sinalização da interface há a mensagem: “Atualize suas informações para manter sua conta segura”, há uma clara indicação do FB em orientar o usuário para manter seus dados atualizados, ou seja, revistados. Esse aspecto remete à vigia constante, um controle das informações que estão sendo fornecidas à plataforma, sob pena do perigo de um terceiro ter acesso. Portanto, se o FB sinalizou uma “lógica suspeita”, quem seria a ameaça? Identificamos, na construção da *ethicidade* sujeito inseguro, que o FB se posiciona sempre como quem ajuda, quem auxilia e protege (conforme vimos na constelação Confiança Programada), e parece-nos que o medo é construído, então, em relação a um inimigo que ainda não apareceu, ou seja, o FB “luta” uma batalha para defender seus usuários de quem? De um suposto inimigo invisível? Um sujeito – conforme delimita Chun (2006) – que pode conferir uma ameaça à Comunidade FB? Esse aspecto é refletido por Lemos (2009), quando menciona a presença das câmeras de vigilância amplamente difundidas em nossa cultura e como são capazes de incitar justamente aspectos negativos, totalmente ao encontro com a sensação protetora ao se deixar ser vigiado. Para isso, ele associa os três postulados sugeridos por Rosello (2008), sendo que

O primeiro postulado afirma que há razões para ter “medo”. O segundo postulado constata que “o cidadão está preso entre dois medos: o medo de quem é (sendo essa uma perspectiva que ela chama de direita) e o vigiado” “medo de quem nos vigiam” (perspectiva que ela aponta como sendo de esquerda). O terceiro postulado reconhece que sentimento de insegurança é “o indesejável” (LEMOS, 2009, p. 626).

De acordo com os autores, esse aspecto constrói um binarismo entre vigiar e ser vigiado, renuncia-se à liberdade e privacidade individual para garantir a segurança social, o que estimula, ainda mais, a vulnerabilidade dos sujeitos. Essa subjetividade de ter acesso ao movimento visível sob circunstância de ser “o outro sempre ameaçador” (LEMOS, 2009) é que compreendemos, a partir da dissecação das interfaces, a seguir, que nos sinaliza haver um risco em estar “lá dentro”, mas o FB opera como uma grande câmera vigia que observa tudo e, em qualquer ameaça, já está pronto para agir.

Figura 68 - Dissecação da coleção Sujeito Inseguro e Lógica Suspeita



Fonte: Elaborado pela autora (2021).

Percebemos sentidos dessa construção em conteúdos como o discurso da plataforma em indicar ao usuário práticas de cuidado e segurança. Parece-nos como uma mãe que orienta (o)a filho(a) “não fale com estranhos”, assumindo a inocência e ingenuidade da criança em passar informações para um adulto desconhecido

Nunca compartilhe suas informações de login. Os golpistas podem criar sites falsos parecidos como Facebook e pedir para você entrar com seu endereço de e-mail e senha. Sempre verifique a URL do site antes de digitar suas informações de login. Quando estiver em dúvida, digite [www.facebook.com](http://www.facebook.com) no navegador para acessar o Facebook. Não encaminhe e-mails da Meta para outras pessoas. Eles podem conter informações confidenciais sobre a sua conta (FACEBOOK, 2021).

Na indicação da mensagem do FB<sub>2</sub> pela dissecação da tela capturada em nossa coleção, está explicitamente declarado que a ameaça se dá, exclusivamente, pela violação de dados produzida por terceiros, eximindo a plataforma de qualquer responsabilidade, acusando o usuário da conta por ter falhado em alguma etapa das políticas que preconizam a privacidade.

Nesse sentido, há questões que envolvem a prática de coleta das informações, dos usuários, para segmentação de campanhas de anunciantes do FB, conforme está indicado na interface “Nós usamos os números de celular para enviar notificações por SMS, ajudar você a entrar na sua conta e personalizar experiências, como a conexão entre as pessoas e o



aprimoramento de anúncios para todos os nossos produtos. Saiba Mais”. Essa execução de coleta e análise de dados de uso, dos usuários do FB, tendo como objetivo realizar um estudo preditivo de comportamentos, na plataforma, para fins de monetização publicitária direcionada, é uma das características do alarmante capitalismo de vigilância, que Zuboff (2020, p. 97, grifo da autora) argumenta com exemplo da empresa Google:

O Google não faria mais mineração de dados comportamentais estritamente para melhorar o serviço para seus usuários, e sim para ler as mentes destes a fim de combinar anúncios com seus interesses, que, por sua vez, eram deduzidos dos vestígios colaterais do comportamento on-line. Com o acesso exclusivo aos dados comportamentais, seria possível então saber o que um indivíduo *específico*, num tempo e espaço específicos, estava pensando, sentindo e fazendo.

Esse modelo de atividade, nomeada como “*matching*”, que vai muito além de simplesmente associar a busca por palavras-chave ao anunciante, excede e extrapola o uso de dados a partir da compilação denominada como *user profile information* (UPI), excluindo a possibilidade de se inferir ou supor algo de interesse de um possível consumidor. Agora, como uso das UPI, a exatidão das informações como resultado de uma análise preditiva de dados, correspondente com os interesses dos anunciantes, garante o *budget* publicitário a ser alocado no *target* específico, seria, de fato, expor o produto, conceito, ideia com precisão matemática ao usuário garantido (ZUBOFF, 2020).

Esse aspecto remete a outra problemática envolvendo o uso da técnica, ou do conhecimento da gestão, coleta, armazenamento e interpretação de dados que é utilizada, atualmente, em ferramentas de gestão de audiência e publicidade *online*. Ter o domínio de como operar a própria funcionalidade Facebook Ads, por exemplo, exige compreender a melhor maneira de alocar a verba de um anunciante para fins de “impulsioneamento” de conteúdo aos usuários da rede, resumidamente. A reforma do formato de compra e venda de mídia e exibição de campanhas publicitárias em veículos de comunicação “tradicionais”, como televisão, rádio e jornal, por exemplo, foi executada por grandes investidores financeiros que alocaram capital no desenvolvimento de uma tecnologia que legitimou a substituição das incertezas humanas pela comprovação matemática.

Na era do capitalismo de vigilância, é o poder instrumentário quem preenche o vazio de substituir relações sociais por máquinas, o que equivale à substituição da sociedade pela certeza, nessa imaginada vida coletiva, abre-se mão da liberdade pelo conhecimento de outros. [...] (ZUBOFF, 2020, p. 436).

De forma complementar, a vigilância instaurada nessa maneira de desenvolver e comercializar campanhas publicitárias com segmentação, a partir das UPI em grandes

plataformas de mídia da contemporaneidade, demonstra que a mensuração de performance em conteúdo *online* se tornou uma característica muito forte das mídias digitais, extrapolando a tríade anunciante/agência/veículo. A metrificação é tida, atualmente, como ferramenta de análise de investimentos em publicidade, perfilhação de audiência, ou seja, dispersou uma cultura que tudo pode ser medido e calculado. Um dos grandes impactos negativos dessa metrificação das coisas, conforme diz Zuboff (2020, p. 436), é que “o vazio que permanece é um forte sinal de vulnerabilidade social. Confusão, incerteza, e desconfiança permitem que o poder preencha esse vazio social. Na verdade, elas o incentivaram a fazer isso”.

Paralelamente ao crescimento da cultura da metrificação, que está presente no FB em diversos recursos de interação, como “curtir, comentar, compartilhar”, para o usuário comum, a maneira de ter acesso ao volume de visualizações ou “likes” dos amigos, em nossas publicações, impõe uma quantificação das relações.

É um fenômeno recente viver de forma contínua sob o olhar dos outros, ser seguido por centenas ou milhares de olhos, aumentado pelos dispositivos, sensores, holofotes, e ondas do Grande Outro, que renderizam, registram, analisam e atuam. O ritmo incessante, a densidade e o volume do olhar enviam um fluxo perpétuo de métrica avaliativa que eleva ou abaixa o valor da moeda social do indivíduo a cada clique. Na China, esses rankings são território público, distintivos reluzentes de honra ou letras escarlates que abrem ou fecham todas as portas. No Ocidente, temos “curtidas”, “amigos”, “seguidores” e centenas de outros rankings secretos que padronizam de modo invisível a nossa vida (ZUBOFF, 2020, p. 527).

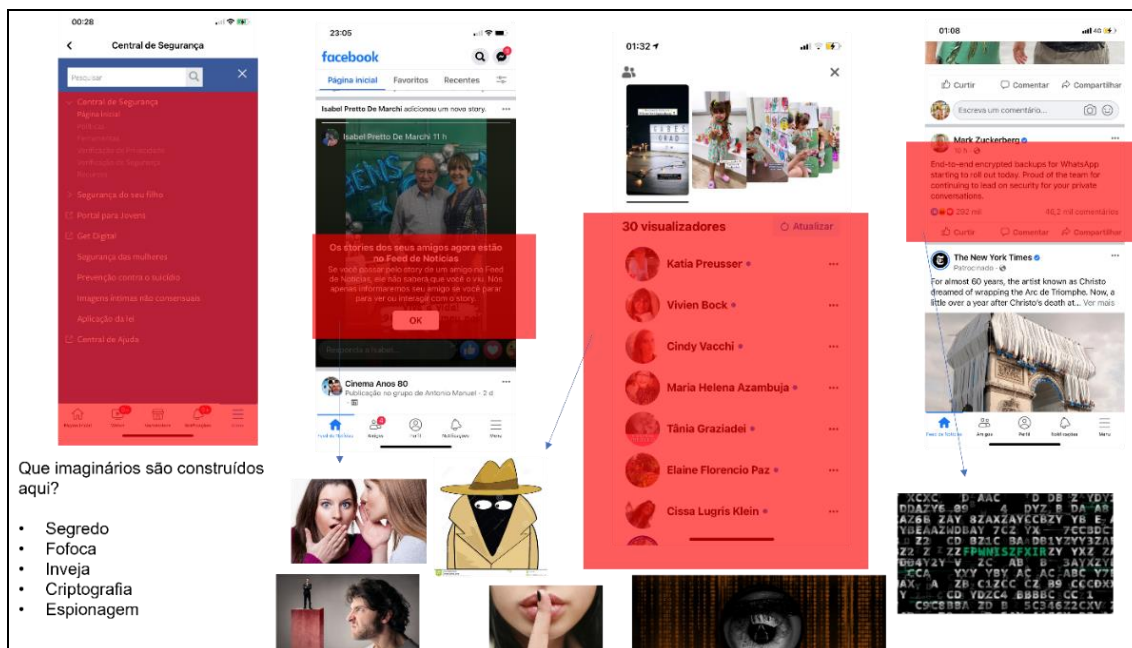
A visão de Zuboff (2020) pode ser compreendida na dissecação do arranjo adiante, onde é indicado o volume de usuários que visualizaram o *story* publicado, assim como aqueles que reagiram com um coração ao conteúdo. A plataforma explicita com foto e nome completo os “amigos” que interagiram e os que não “engajaram” na postagem. Na dissecação aparecem sentidos evocados que constroem imaginário de segredo, fofoca, espionagem, anonimato, quando a plataforma informa que “Os stories dos seus amigos agora estão no feed de notícias. Se você passar pelo story de um amigo no Feed de Notícias, ele não saberá que você o viu. Nós apenas informaremos seu amigo se você parar para ver ou interagir com o story”.

O que fica claro, nesse posicionamento da plataforma, é que há uma construção de “sacanagem” ou de traição, já que o FB explica como fazer para visualizar algo sem que outro saiba, ou seja, perpetua também a cultura de fazer “às escondidas”, de ser um *stalker*<sup>19</sup> e espiar algo dos próprios “amigos”.

---

<sup>19</sup> Termo utilizado para designar a prática de vigiar anonimamente alguém na cultura digital, principalmente, envolvendo o uso de plataformas e redes sociais.

Figura 69 - Dissecação da coleção Sujeito Inseguro e Lógica Suspeita



Fonte: Elaborado pela autora (2021).

Entendemos que esse tipo de postura, sendo incitada pelo FB, demonstra que, na verdade, os denominados “Padrões de Comunidade”, defendidos em sua Central de Segurança, não passam de meros termos de uso que nem seus desenvolvedores têm o hábito de mantê-los. Além disso, estimular a vulnerabilidade, uma postura maldosa por seus usuários, pela presença de alguém estar vigiando, perpetua a cultura do sujeito inseguro, já que a angústia é gerada, aumentando o medo e a paranoia, “aí a essência do ‘sujeito inseguro’ moderno” (LEMOS, 2009, p. 627). Nessa declaração, é reforçado o sentido de que no relacionamento do usuário com a plataforma ela é a única que pode ser confiável, afastando as relações humanas, conforme preconiza o poder instrumentário, e estimulando recorrentemente a vulnerabilidade dos sujeitos que passam a ver como único “amigo” o próprio FB que sabe de todos os seus segredos.

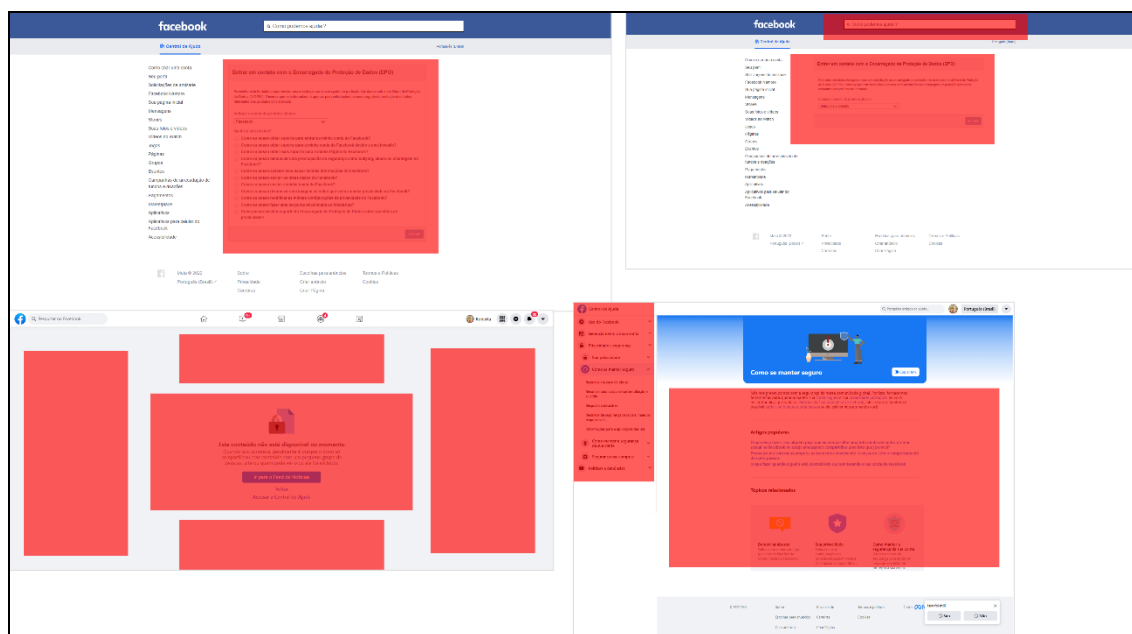
De forma complementar à defesa das informações quantificadas, na dissecação na interface há uma postagem realizada por Mark Zuckerberg, sinalizando aos seus “amigos” o lançamento da tecnologia da criptografia sendo disponibilizada para os usuários do produto WhatsApp. Esse conteúdo carrega sentidos muito fortes associados à matemática, ao uso da comunicação secreta de alta performance, associada ao militarismo para a defesa da privacidade (e do próprio Zuckerberg como *eticidade* do FB). O texto informa: “Backups criptografados de ponta a ponta para o WhatsApp começam a ser lançados hoje. Orgulhoso da

equipe por continuar liderando a segurança de suas conversas privadas”<sup>20</sup>. Novamente, o FB, via seu fundador, deliberadamente realizar a defesa “pela segurança para as *suas* conversas privadas”, extrapolando a necessidade de informar ao usuário a responsabilidade por manter seus dados seguros.

Para finalizarmos a dissecação das interfaces que compõem a coleção, compreendemos que a construção da lógica suspeita se faz presente em diversos momentos, tanto em espaços mais “divertidos” no FB, como a *newsfeed* e *timeline*, mas também nas escavações realizadas em seções como Configurações da Conta. Uma das indicações que verificamos é a constante presença da possibilidade de algo suspeito acontecer no FB, seja a ameaça aos dados do usuário, seja um comportamento “inapropriado” ou criminoso. Na Figura 70, a seguir, dissecamos dois momentos “dentro” da seção Central de Ajuda, que informam:

entre em contato com o Encarregado pela Proteção de Dados. Preencha este formulário para enviar uma solicitação ao encarregado da proteção dos dados sob a Lei Geral de Proteção de Dados (“LGPD”). Observe que este formulário é apenas para solicitações ao encarregado da proteção de dados referentes aos produtos do Facebook (FACEBOOK, 2021).

Figura 70 - Dissecação da coleção Sujeito Inseguro e Lógica Suspeita



Fonte: Elaborado pela autora (2021).

<sup>20</sup> “End-to-end encrypted backups for WhatsApp starting to roll out today. Proud of the team for continuing to lead on security for your private conversations.”

Nesse espaço é possível percebermos que há sinalização formal associada à coleta e uso de informações sobre os usuários da plataforma. Porém, fica explícito que essa seção não apresenta nenhum recurso para interação do usuário com sua própria rede de amigos, é uma área “institucional”, sem ilustração, cores ou desenhos. O imaginário que entendemos construído aqui é de um espaço “fora” da festa, independente do FB, reforçado pelo texto criado para isentar o FB da coleta de dados. Pelo texto e *layout* da interface, bastante hostil, fundo branco e uma única mensagem fria e séria centralizada na tela, parece-nos que as informações estão nas mãos de um escritório de advocacia, não do FB.

Em nossa *flânerie* e escavação realizamos a tentativa de selecionarmos as informações que gostaríamos de solicitarmos a esse “encarregado invisível”, e, após selecionarmos no **menu** as informações desejadas, fomos clicar em Enviar. Porém, a página não funcionava mais, como demonstra a dissecação. De forma complementar, compreendemos, ao intervirmos no objeto, que esse clima hostil e frio, se mantém em outras duas interfaces do arranjo, espaços de “erro” ou páginas com *links* descontinuados/quebrados no FB. Um deles sinaliza que nós não tínhamos acesso ao conteúdo “privado” de outro usuário, pela mensagem acompanhada da ilustração de uma casa com um cadeado trancado: “Este conteúdo não está disponível no momento”, quando, na verdade, ele é restrito a alguns usuários, pela afirmação do FB: “Quando isso acontece, geralmente é porque o dono só compartilhou esse conteúdo com um pequeno grupo de pessoas, alterou quem pode vê-lo ou foi excluído”. Novamente, temos a manifestação da cultura do medo, de não fazer parte, estimulada pela lógica do usuário inseguro. A partir dos sentidos produzidos, o imaginário construído parece criar molduras ao “contar um segredo somente para um amigo, enquanto o outro observa curioso e triste”, promovendo discórdia e exclusão.

Ao longo da dissecação, fomos percebendo que a *ethicidade* Sujeito Inseguro e Lógica Suspeita carrega os avisos, alertas e demais construções imagéticas e textuais, na plataforma, lançando a construção de um ambiente que, apesar de se declarar como defensor da Comunidade, pratica uma construção do vazio pela vulnerabilidade. A *desconfiança* produzida pela plataforma parece-nos alicerçada na construção de molduras que enquadram o conceito de um sujeito inseguro, povoado pelo medo e paranoia social. De forma complementar, na constelação, verificamos outra *ethicidade* que se dá por sentidos que constroem uma *imageria* do culto ao segredo, protegido e trancado, que iremos explorar melhor na coleção a seguir.

### 4.3.2 Coleção *Tecnoinsegurança*

Conforme verificamos na dissecação da coleção Usuário Inseguro e Lógica Suspeita anteriormente, o FB assume um personagem numa espécie de papel de “zelador” dos dados de quem circula por seu ambiente, informando, em diversos momentos, que o risco está, na verdade, em terceiros acessarem os dados, isentando o fato do usuário ceder suas informações para a empresa FB e seus anunciantes. Fomos percebendo que esse suposto “zelar” pela proteção dos usuários contra ameaças “externas” ao FB também acontece alicerçado em práticas de molduras e moldurações que produzem sentidos comunicados por uma *imageria* da comunicação “segura”. Podemos ver esse discurso diversas vezes nas capturas realizadas, conforme a intervenção nas imagens, a seguir, irá autenticar a proposta, e na locução da animação que compõe uma das interfaces da Central Segurança no Facebook:

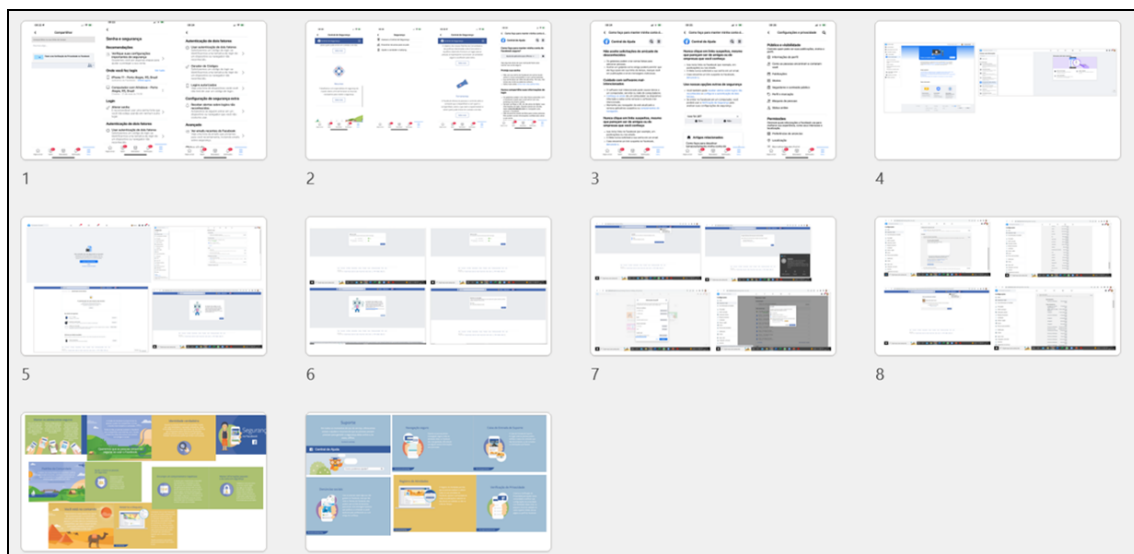
Todos os dias, as pessoas acessam ao Facebook para compartilhar suas histórias, ver o mundo através de outros olhos e se conectar com familiares e amigos. A sua segurança é a nossa responsabilidade mais importante, criamos os padrões da comunidade cujo objetivo é encontrar o equilíbrio certo entre oferecer a você um lugar para se expressar e promover uma comunidade acolhedora e segura para todos [...] (FACEBOOK, 2021).

Compreendemos que há a construção da proteção dos dados ou de uma relação do usuário contra um inimigo invisível feita através do discurso do FB. É, portanto, uma proteção concedida ao FB ser o “tutor” **dos dados**, e de se defender, constantemente, de possível ameaça nesse ambiente, seja por políticas e termos de uso, seja por exaustiva comunicação que alerta o usuário sobre ser conivente e estar “navegando” em um ambiente passível de ameaças. Essa construção de um imaginário que, então, estamos chamando pela *eticidade tecnoinsegurança*, é que constrói e alimenta a constante vigia ao suposto inimigo. Porém, identificamos que essa cultura do sujeito inseguro, dentro do FB, fica cada vez mais explícita ao escavarmos a plataforma e chegarmos em seções como Segurança, Configurações, Configurações de Privacidade e Central de Ajuda. Claramente, já se anunciam como espaços que tratam dessas temáticas (apesar de já verificarmos nas coleções anteriores que a *eticidade* usuário vulnerável constrói sentidos em diversas seções, como *timeline*, *newsfeed* e segurança no FB, por exemplo), mas que são alicerçados em uma *imageria* da comunicação “segura”, ou seja, há a presença de recursos associados à segurança do mundo digital e *offline* que percebemos fortemente na dissecação.

Estamos chamando por *imageria*, termo originalmente proposto por Rancière (2012), conforme mencionamos na introdução dessa tese, como relativo à reprodução de imagens que

estão associadas à construção de uma forma de expressão humana, carregando potência de significação. Por isso, apresentamos no arranjo de imagens que compõem a coleção *tecnoinsegurança*, segunda que faz parte da constelação Usuário Vulnerável, assim como o código QR para melhor visualizar o conteúdo em interface gráfica, manifestações dessa *imageria* de *tecnoinsegurança* que estamos identificando.

Figura 71 - Coleção *Tecnoinsegurança*



Fonte: Elaborado pela autora (2021).

Figura 72 - Código QR para visualização da coleção *Tecnoinsegurança*

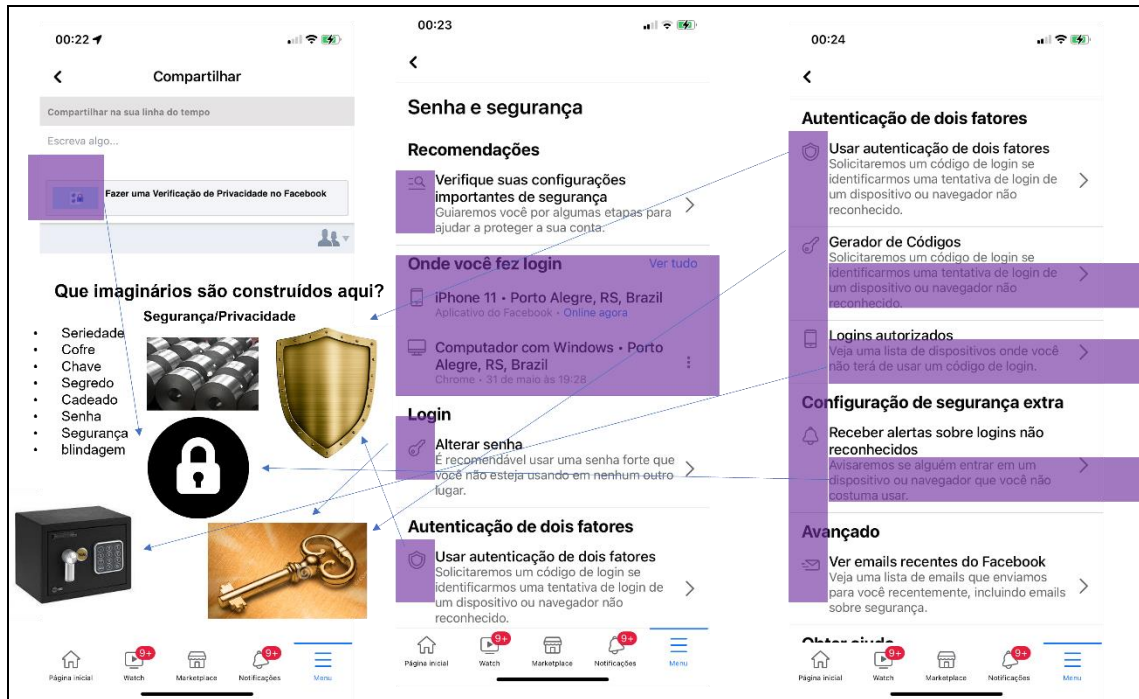


Fonte: Elaborado pela autora (2021).

Para autenticar a *eticidade tecnoinsegurança* nas interfaces que dissecamos, é importante relembrarmos que compreendemos, com base na proposta metodológica desenvolvida por Kilpp (2010, p. 18), que “as autenticações remetem, por sua vez, àquelas características do objeto que vão sendo percebidas pelo pesquisador de acordo com suas afecções (fundamentais também no método intuitivo [...])”, nesse viés, a *eticidade tecnoinsegurança* tem sentidos identitários a partir dos imaginários do que significa comunicação segura em nossa *tecnocultura* e sociedade. Isso remete ao uso frequente de uma *imageria* associada à segurança e privacidade de algo, porém, quanto mais se alerta para esses

aspectos, mais se cria a paranoia de insegurança. Vejamos as indicações desses sentidos na dissecação a seguir:

Figura 73 - Dissecação da coleção *Tecnoinsegurança*



Fonte: Elaborado pela autora (2021).

Pelas indicações da dissecação realizada nas imagens das interfaces do aplicativo FB, interferimos cirurgicamente em diversos espaços, e percebemos, como uma espécie de diagnóstico do procedimento, que os imaginários que comunicam os sentidos de segurança nesses ambientes estão construídos em indicações ilustradas de cadeados, chaves, cofres e escudos, mas também associados à vigilância. Assim como o FB informa que se protege, “a comunidade” que faz parte de sua rede, reforça explicitamente em áreas como Configurações, como proteger e manter privados os dados dos usuários, não suas amizades ou familiares.

Os elementos da imagem: um elemento é visto após o outro. O vaguear do olhar é circular: tende a voltar para contemplar elementos já vistos. Assim, o “antes” se torna “depois”, e o “depois” se torna “antes”. O tempo projetado pelo olhar sobre a imagem é o eterno retorno. O olhar diacroniza a sincronidade imaginística por ciclos (FLUSSER, 1985, p. 7).

Nas indicações acima, percebemos relevância no uso de referências culturalmente construídas as redor do termo, algumas igualmente fantasiosas, como diz Krapp (2020b) sobre o influente papel das mídias na construção desses imaginários sociais a respeito do significado de uma comunicação segura. Conforme vimos na introdução dessa tese, o envolvimento do



mercado publicitário, audiovisual e cultural em relação a essa temática é muito forte, e entendemos que o FB é um “palco” onde muitas dessas construções se refletem e são enunciadas. Mas, como atenta Krapp (2020b), essa característica, na verdade, é carregada fortemente pela cultura digital que está constantemente trazendo a segurança como algo central na atualidade. A disseminação de informações falsas, os escândalos de Snowden, Cambridge Analytica, a presença das câmeras de vigilância, sistemas de inteligência de reconhecimento facial, a “popularização” da criptografia, a lógica do sujeito vulnerável e inseguro, trazem a preocupação com privacidade e segurança de dados como um debate comum, o que leva ao uso caricato e fantasioso, a partir da reprodução pelas mídias, do real significado do que é comunicação segura.

O sujeito pode não saber o significado, mas o evento é compreensível na medida em que diz respeito (pertence e olha) ao sujeito. A paranoia também impulsiona essas reavaliações críticas na medida em que elas constroem a prevenção como uma tarefa (ou para colocar em termos mais lacanianos, na medida em que eles se concentram no significado e não na verdade). Tecnicamente falando, a paranoia é uma técnica válida de processamento de informações; não apenas as interpretações paranoicas estão corretas, mas a obsessão de um paranoico com significado, sua atração por termos aparentemente irrelevantes, fundamenta a prevenção na era da fibra óptica. O armazenamento digital automático e as redes permitem um pós-acontecimento<sup>21</sup> (CHUN, 2006, p. 257, tradução nossa).

Pela visão de Chun (2006), a paranoia e a obsessão social por controlarmos as nossas vidas e nossas informações está diretamente relacionada com a igualmente fantasiosa ideia de liberdade. Tara McPherson (2006), comenta na capa da obra de Chun (2006) que a proposta da autora se diferencia do binarismo tecno-euforia, *versus* tecnofobia “desafiando as suposições populares de que o computador é poderoso e transparente ou uma máquina de vigilância impecável”<sup>22</sup>.

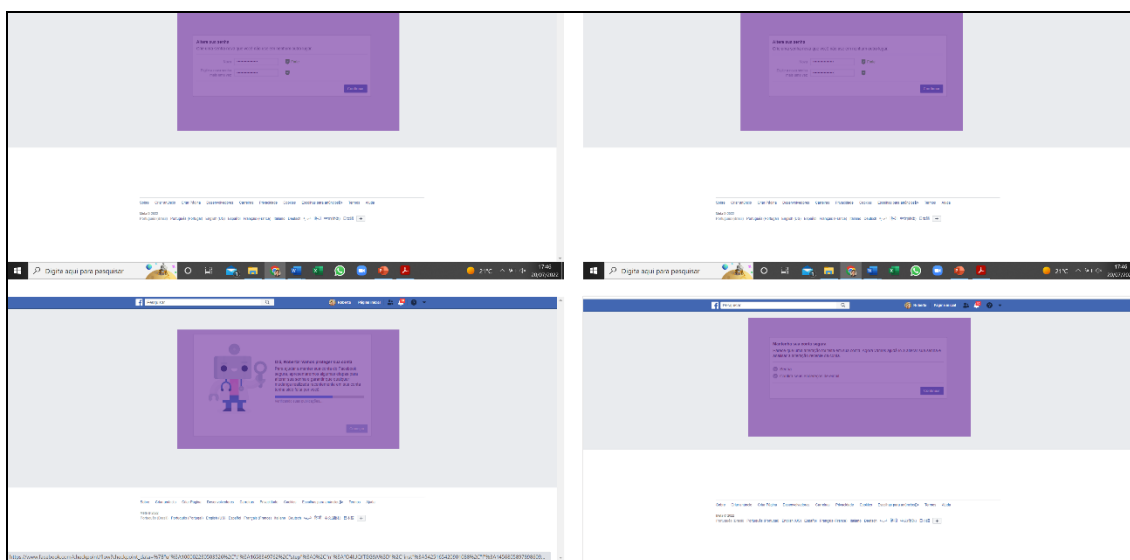
O arranjo de imagens da versão para acesso via um navegador da *web* e que foram dissecadas carregam subjetividades virtuais, ou as *ethicidades* de segurança que reforçam essa *imageria* do cadeado, do escudo, para se defender de algo e de “guardar a sete chaves” os segredos dos dados dos usuários. Mas vai além disso, utiliza recursos claramente “próprios” da cultura digital, como diz Krapp (2020b), para construir sentidos de privacidade e de

<sup>21</sup> “The subject may not know the meaning, but the event is understandable in that it regards (pertains to and looks at) the subject.<sup>13</sup> Paranoia also drives these critical reassessments to the degree that they construct prevention as a technological, rather than a political, task (or to put it in more Lacanian terms, to the extent that they focus on meaning rather than truth). Technologically speaking, paranoia is a valid information-processing technique; not only are paranoic interpretations correct, but a paranoid’s obsession with meaning, his or her pull to seemingly irrelevant terms, grounds prevention in the age of fiber optics. Automatic digital storage and networks enable a postevent.”

<sup>22</sup> “Challenging popular assumptions that the computer is either empowering and transparent or a relentless surveillance machine.”

confiança na plataforma. São funcionalidades como dicas e sugestões para troca frequente de senhas, como melhorar as senhas, ativação em duas etapas (vinculando *login* com *e-mail* e posterior disparo de um código encaminhado via SMS para confirmar se o usuário é o mesmo cadastrado na conta) e há, também, a possibilidade de fazer uma avaliação pelo FB de o quão segura está aquela conta do usuário. Entendemos que essa construção, ao invés de defender ou proteger o usuário, conforme é cirurgicamente construída, acaba por proteger constantemente o próprio FB de possíveis questões associadas à violação de dados e privacidade, que tanto marcam seu histórico. A plataforma assume o papel de “guardião” máximo ao nos informar ser capaz de avaliar o quanto segura a conta seria, ou seja, claramente anuncia que o vilão é um externo, já que o FB auxilia o usuário a manter sua privacidade de dados.

Figura 74 - Dissecção da coleção *Tecnoinsegurança*



Fonte: Elaborado pela autora (2021).

Conforme percebemos na reflexão de Castoriadis (1982), há uma função claramente simbólica sendo representada na interface do FB para garantir o significado de “comunidade” segura e que se preocupa com o bem-estar de todos seus integrantes.

O desenvolvimento do pensamento racional lúcido torna possível unir e distinguir, numa relação ao mesmo tempo firme e flexível, os três elementos que compõem o simbólico: o significante, o significado e o seu vínculo *sui generis*. O uso ‘correto’ da função simbólica supõe a função imaginária e seu domínio pela função racional (CASTORIADIS, 1982, p. 155).

Os sentidos que encontramos nas imagens, no arranjo anterior, indicam algumas etapas para proteger a senha e os dados dos usuários, e um deles, especificamente o FB, assume a ilustração de um robô, espécie de super-herói, vestindo um jaleco, carregando uma

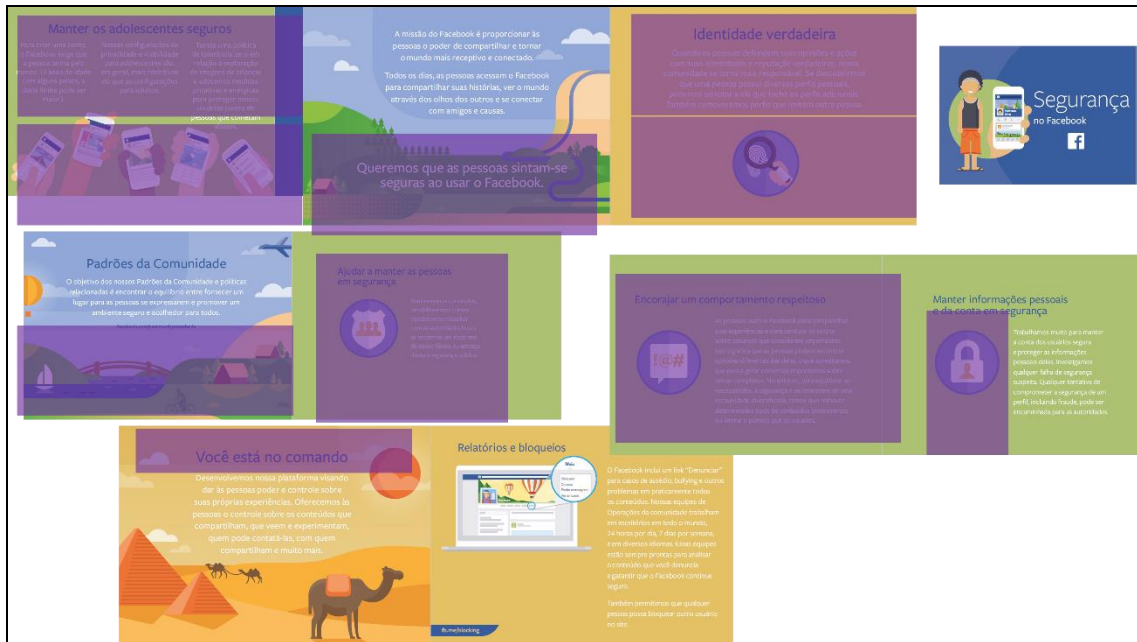
ferramenta, uma lupa e um estetoscópio, simulando um misto de médico, engenheiro mecânico e investigador, com o seguinte texto: “Olá, Roberta! Vamos proteger sua conta. Para ajudar a manter sua conta do Facebook segura, apresentaremos algumas etapas para alterar sua senha e garantir que qualquer mudança realizada recentemente em sua conta tenha sido feita por você”. Compreendemos que essa metáfora, construída de ícones, dá significado de proteção aos seres humanos, também comparece na *imageria* associada à proteção de dados da conta, como método de segurança. Chun (2006, p. 256) comenta sobre o contraste da relação proteção *versus* liberdade na internet, principalmente porque as tecnologias modernas reforçam as maravilhas da praticidade em nossos cotidianos, mas, também, são ambientes que podem ser utilizados para todos os fins como nos atos terroristas de 11 de setembro, “a Net parecia uma dádiva de Deus... Mas também há toda a probabilidade de que os terroristas também tenham explorado a Internet, usando contas facilmente disponíveis e virtualmente não rastreáveis no Yahoo ou Hotmail, e se reunindo em salas de bate-papo”<sup>23</sup>.

Essa ilustração do super-herói que é um pouco médico, engenheiro e detetive, está alinhada à concepção de Castoriadis (1991, p. 277) sobre a construção dos imaginários sociais serem produzidos pela relação com a sociedade e psiquê, ao explicitar então que “o imaginário social é primordialmente criação de significações e criação de imagens ou figuras que são seu suporte. A relação entre a significação e seus suportes (imagens ou figuras) é o único sentido preciso que se pode atribuir ao termo simbólico”.

De forma complementar à construção dos sentidos de proteção de dados estar relacionada à *imageria* de cuidado técnico e medicinal, as interfaces do arranjo, a seguir, demonstram conteúdo de segurança mas, associado aos “bons costumes” de uma comunidade, apoiado pelo uso da ilustração, das cores neutras, muito alicerçado na proposta de Bauman (2003), e que corresponde ao controle e monitoramento de indivíduos dentro de uma conduta pré-estabelecida e aceita por todos os indivíduos que nela convivem.

---

<sup>23</sup> “The contrast dramatizes a long-recognized truism: modern technologies that add efficiency, power and wonder to our lives inevitably deliver the same benefits to evildoers. The Internet is no exception. On Sept. 11 the Net seemed like a godsend... But there is also every likelihood that the terrorists had exploited the Internet as well, using easily available and virtually untraceable accounts on Yahoo or Hotmail, and meeting in ad hoc chat rooms.”

Figura 75 - Dissecção da coleção *Tecnoinsegurança*

Fonte: Elaborado pela autora (2021).

Essas interfaces foram coletadas na seção Segurança no FB, onde é apresentado um documento em versão .pdf, sob o título “segurança no Facebook”, que traz uma série de dicas e sugestões de como a segurança do cidadão, do usuário, pode ser estimulada. Essa iniciativa do FB em mencionar a proteção do usuário, do indivíduo, e não dos seus dados, retoma a discussão sobre perigo e confiança. Alguns dos conteúdos são:

**Manter os adolescentes seguros.** Para abrir uma conta, o Facebook exige que a pessoa tenha pelo menos 13 anos de idade (em alguns países a idade limite pode ser maior). Nossas configurações de privacidade e visibilidade para adolescentes são, em geral, mais restritivas do que as configurações para adultos. Temos uma política de tolerância zero em relação à exploração de imagens de crianças e adotamos medidas proativas e enérgicas para proteger nossos usuários jovens de pessoas que cometam abusos (FACEBOOK, 2021).

Não encontramos na plataforma quais seriam, de fato, as medidas mais enérgicas, mas é possível ver que há uma postura do FB em assumir práticas de controle exercidas sobre as publicações realizadas por usuários. Uma delas é sobre a metáfora da proteção de adolescentes e imagens de crianças de possíveis criminosos que habitam em seu ambiente, ou seja, há um “Big Brother” acontecendo dentro da plataforma, um grande irmão que vê e escuta tudo, mas sob a desculpa da proteção e bem-estar do usuário.

Percebemos que a *eticidade tecnoinsegurança* é construída por esses imaginários que revelam sentidos de medo sob o viés “velado” de uma prática que se anuncia como segurança, mas que, na verdade, age pelo monitoramento e controle de tudo que está sendo postado,

sendo o FB o melhor amigo que se pode confiar, já que o emolduramento criado está “protegendo” os seus usuários, não apenas os seus dados. Esse tipo de conteúdo caracteriza-se, de acordo com Zuboff (2020), por um tipo de manipulação emocional dos usuários praticada pelo FB, que opera de maneira oculta de acolhimento, que visa alterar estados de espírito e comportamento das pessoas, e entre as ferramentas está a constante comparação social.

O Facebook, e as mídias sociais em geral, é um ambiente projetado para induzir e exagerar esse sentimento de manada humana como lar, em particular entre os jovens. Somos seduzidos para o espelho social, nossa atenção cravada nos encantos sombrios da comparação social, pressão social e influência social. “Conectado o dia todo”, “conectado quase o dia todo”. Ao nos fixarmos na manada, os caçadores comerciais equipados com a tecnologia nos rondam, sorrateiros, e lançam suas redes. A intensificação artificial da manada como lar só pode complicar, atrasar, ou impedir a negociação difícil psicológica do equilíbrio eu-outro (ZUBOFF, 2020, p. 527).

A construção de um ambiente tido como lar para os adolescentes, também pode ser visualizada em outro momento da dissecação, quando verificamos a missão do FB apresentada como:

A missão do Facebook é proporcionar às pessoas o poder de compartilhar e tornar o mundo mais receptivo e conectado. Todos os dias, as pessoas acessam o Facebook para compartilhar suas histórias, ver o mundo através dos olhos dos outros e conectar com amigos e causas. Queremos que as pessoas sintam-se seguras ao usar o Facebook (FACEBOOK, 2021).

A autora Shoshana Zuboff (2020) argumenta esse posicionamento da empresa em criar um utopismo, a partir da engenharia comportamental. Uma ideia ou concepção de mundo que acontece lá dentro da plataforma, um ambiente que preconiza a proteção, o dia de sol, as amizades, comunidade feliz e segura, que se desvia de antigas fronteiras institucionais oferecendo liberdade e espaço para a autoexpressão dos usuários à vontade.

A utopia aplicada do Facebook é um protótipo do futuro instrumentário, pois demonstra feitos de engenharia comportamental que preparam populações para os rigores das harmonias coercitivas do instrumentarismo. Suas operações são planejadas para explorar a inclinação humana no que diz respeito a empatia, pertencimento e aceitação. O sistema sintoniza o tom do nosso comportamento com as recompensas e punições da pressão social, pastoreando o coração humano na direção da confluência como meio para finalidades comerciais de outros (ZUBOFF, 2020, p. 528).

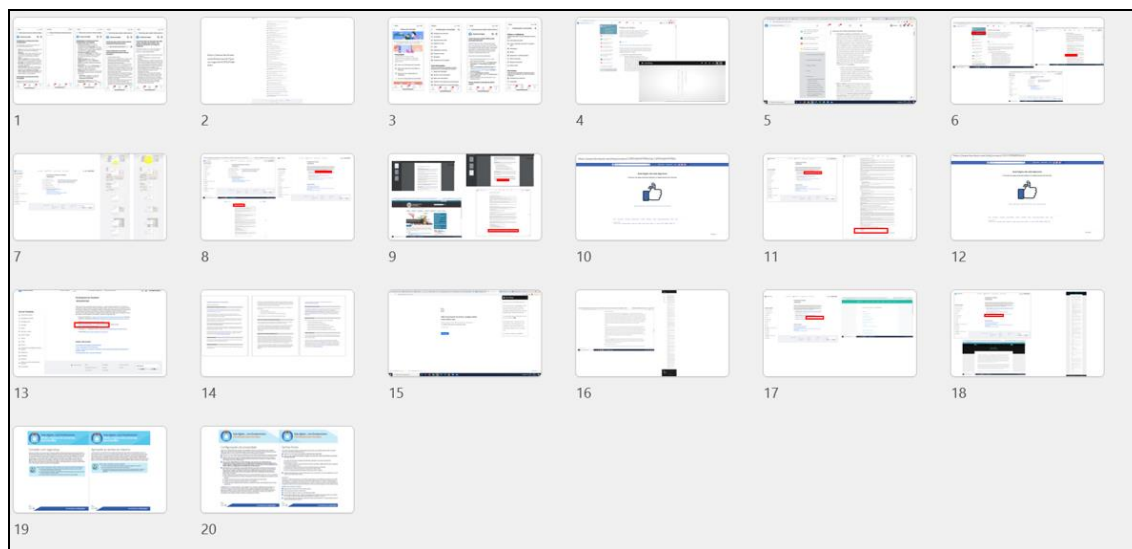
Esta colocação da autora, nos conduz aos termos de Bauman (2003), para o conceito das “fábricas de obediência”, que poderiam ser associadas ao ambiente do FB, pois fomos

percebendo, a partir da dissecação e da escavação das interfaces, que os sentidos de *tecnoinsegurança*, ultrapassam a ideia de amparar os usuários ou dados, mas, fomos vendo que há tentativas constantes de defesa do próprio FB em criar uma proteção contra possíveis ameaças à plataforma e mau uso de dados. Essa blindagem perpassa pela coleção seguinte, que estamos nomeando por Políticas de Pergaminho, onde reside o lado mais formal da defesa, da legalidade e dos chamados termos de uso e políticas das plataformas digitais.

#### 4.3.3 Coleção Políticas de Pergaminho

A terceira coleção, Políticas de Pergaminho, apresenta conjuntos de imagens que carregam *ethicidades* muito próprias da *web* e da cultura digital em fornecer políticas de regulamentação para as plataformas, mas, também, termos de uso que estão bem distantes do imaginário da coleção Infância que busca criar um universo colorido, como na constelação anterior. Estamos nomeando por Políticas de Pergaminho justamente pela associação a uma grande quantidade de conteúdo estar escrito sobre a pele de cordeiro, garantindo a fixação da tinta na superfície, e, propositalmente, dificultando a compreensão dos termos descritos sem nenhum apelo visual que vise reter a permanência do usuário. Na verdade, compreendemos que a intenção é repelir desses espaços intencionalmente, já que não são seções responsáveis por gerar receita publicitária.

Figura 76 - Arranjo de interfaces da coleção Políticas de Pergaminho



Fonte: Elaborado pela autora (2021).

Figura 77 - Código QR para visualização da coleção Políticas de Pergaminho



Fonte: Elaborado pela autora (2021).

Nesses espaços, verificamos que as interfaces assumem o lugar de fala da plataforma, como por exemplo: “Quais tipos de informações coletamos?”, “Como usamos essas informações?”, “Como operamos e transferimos dados como parte de nossos serviços globais?”. Esses conteúdos estão em seções claramente nomeadas como **Privacidade, Segurança no Facebook, Termos e Políticas do Facebook**. São lugares que o FB anuncia explicitamente os temas: privacidade, segurança (da conta, do usuário, e dos dados) e termos e políticas de uso. É possível verificarmos, pela escavação que realizamos, que esses temas foram ganhando muito mais espaço na plataforma ao longo de suas atualizações de *design*. Podemos ver que, nas primeiras versões, ainda sob o título The Facebook, no seu ano de lançamento, 2004, as questões envolvendo as então chamadas “Políticas de Privacidade”, não ocupavam mais de uma página do *site*.

Figura 78 - Coleção Território do FB - excerto de tela da seção Privacidade de 2004 no The Facebook



Fonte: Internet Archive (2021).<sup>24</sup>

Na configuração de *design* de interface na qual estamos nos debruçando à dissecação e que representam o modelo “atual” da plataforma, colecionamos, em nossa seleção, diversas capturas de telas onde o tema Privacidade e Segurança são anunciados. Ou seja, conforme os usuários foram demandando conhecimento (e os escândalos aparecendo como vimos previamente) foram ganhando força em torno da marca FB; o tema foi recebendo atenção da empresa como percebemos no aumento de volume de interfaces abordando o assunto especificamente. Nossa análise comparativa está baseada em algumas capturas que realizamos na ferramenta Wayback Machine, no Internet Archive, como exposto anteriormente. Lá

<sup>24</sup> Maiores informações em <https://web.archive.org/web/20070630042627/http://www.facebook.com/terms.php>.



fizemos tentativas de aplicação de URL, conforme o conteúdo de privacidade e segurança e encontramos as imagens que estão com o *layout* do FB numa configuração de arte criada (assumindo aqui uma dimensão mensurável do tempo) para publicação logo em seu período de lançamento, no ano de 2004.

Ao longo dos anos e da mudança de alteração de *layout* da plataforma, questões específicas de exibição do tema privacidade e segurança foram sendo suprimidas nesses termos, e foram sendo claramente atribuídas a uma arte simples e carregada de políticas e regulamentações. No decorrer do desenvolvimento da dissecação das interfaces, fomos impactados pela mudança de nome da empresa Facebook Inc. para Meta, conforme já mencionamos. Essa alteração, associada fortemente ao Metaverso<sup>25</sup>, também reverberou na suposta “revisão” das políticas de privacidade da empresa, conforme relato da Privacy Tech (2022), portal dedicado à publicação de conteúdo sobre privacidade e proteção de dados:

Para facilitar compreensão, Meta atualiza políticas de privacidade do Facebook e Instagram. Desde que se tornou “Meta”, a empresa dona do Facebook e do Instagram vem anunciando diversas mudanças. A mais recente é a mudança nas políticas de privacidade das suas redes sociais e também do aplicativo Messenger.

Conforme relato na notícia, o profissional que atua como vice-presidente da empresa, Rob Sherman (PRIVACY TECH, 2022), assume que “atualmente, a política de privacidade é uma grande muralha de texto. Além de ser longa, é complicado para as pessoas entenderem”. De fato, fomos percebendo essas enormes construções textuais como perfeitas muralhas virtuais, que apresentam um grande volume de informação e termos técnicos, muito associados ao campo jurídico e distantes da compreensão do público em geral. Claramente, o próprio FB percebeu essa característica em suas interfaces e assumiu que, nas palavras de Sherman (PRIVACY TECH, 2022):

Inspirados pelo feedback de especialistas em privacidade e dos usuários das nossas tecnologias, reescrevemos e redesenhamos a política para facilitar a compreensão das pessoas para que assim pudessem tomar decisões informadas sobre como desejam usar nossos produtos. Em segundo lugar, queríamos dar uma cara nova ao local onde as pessoas conseguem encontrar informações sobre as nossas práticas de dados e dar mais visibilidade às ferramentas e controles de privacidade disponíveis.

---

<sup>25</sup> “O primeiro uso do termo foi no ano de 1992, por Neal Stephenson no romance *Snow Crash*. No livro os personagens utilizam avatares digitais para explorar um universo virtual feito em computação gráfica 3D. Em quase 500 páginas, o autor previa que o metaverso seria um sucessor da internet e das redes sociais” (LABMEM, 2022).

A seguir, é possível verificarmos o comunicado oficial da empresa, aos usuários da plataforma, referente à alteração de nome através de conteúdo publicado em *banner* na *newsfeed* do FB:

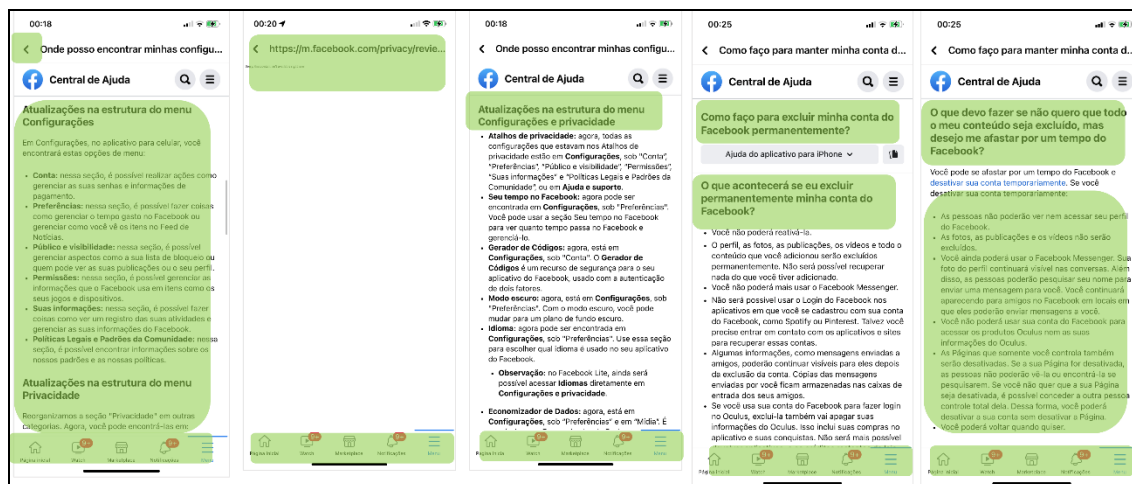
Figura 79 - Captura de tela da sinalização de mudança de nome da empresa Facebook Inc. para Meta (1 nov. 2021)



Fonte: Elaborado pela autora (2021).

Nesse sentido, realizamos uma escavação dessas interfaces, como na seção **minhas configurações**, que são propositalmente negligenciadas pelo FB, ou melhor percebemos que há seções que o FB deseja que sejam renegadas pelo usuário, pois são áreas da plataforma dedicadas a conteúdos sobre configurações e segurança de cada conta, dados de acesso, histórico de buscas, reconhecimento facial. Nesse ambiente não há aproveitamento comercial de anúncios, tampouco área para publicação de conteúdo ou interação com os demais usuários do FB. O espaço é dedicado para informar sobre a conta de usuário cadastrado. Uma relação restrita à plataforma *versus* usuário, onde são ofertadas as informações principais sobre nossas preferências e suas opções de navegação.

Figura 80 - Dissecção da coleção Políticas de Pergaminho



Fonte: Elaborado pela autora (2021).

Percebemos, pela dissecção do arranjo de capturas de tela da interface do aplicativo do FB para dispositivos móveis, que aquele ambiente colorido e alegre foi substituído por longos textos explicativos e técnicos. Com pouco apelo visual, poucos *hiperlinks* e nenhuma imagem ou ilustração de apoio. Na verdade, as interfaces apresentam fundo branco e texto em preto, com fonte pequena e um emaranhado de conteúdo mal diagramado. É possível verificarmos que os imaginários que comunicam sentidos de *tecnosegurança* aqui estão sendo alicerçados em uma prática de regulamentação, que auxilia a construir a arquitetura de confiança com o usuário, a partir de associações com legislação e diretrizes regulamentárias de “boas práticas” para a comunidade democrática do FB.

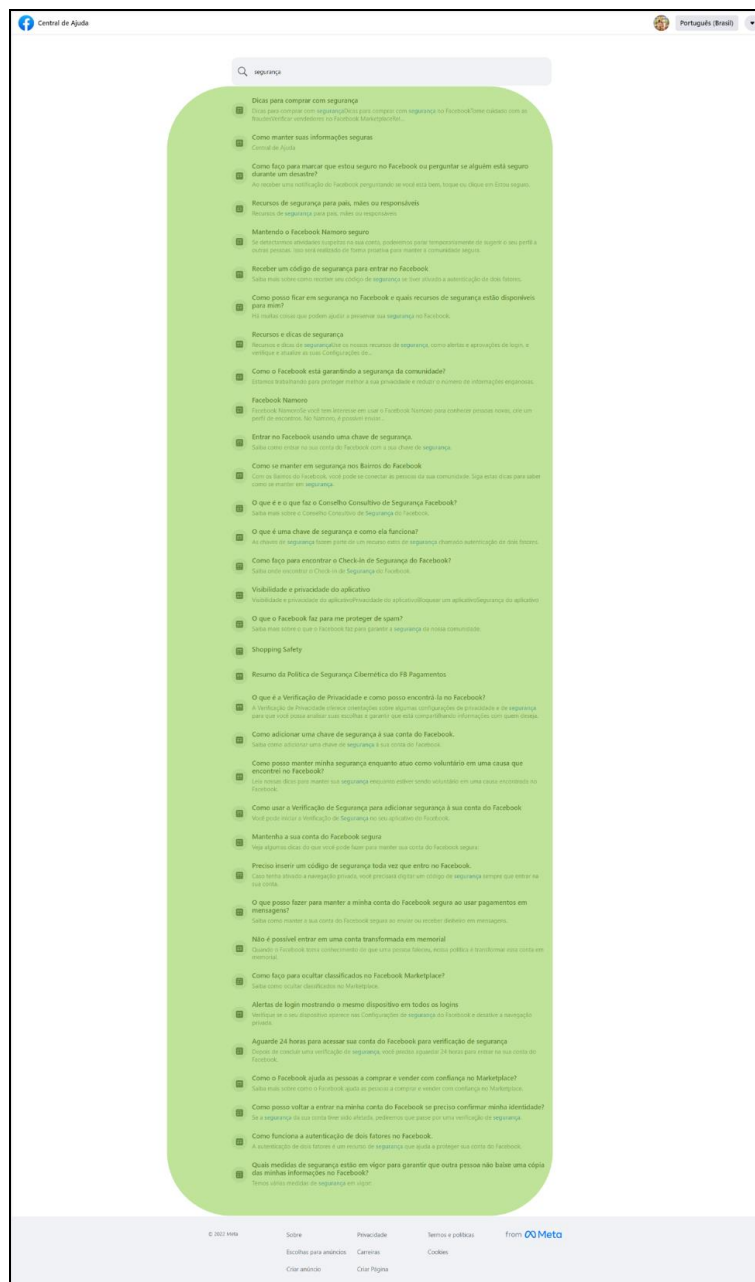
Além disso, encontramos algumas táticas de fuga da seção, ou seja, convites do FB para chamar a atenção do usuário para influenciar a retornar para a *newsfeed* ou *timeline*, conforme a sinalização em grande destaque na cor vermelha na área inferior da interface, a única que apresenta o recurso do desenho da *ethicidade* infância, neste local. A sinalização com a seta, no topo superior da tela, indicando como retornar ao conteúdo anterior também reforça a indicação para não seguir adiante, ou seja, claramente informando o usuário para retornar e não avançar em compreender diretrizes e políticas de uso.

Permanecendo no movimento de escavar os conteúdos, utilizamos a ferramenta de busca da plataforma, dentro da seção Minhas configurações, e digitamos o termo segurança. A seguir, a interface explicita o resultado do buscador a partir da indexação de conteúdo associados à *tag* e apresentados em um formato de texto corrido sem nenhum direcionamento, por exemplo, à Central de Segurança do FB, que dissecamos nas coleções anteriores. Associamos os sentidos enunciados como um grande papiro, um documento longo e repleto

de texto, comunicando as vinculações do tema segurança e FB. Dentre os resultados, há sugestões como “Dicas como comprar com segurança”, “O que é e o que faz o Conselho Consultivo de Segurança do Facebook?”, “O que o Facebook faz para me proteger de spam?”, “O que é uma chave de segurança e como ela funciona?”, “Mantenha sua conta do Facebook segura” e “Como o Facebook está garantindo a segurança da comunidade?”.

Inferimos que o imaginário que emerge desses conteúdos associados ao Direito, à regulamentação, reforça que o ambiente possui leis e, portanto, é protegido por alguém. O FB acaba criando atuação de protetor e, também, como uma espécie de postura de constante defesa, ou seja, quanto mais regulamenta, mais se controla o que acontece lá dentro, mais se monitora e vigia, autenticando, assim, a *ethicidade* das políticas de pergaminho como certificação para manter a comunidade “segura”.

Figura 81 - Dissecção da coleção Políticas de Pergaminho

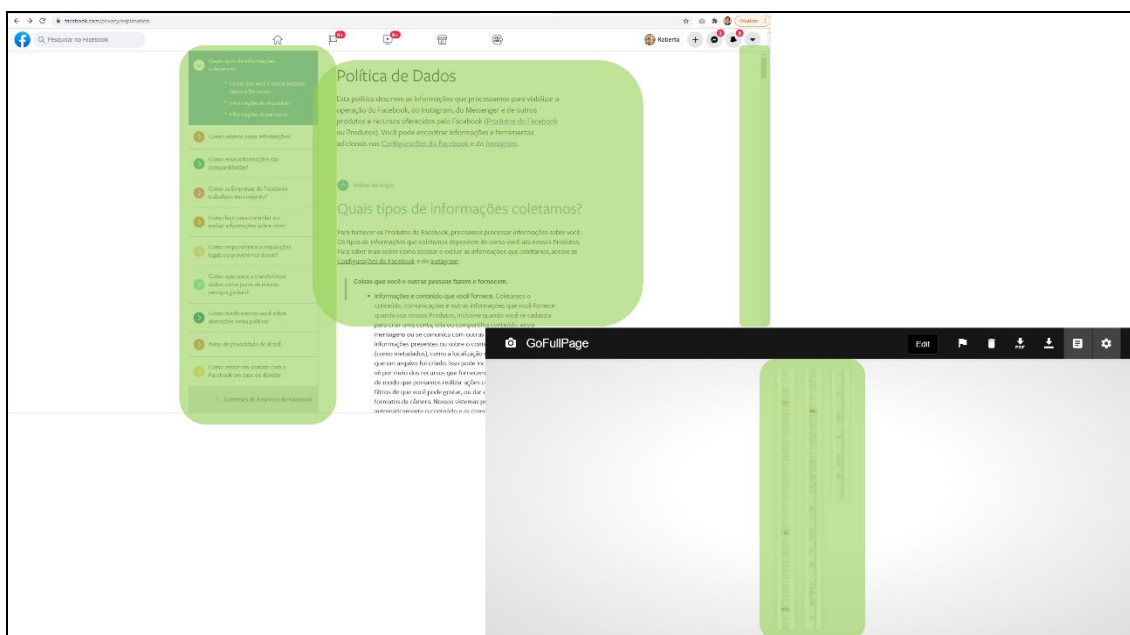


Fonte: Elaborado pela autora (2021).

E, ao vagar por áreas nomeadas claramente pelo FB, como na seção Privacidade, essa construção se torna cada vez mais “adulta”, com a supressão de cores e estímulos interativos ao usuário. Aqui nesse espaço, são expostas as “leis” de proteção dos dados do usuário (e também a própria defesa em favor do FB), que é disponibilizada em uma página contendo mais de uma centena de questionamentos e diretrizes. A seguir, realizamos a captura da interface “atualizada”, recentemente, de acordo com a revisão das políticas de uso da Meta para se tornar mais acessíveis e compreensíveis pelos usuários do FB. Porém, ironicamente, nossa ferramenta de captura das imagens na *web*, Google Full Page Screen Capture (2022,

tradução nossa), nos sinalizou a seguinte mensagem após darmos o comando de coleta: “Nota: esta página é muito grande para o navegador capturar como uma imagem. Será dividido em 3 imagens”<sup>26</sup>, ou seja, a página gigantesca foi separada em 3 imagens diferentes por se tratar de um conteúdo muito extenso. Na Figura 82, é possível verificarmos a captura da página inteira, e as seções aproximadas para leitura de cada etapa pelo usuário:

Figura 82 - Dissecção da coleção Políticas de Pergaminho para compararmos leitura aproximada e captura da página completa

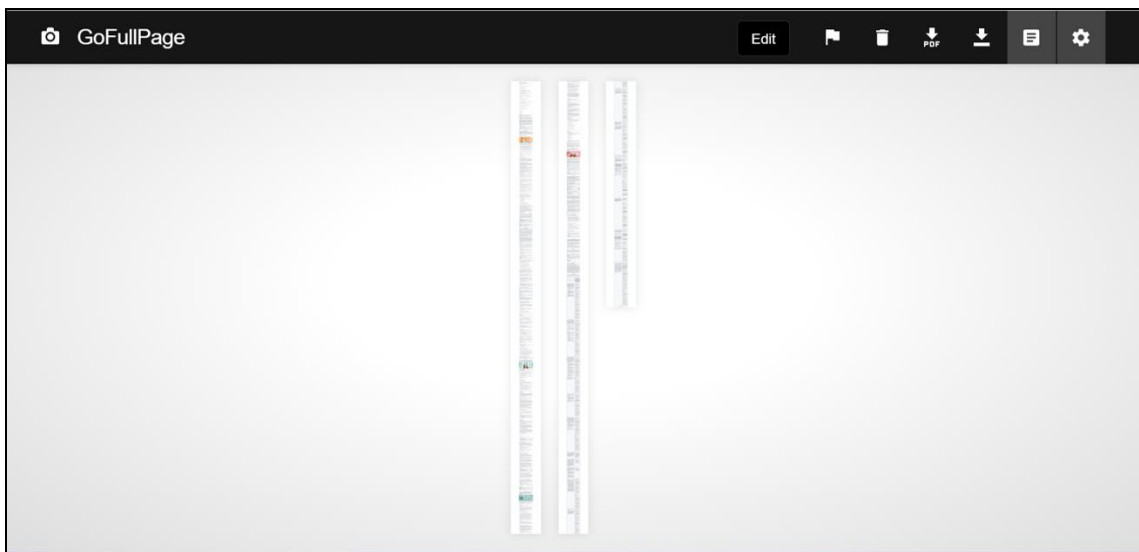


Fonte: Facebook (2022)<sup>27</sup>.

<sup>26</sup> “Note: this page is too large for the browser to capture as one image. It will be split into 3 images.”

<sup>27</sup> Maiores informações em <https://free.facebook.com/privacy/policy/#>.

Figura 83 - Captura das 3 imagens que compõem a seção completa das Políticas de Privacidade do FB



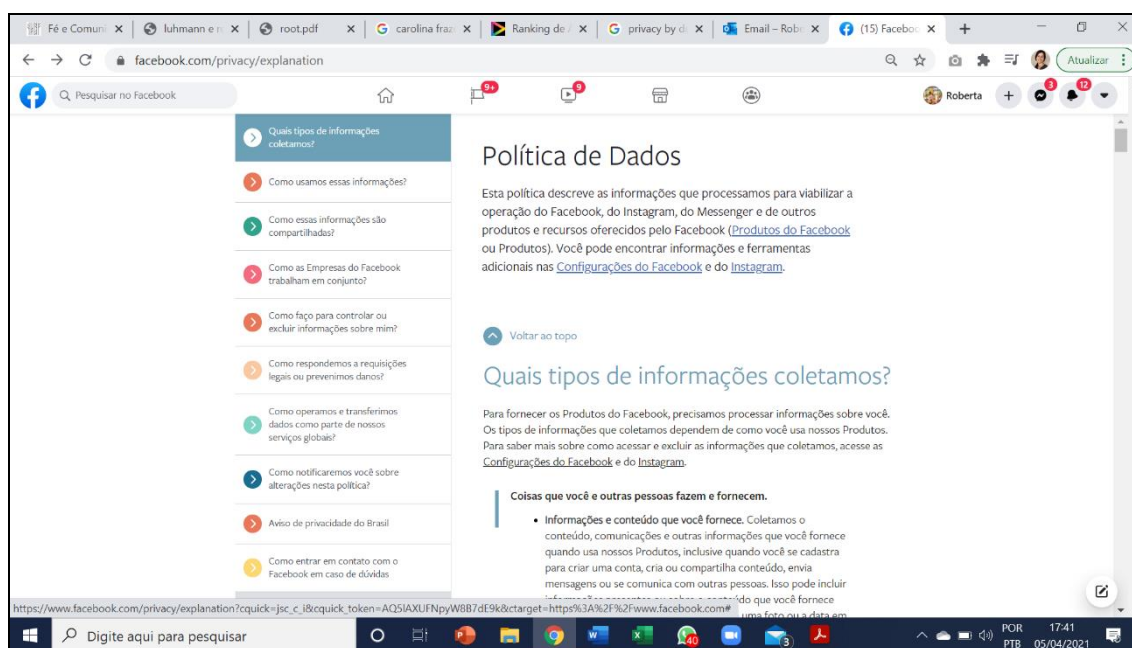
Fonte: Facebook (2022).

Claramente, esses termos são produzidos para defender e tentar “blindar” o FB de ameaças jurídicas, do que servir para o apoio ao usuário comum, já que seu conteúdo e interface não são nada convidativos para acesso ou compreensão. Nesse aspecto, Zuboff (2020) comenta sobre os chamados “termos de adesão de serviços” que foram sendo estendidos por “políticas de privacidade”, ou termos de expropriação, que acabam por apresentar muito mais práticas impositivas do que em consenso, porque, de acordo com peritos jurídicos, não é dada a opção ao usuário de discordar, ou seja, para usufruir do FB, pois ou você aceita os termos, ou não vai criar uma conta na plataforma.

Contratos online tais como acordos de termos de serviço ou termos de uso também são conhecidos como *click-wrap*, literalmente clicar-embrulhar, em inglês, porque como grande parte das pesquisas mostra, a maioria das pessoas fica enrolada nesses termos de contrato opressivos, e apenas clica na caixinha que diz “eu concordo” sem sequer ler o acordo. Em muitos casos, o simples ato de navegar por um site já obriga o internauta ao acordo de termos de serviço mesmo que ele não saiba disso (ZUBOFF, 2020, p. 64).

Nesse aspecto, a autora colabora com a defesa da LGPD que comentamos anteriormente nessa tese, e sobre o uso personalizado e sob consentimento de *cookies* para coleta de informações sobre os usuários que visitam um *site* no Brasil, por exemplo.

Figura 84 - Excerto de tela da seção Políticas de Privacidade, na versão anterior à atualização da Meta (jul. 2022)



Fonte: Facebook (2021).<sup>28</sup>

Após realizarmos a dissecação, tirarmos as imagens do fluxo da *web* e tentarmos autenticarmos sentidos da coleção das *eticidades*, percebemos que há uma construção de um possível consentimento desinformado, por parte do usuário, ao concordar com esses termos de uso e políticas de dados. Esses documentos são exaustivamente longos e complexos e acabam por, intencionalmente, desincentivar o usuário a ler o conteúdo.

Os termos de serviço podem ser alterados de modo unilateral pela empresa a qualquer momento, sem o conhecimento ou consentimento específico do usuário, e, em geral, os termos costumam implicar outras empresas, (associados, fornecedores, distribuidores, intermediários em propaganda, etc) sem declarar ou aceitar responsabilidade pelos termos de serviço delas. Esses “contratos” impõem ao usuário uma regressão infinita impossível de ser vencida e a qual a professora Nancy Kim descreve como “sádica” (ZUBOFF, 2022, p. 65).

Outra característica desses ambientes, que apresentam molduras desse tipo no FB, é a complexa arquitetura de informação, ou seja, os *links* que o próprio termo apresenta, ou redireciona o usuário para um clique anterior, ou leva para outro ambiente que o “dispersa”, ou apresenta um *link* quebrado, ou seja, ele nunca “avança” no conteúdo.

Pela escavação que realizamos, para tentar compreendermos esse ambiente das políticas de privacidade de FB, nos deparamos com diversos “becos sem saída”, uma espécie de labirinto de *links* e páginas que claramente nos confundem em compreendermos o

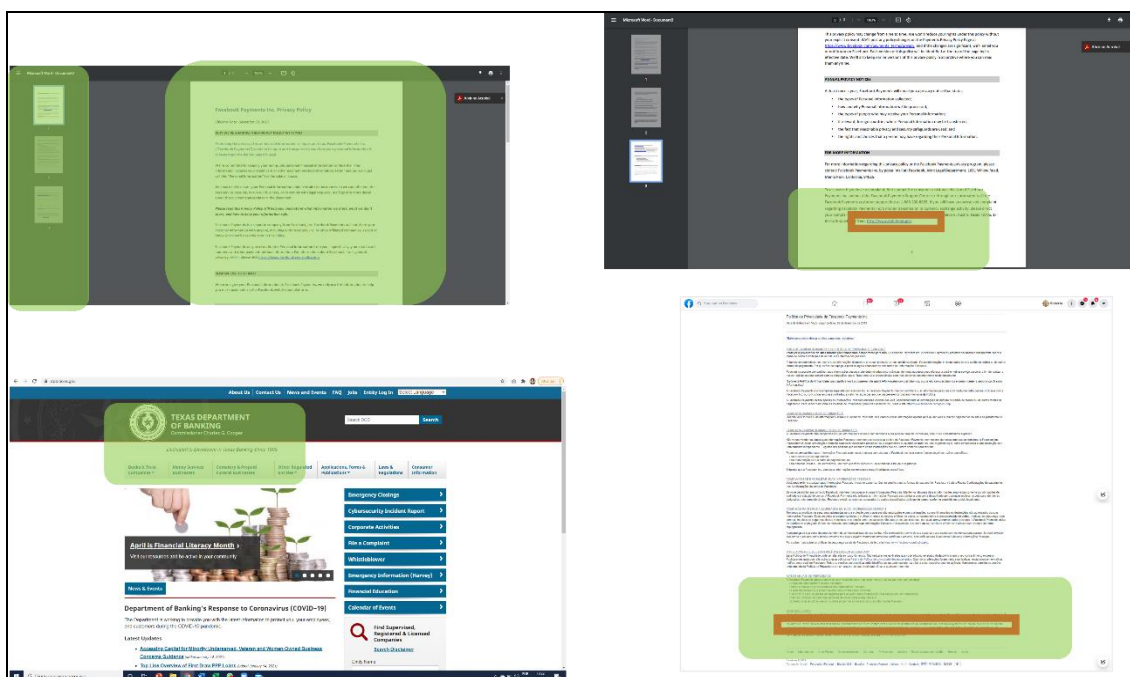
<sup>28</sup> Maiores informações em <https://www.facebook.com/settings/?tab=account>.



conteúdo e, de fato, “onde estamos” nas políticas apresentadas. A seguir, demonstramos as capturas de alguns dos movimentos em seções que fomos direcionados, partindo da página de política de privacidade. Fomos clicando nos *links* ofertados para tentarmos compreender quais são os temas relacionados aos termos, e, nessa dispersão intencional do FB, fomos redirecionados para páginas externas contendo desde regulamentação de dados da união europeia até um *site* de impostos sobre compras do estado norte-americano do Texas, o Texas Department of Banking.

Além disso, é importante salientarmos que, frequentemente, os *links* abrem documentos em arquivos com extensão .pdf, arquivos não editáveis, apresentando documentação ou políticas e termos e contratos de uso, como a ferramenta Facebook Payment Inc. Privacy Policy, que detém as formas de monetização dos anúncios dentro da plataforma, como uma outra empresa responsável pelos pagamentos dos anunciantes do FB. Também nos deparamos com um documento disponível para *download* contendo a prepotente sugestão de “Dicas e tópicos de conversas para famílias”, com fundamentos para as pessoas “se tornarem mais digitais”, com segurança a partir do FB.

Figura 85 - Dissecção da coleção Políticas de Pergaminho em áreas dispersas ao FB



Fonte: Elaborado pela autora (2021).

Dentre as molduras enunciadas nos *links* “quebrados” e páginas descontinuadas, textos infinitos e explicativos com linguagem complexa, falta de possibilidade de interação e contato com demais usuários da rede, recursos legais explícitos, cuja intenção da plataforma sinaliza,

em seus extensos termos de uso, auxiliam a comunicar sentidos que enunciam a construção de vulnerabilidade ao usuário, construindo uma lógica sombria de quem não respeitar as regras, poderia ser uma ameaça hostil que, sob penalidade, estaria fora da comunidade FB.

Para dar continuidade à dissecação das coleções, o próximo subcapítulo apresenta a última constelação que compõe a galáxia da *tecnosegurança* pela ambiência FB. Estamos chamando Ambiência da *Tecnosegurança* Contemporânea a junção por afinidades eletivas de capturas de interfaces que não são de “dentro” do FB, mas, de interfaces que reforçam e autenticam sentidos que dissecamos no e do FB.

#### **4.4 Terceira constelação - Ambiência da *Tecnosegurança* Contemporânea**

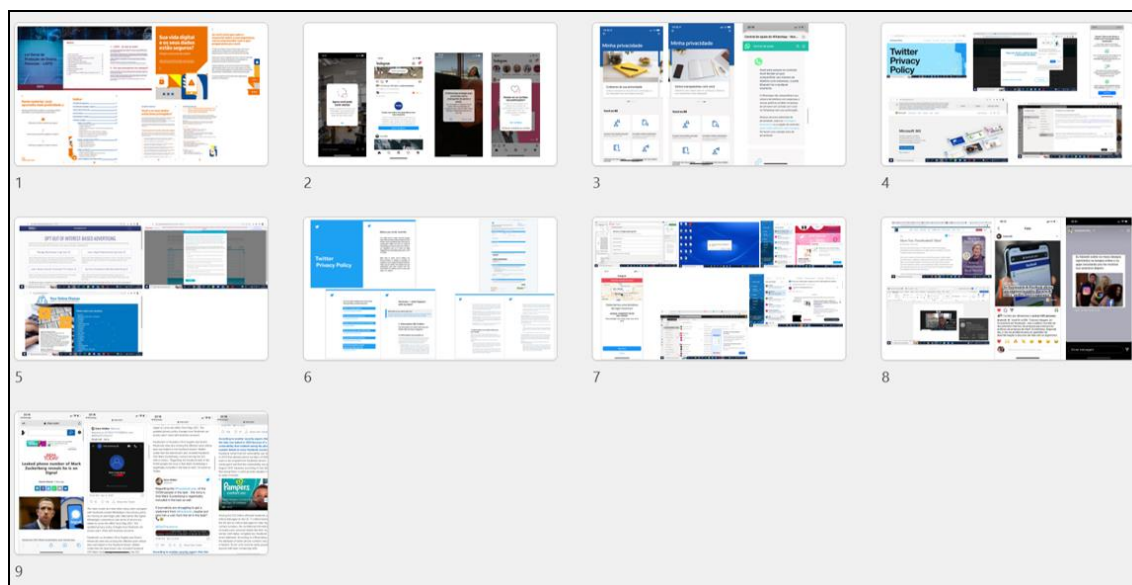
A terceira e última constelação de nossa tese, denominada por Ambiência da *Tecnosegurança* Contemporânea, contém duas coleções de imagens de interfaces coletadas ao longo de nossa *flâneria*. Essas capturas foram realizadas em ambientes paralelos ao FB, quando selecionamos e fomos guardando diversas manifestações na *web*, em aplicativos de dispositivos móveis e em outros *softwares* que fazem parte da nossa *tecnocultura* atual. São coletas de outros espaços que carregam imaginários sobre a preocupação do mundo *cyber* com a dimensão da segurança, que compõem o que estamos chamando por ambiência da *tecnosegurança*. Optamos por fazer esse movimento desde que fomos percebendo, no FB, os sentidos e as *ethicidades* que já apresentamos ao longo das constelações anteriores, mas, pelo nosso olhar, através da pesquisa, compreendemos que a segurança está enraizada no processo da computadorização e softwarização da cultura, desde a “chegada” da presença da internet e tudo o que ela produz em nossa sociedade.

O termo ambiência aqui escolhido, remete ao conceito proposto por Lopes (2014, p. 33) quando sugere, em sua tese de doutoramento, a nomenclatura para contextualizar “um contexto dinâmico, sempre em mutação, que surge das tensões e dos atravessamentos provocados pelas práticas sociais que se efetuam sobre os meios técnicos de dada cultura”. E, nesse sentido, compreendemos que essa constelação compõe, junto com as demais que mapeamos em nossa cartografia, a galáxia da *tecnosegurança* como uma espécie de “fotografia” dos sentidos que constituem a ambiência da *tecnosegurança* contemporânea.

#### 4.4.1 Coleção Medo e Vigilância

As duas coleções contém *imaginários* que dão origem às *ethicidades*, que são agenciados por *emolduramentos*, nessas imagens das interfaces, e optamos por segmentar em duas coleções, na primeira delas, nomeada Medo e Vigilância, percebemos imaginários que comunicam sentidos associados a apreensão em relação ao ambiente da *web*, algo complementar ao que já dissecamos na constelação usuário vulnerável, pois percebemos claramente enunciações de vigilância e perigo de maneiras mais explícitas do que no FB. Essas construções vão desde conteúdos associados ao Direito Digital<sup>29</sup>, até o reforço da *imageria* em torno do medo da violação de privacidade e do roubo de dados. Além disso, há sentidos de vigilância, próximos ao que dissecamos na constelação Confiança Programada, mas que, também, se dispersa por ambientes financeiros, notícias, serviços de provedores de *e-mail* e redes sociais, por exemplo.

Figura 86 - Arranjo das interfaces que compõem a coleção Medo e Vigilância



Fonte: Elaborado pela autora (2021).

<sup>29</sup> O Direito Digital é um ramo do Direito que tem como objetivo proporcionar as normatizações e regulamentações do uso dos ambientes digitais pelas pessoas, além de oferecer proteção de informações contidas nesses espaços e em aparelhos eletrônicos (FACHINI, 2022).

Figura 87 - Código QR para visualização da coleção Medo e Vigilância



Fonte: Elaborado pela autora (2021).

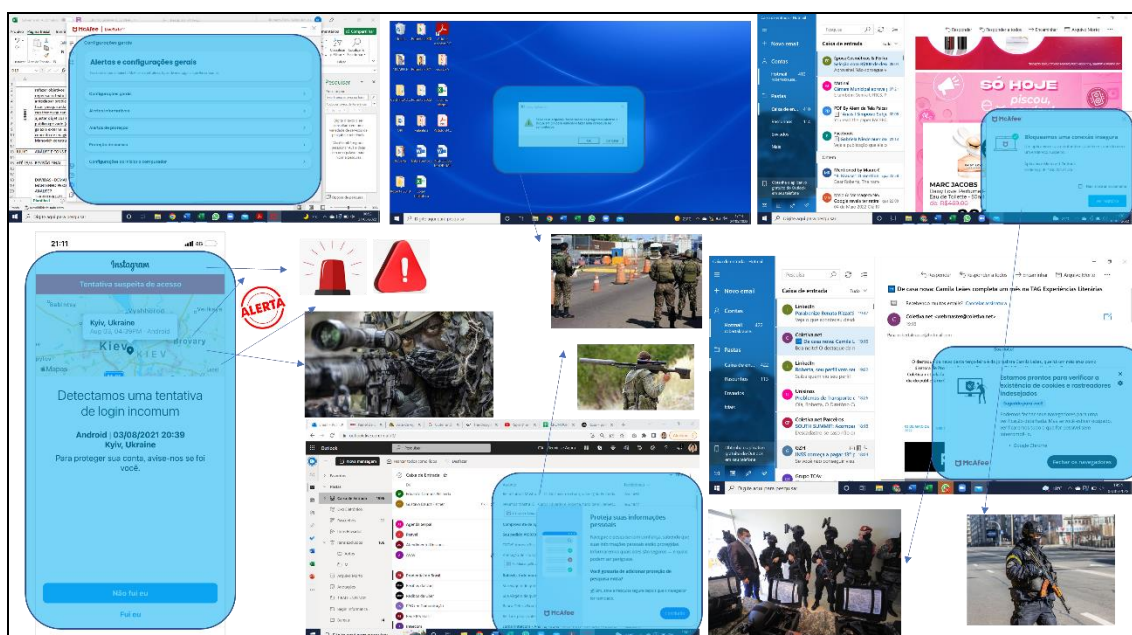
Para dar início ao processo de dissecação das interfaces e demonstrar nosso modo de “identificar as marcas de enunciação de culturas (identidades coletivas), manifestas e visíveis nos discursos, na arte, nos produtos culturais... ou que são por eles mediadas” (KILPP, 2010, p. 18), a partir dos imaginários, precisamos demonstrar que a coleção é composta por capturas de telas de diferentes momentos (assumindo novamente aqui a dimensão mensurável do tempo) durante o doutoramento, algumas pertencem ao formato de tela para dispositivos móveis, outras foram coletadas na *web* em formato *desktop*. Fomos percebendo essas construções de sentidos paralelamente ao que estávamos encontrando nas dissecações das interfaces do FB, e fomos armazenando, em pastas diferentes, em nosso computador. Porém, nossa intenção aqui não é tratarmos de maneiras distantes ou opostas essas interfaces “externas” ao FB, mas, justamente, assumirmos que há uma discussão sobre segurança, ou melhor, *tecnosegurança*, em nossa cultura, que está entranhada no pano de fundo da internet e sua promessa como um espaço que transita na dicotomia entre público e privado, proteção e controle. Conforme traz Chun (2016, p. 104, tradução nossa),

Em meados da década de 1990, a Internet surgiu como “ciberspaço”, um espaço de liberdade e anonimato. Em 1996, John Perry Bar Low declarou infamemente a independência do ciberspaço, escrevendo: “Nós [no ciberspaço] estamos criando um mundo no qual todos podem entrar sem privilégios ou preconceitos concedidos por raça, poder econômico, força militar ou estação de nascimento. Estamos criando um mundo onde qualquer pessoa, em qualquer lugar, pode expressar suas crenças, por mais singulares que sejam, sem medo de ser coagida ao silêncio ou à conformidade.” A ficção científica apresentou essa crença na internet de meados dos anos 1990 como ciberspaço, como espaço ideal livre de coerção física. Sentado em uma máquina de escrever e inspirado pelo mundo dos fliperamas e punk rock, William Gibson cunhou o termo “ciberspaço” em 1982, onze anos antes do National Center for Supercomputing Applications (NCSA) apresentar o Mosaic, o primeiro navegador da web baseado em gráficos.<sup>30</sup>

<sup>30</sup> “As outlined in chapter 2, in the mid 1990s, the Internet emerged as ‘cyberspace’, a space of freedom and anonymity. In 1996, John Perry Bar low infamously declared the independence of cyberspace, writing, ‘We [in cyberspace] are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity’. Science fiction grounded this belief in the Internet of the mid 1990s as cyberspace, as an ideal space free from

Nas interfaces que dissecamos, fomos percebendo esses sentidos associados à imaginários de medo, com constantes alertas e sinalizações de perigo pelas interfaces, como, por exemplo, situações suspeitas detectadas em *login*, como demonstra a captura do aplicativo Instagram, sinalizando um suposto acesso realizado em nossa conta, mas, na localização geográfica da cidade de Kiev, Ucrânia<sup>31</sup>, o que sinaliza um acesso duvidoso, visto que felizmente não estávamos lá (assumindo agora a dimensão da materialidade, espacial). Com sinalização em cor vermelha, a mensagem também carrega sentidos de vigilância quando identifica o sistema operacional do suposto *login*, data, região e horário da tentativa.

Figura 88 - Dissecção da coleção Ambiência da Tecnosegurança Contemporânea



Fonte: Elaborado pela autora (2022).

Na dissecção das imagens, identificamos sentidos de medo e vigia, com um misto de imaginários de controle e perigo. As imagens que representam esses sentidos, quando utilizamos as palavras-chave em buscadores, aparecem em imaginários de exército, armamento e ameaça. As mensagens de sistemas antivírus, por exemplo, carregam a *imageria* fantasiosa que Krapp (2020b) alerta e autentica as mídias como o grande responsável por disseminar essa construção utópica de que segurança *versus* vírus *versus* proteção, se dariam

---

physical coercion. Sitting at a typewriter and inspired by the world of video arcades and punk rock, William Gibson coined the term 'cyberspace' in 1982, eleven years before the National Center for Supercomputing Applications (NCSA) introduced Mosaic, the first graphics-based web browser."

<sup>31</sup> É importante salientarmos que a cidade de KIEV foi o primeiro alvo de bombardeiro da Rússia na Guerra declarada por Vladimir Putin, presidente Russo, em fevereiro de 2022. "Nas primeiras horas de 24 de fevereiro, Vladimir Putin anunciou a operação militar que, desde então, se aproxima da capital Kiev e se tornou um dos maiores conflitos militares na Europa desde a Segunda Guerra Mundial, desencadeando a maior crise de segurança no continente desde a Guerra Fria" (CNN BRASIL, 2022).

com pirotecnia. Na verdade, o que o autor comenta é que um possível crime cibernético jamais faria isso a partir de algum alerta ou sinal vermelho, mas de forma extremamente silenciosa preconizando a discrição e impercepção por parte do usuário ou do sistema operacional. De maneira complementar, Chun (2016, p. 208, tradução nossa) reforça que “curiosamente, em termos de crimes sexuais envolvendo jovens, o maior número de casos envolvendo SRS (sites de redes sociais) foram operações secretas, nas quais os investigadores criaram páginas da web e perfis ao retratar menores online”<sup>32</sup>.

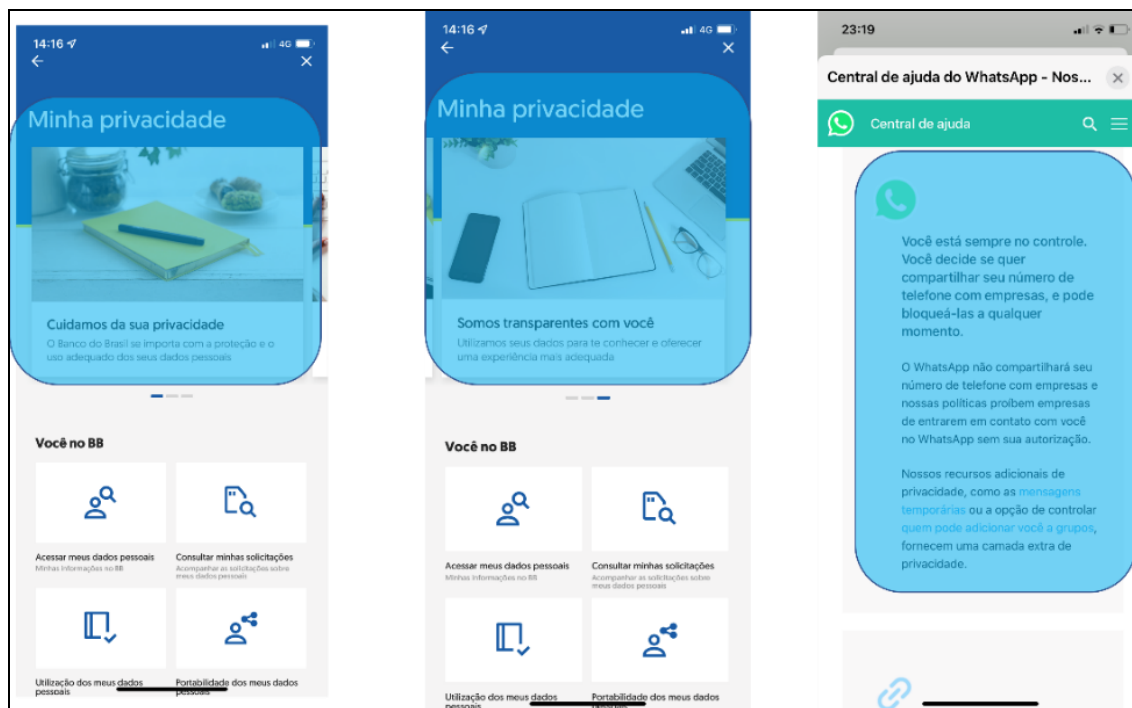
Identificamos nas interfaces conteúdos alarmantes de nosso *software* antivírus como: “estamos prontos para verificar a existência de cookies e rastreadores indesejados”, “Proteja suas informações pessoais”, “Bloqueamos uma conexão insegura”, “Salve seus arquivos. Feche todos os programas abertos e clique em ok para reiniciar e fazer uma varredura no computador”, alimentando um imaginário de tropa de defesa, que está em constante alerta para “cuidar” da proteção do usuário. Percebemos que declarações como essas, assim como os imaginários que emergem desses sentidos comunicados, são reflexo e também produtores do que acontece na constelação usuário vulnerável, pois expõe ao medo e desconfiança o usuário, criando uma situação de vulnerabilidade e, por isso, insegurança. Tal como o efeito que Lemos (2009) comenta sobre a presença das câmeras que encaramos em tantos momentos de nossas vidas, que vigiam de forma silenciosa e de maneira sutil, deixando o usuário com a sensação ubíqua de liberdade e monitoramento constante.

Paralelamente à construção de um ambiente seguro, há o discurso das plataformas em “zelar” pelo cuidado e bem-estar do usuário, criando a falsa sensação de que ele está no controle da coleta e uso dos dados, quando, na verdade, está sendo vigiado, conforme demonstra o conteúdo a seguir, capturado em aplicativo de sistema bancário para dispositivo móvel: “Minha privacidade. Cuidamos da sua privacidade. O Banco do Brasil se importa com a proteção e o uso adequado dos seus dados pessoais.” “Somos transparentes com você. Utilizamos seus dados para te conhecer e oferecer uma experiência mais adequada.”. Esse uso reforça o que dissecamos na constelação Confiança Programada, mais especificamente na coleção Guardião de Memórias no FB, onde são simulados amizade, senso de confiança e pertencimento à comunidade pelo discurso de melhoria de experiência do próprio usuário.

---

<sup>32</sup> “Intriguingly, in terms of sex crimes involving juveniles, the largest number of cases involving SNSs [social networking sites] was undercover operations in which investigators set up web pages and profiles in the course of portraying minors online.”

Figura 89 - Dissecação da coleção Medo e Vigilância

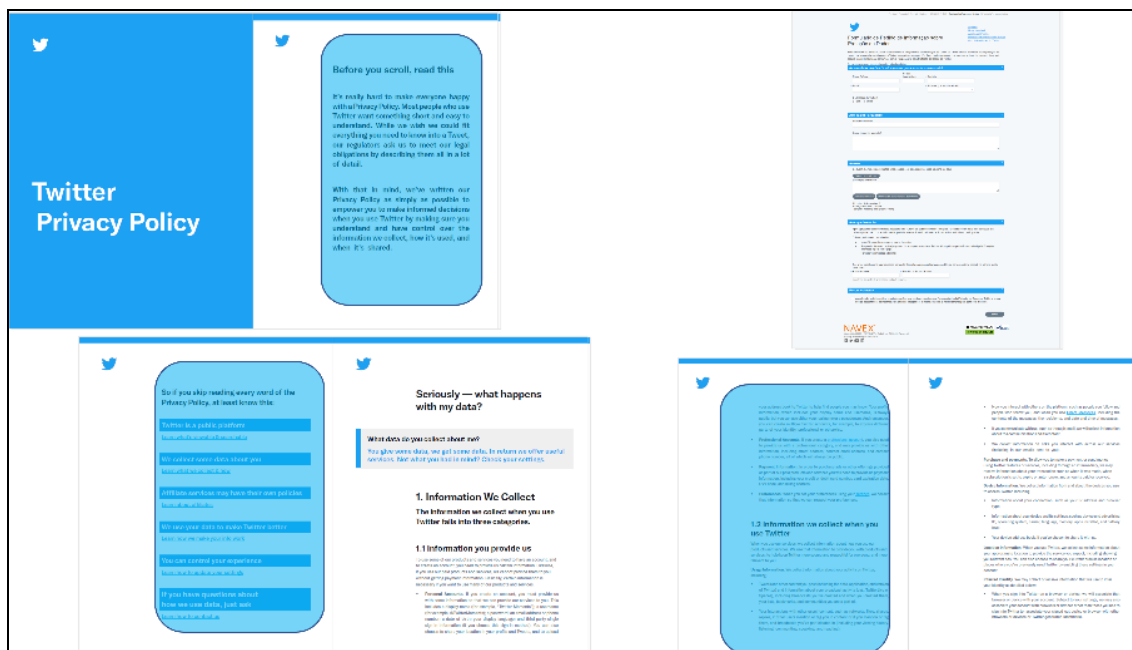


Fonte: Elaborado pela autora (2021).

Na dissecação da Figura 89, verificamos na mensagem que o aplicativo WhatsApp apresenta na seção que escavamos denominada por Central de ajuda do WhatsApp. O conteúdo indica: “Você está seguro e no controle. Você decide se quer compartilhar seu número de telefone com empresas, e pode bloqueá-las a qualquer momento”. De forma complementar, o Twitter publicou uma versão de sua Política de Privacidade mais concisa, sob o discurso de simplificar o entendimento do usuário, mas sempre criando a utopia de que o usuário pode acessar o que é coletado e que está em suas mãos a responsabilidade pelas informações.



Figura 90 - Coleção Medo e Vigilância



Fonte: Elaborado pela autora (2021).

Ou seja, a plataforma se esquia de assumir a incumbência de coletar, armazenar e compartilhar dados com parceiros, como anunciantes e provedores de serviços e afiliados, informando que “você pode controlar sua experiência”<sup>33</sup> (TWITTER, 2021, tradução nossa), a partir de uma linguagem que visa claramente reduzir a relevância do conteúdo, ao informar que

nós escrevemos nossas políticas de privacidade o mais simples possível para empoderar você para fazer decisões informadas quando você usa Twitter garantindo que você compreende e controla as informações que coletamos, como são usadas e quando são compartilhadas<sup>34</sup> (TWITTER, 2021).

Esses documentos, publicados pelo Twitter, estão em formato .pdf, contendo as políticas de privacidade dentro da plataforma, reforçam a *eticidade* políticas de pergaminho que dissecamos nas interfaces do FB, que justamente “atualizou” seus termos de uso, assumindo sua complexidade e falta de adequação à linguagem comum do usuário. Verificamos que essa espécie de postura de simular a concessão da administração do uso de dados, aos usuários da internet, é uma prática que segue em demais serviços na *web*, não apenas em plataformas de redes sociais gigantes, mas, em iniciativas como laboratórios de

<sup>33</sup> “You can control your experience.”

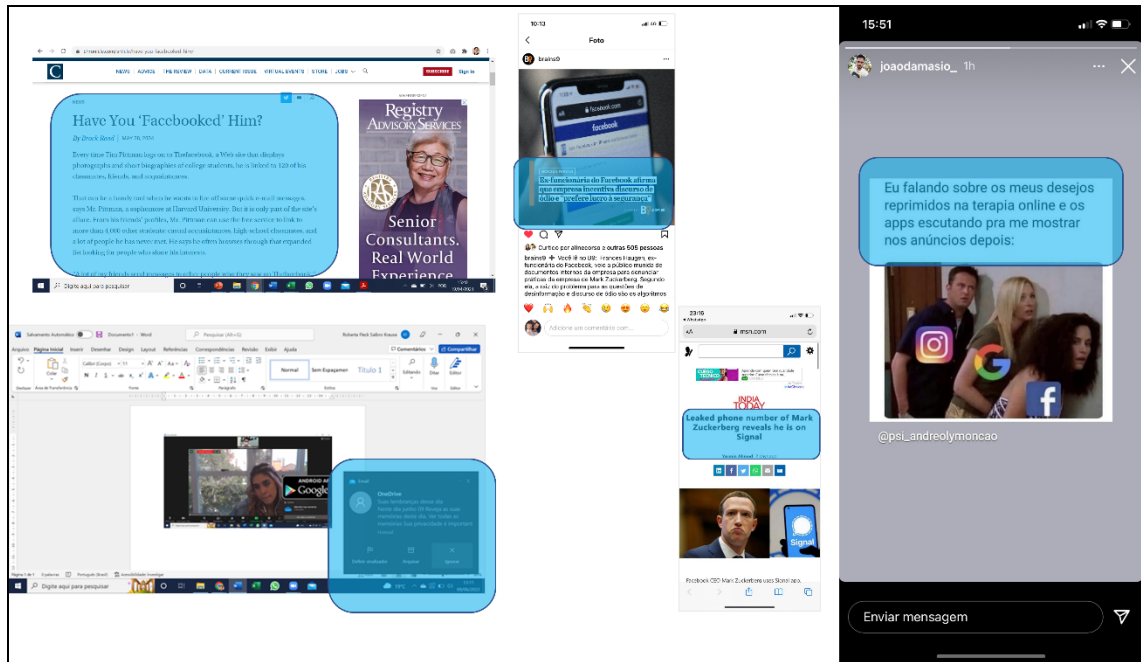
<sup>34</sup> “we’ve written our Privacy Policy as simply as possible to empower you to make informed decisions when you use Twitter by making sure you understand and have control over the information we collect, how it’s used, and when it’s shared.”



exames, serviços bancários, serviços de mensagens *online*, etc. Percebemos que as iniciativas estão alicerçadas em linguagem orientada para a compreensão a partir da LGPD, regras para o uso de *cookies* no navegador do usuário, novas regulamentações para publicidade segmentada concedendo ao usuário a opção por algumas preferências no impacto de mensagens comerciais. Porém, essas escolhas camufladas, sustentam o que Zuboff (2020, p. 65) designa como “domínio eminente privado”, caracterizando-se pela forma de posse unilateral e injusta de direitos sem o total consentimento do usuário, como “uma degradação moral e democrática do domínio da lei e da instituição do contrato, uma perversão que reestrutura os direitos dos usuários concedidos mediante processos democráticos [...]”.

De maneira complementar, para encerrarmos a coleção Medo e Vigilância, percebemos que o medo de ser exposto, de mau uso de dados e da constante vigilância ganharam, de vez, o espaço nas mídias, através de notícias (e muito alimentados pelos escândalos, do caso Snowden, Cambridge Analytica, etc...) e reforçam a produção e circulação de memes, piadas e curiosidades que estão centralizadas no tema do medo, segurança e vigilância a partir de dispositivos conectados à internet. Como a notícia que revela que, no mais recente episódio de vazamento de dados de 533 milhões de usuários do FB, o próprio Mark Zuckerberg foi vítima da divulgação indevida. Na publicação foi informado que ele mesmo não utiliza apenas os produtos da Meta para se comunicar, mas usa também o aplicativo Signal, que entre os concorrentes do WhatsApp, foi o precursor a utilizar criptografia nas mensagens de seus usuários.

Figura 91 - Dissecação da coleção Medo e Vigilância



Fonte: Elaborado pela autora (2021).

Para dar sequência à constelação *Ambiência da Tecnosegurança Contemporânea*, iremos apresentar, a seguir, a última coleção que produzimos em nossa tese a partir de nossas coletas de imagens. Denominada por *Serviços Autenticadores*, o grupo de interfaces carrega sentidos muito fortes em um tipo de “chave-mestre”, que abre portas pela *web* mas que, paralelamente, exige que o usuário esteja associado a uma conta, *login* ou serviço que nos parece muito com um “batismo digital”. Ou seja, se não recebeu a bênção de empresas “gigantes da tecnologia”, como FB, Google, Microsoft e outras, o usuário não recebe acesso ao direito de desfrutar de vários dos “benefícios” da internet.

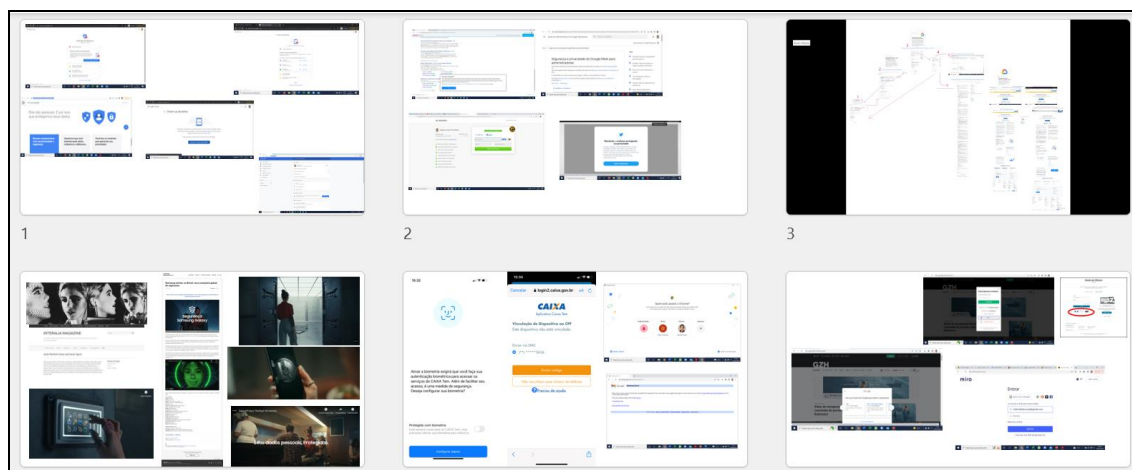
#### 4.4.2 Coleção Serviços Autenticadores

A coleção serviços autenticadores é composta por um conjunto de imagens capturadas ao longo do desenvolvimento de nossa *flâneria* pela *web* e por alguns movimentos de escavação, no sentido material, da atualidade (em termos bergsonianos) pelas interfaces que nos deparamos. Estamos chamando por serviços autenticadores a possibilidade dos *softwares* de legitimar determinado usuário na internet pela execução de algumas etapas que visam verificar sua identificação. Conforme citamos na introdução dessa tese, exercitamos a proposta em artigo apresentado na Intercom, que justamente visava perceber como os serviços de *login*, em plataformas como Google e FB, tinham o caráter de validação para entradas

“seguras” em serviços de terceiros, denominado como *login social*. Àquela época, verificamos como esses serviços são acompanhados de uma *imageria* associada à segurança, muito alicerçados em imaginários criados no ambiente *offline*, como cadeado, escudo e chaves.

Porém, percebemos que, além do uso desses recursos para demonstrar ou sinalizar que o conteúdo estaria protegido de uma aparente ameaça, vimos que o próprio serviço de adentrar outro ambiente que demanda identificação, a partir de um *sign wall*, como um jornal digital *online*, por exemplo, pode ser realizado por intermédio de um cadastro prévio no FB ou Google. É interessante realizarmos a comparação com essa maneira de reconhecimento do usuário legitimado pela confirmação de seu perfil, cadastrado previamente em uma rede social ou outro serviço, como *e-mail*, por exemplo. A seguir, demonstramos a coleção completa na Figura 92, que tem capturas de interfaces de serviços como Google, FB, bancários, jornais digitais e campanhas publicitárias e produção audiovisual.

Figura 92 - Coleção Serviços Autenticadores



Fonte: Elaborado pela autora (2021).

Figura 93 - Código QR para visualização da Coleção Serviços Autenticadores



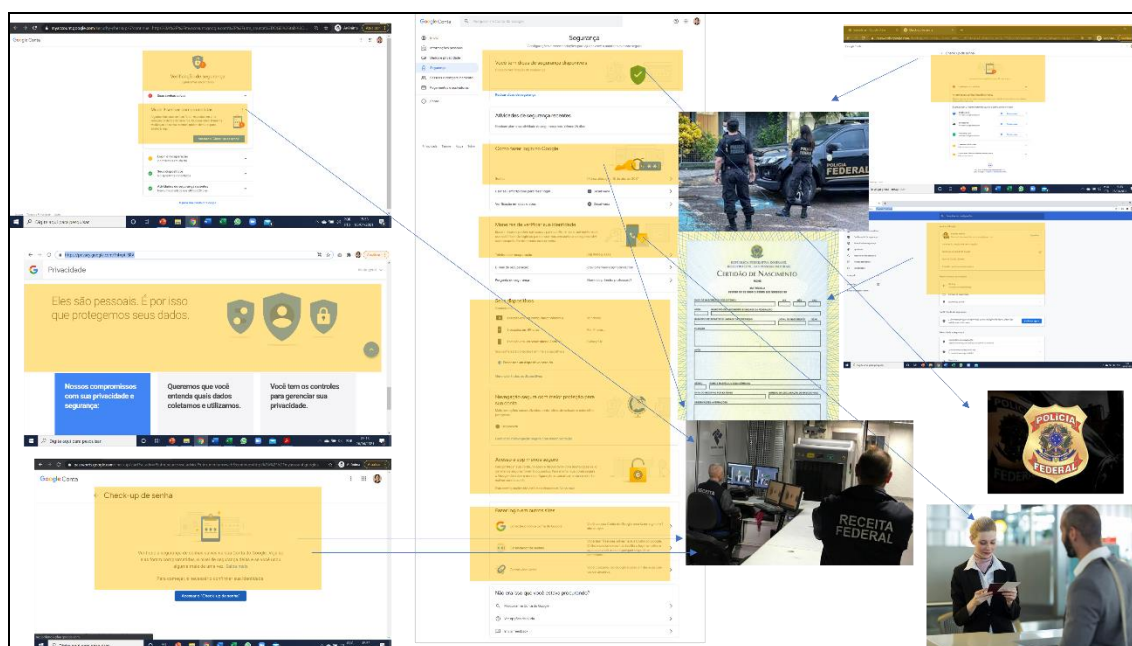
Fonte: Elaborado pela autora (2021).

Partimos para o exercício de dissecação dessas interfaces, que sinalizou as *ethicidades*, que são convocadas por imaginários construídos de serviços autenticadores, concedendo aos detentores das plataformas a função de verificador de identidades, algo como uma alfândega

entre as possíveis fronteiras geográficas desse ciberespaço. Fizemos a dissecação das imagens e mantivemos o movimento de dar a ver as associações com imaginários a partir dessas palavras-chave em buscadores. Operando sobre as capturas, percebemos que essas imagens que retiramos do fluxo da seção <https://myaccount.google.com/security>, por exemplo, apresentam uma série de informações sobre nosso histórico de navegação, preferências de *login*, e inúmeras configurações de privacidade dos dados, alicerçadas na *ethicidade* infantil, que sinalizamos na dissecação do FB. É claro o uso do recurso da ilustração, do desenho e das cores para construir um imaginário que reduz a seriedade da informação lá contida. O que as interfaces mostram como atualização de algo seguro e privado/dentro/íntimo estão alicerçadas em construtos como a infância, o cuidado, a comunidade – algo que vai além de recursos da *imageria*, da segurança comumente associada ao uso de chaves, escudos ou do que seria essa comunicação confidencial, conforme a coleção *tecnoinsegurança*.

Porém, quando associamos os termos como autenticação de identidade, verificação de Cadastro de Pessoa Física (CPF), alfândega ou registro de cidadão, nos deparamos com resultados de imagens bem distintas ao universo infantil. Conforme é possível verificarmos, na dissecação a seguir, os resultados que chegamos no buscador do Google são justamente associados a uma *imageria* séria, carregada de escudos e brasões que representam, na sociedade atual, instituições como Polícia Federal, Receita Federal e áreas profissionais públicas associadas ao controle e inspeção, como as barreiras alfandegárias:

Figura 94 - Dissecação dos Serviços Autenticadores



Fonte: Elaborado pela autora (2021).

Verificamos que na interface coletada do Google há a mensagem: “Eles são pessoais, por isso protegemos seus dados”, ora a empresa assume a postura de Guardião de Memórias, mas que, também, tem a pretensão e certa intransigência de informar que os dados só estarão seguros se foram “armazenados” com o Google. Essa construção de um espaço que pode arquivar informações faz parte do discurso das “novas” mídias, conforme sua promessa de guardar tudo, de acordo com Chun (2006), mas que auxilia a alimentar uma *imageria* de lugar que cuida, quando, na verdade, estão na completa fluidez da *web*, um espaço cheio de falhas, rupturas, páginas descontinuadas e *links* “quebrados”.

O ciberespaço perde o lugar, pois o lugar não é mais estável ou adequado. Os lugares desaparecem e/ou movem-se rapidamente; criadores/gerentes de páginas da Web geralmente movem ou apagam páginas da Web com pouca consideração por aqueles que as marcaram ou criaram links para elas, ou para os mecanismos de pesquisa que as indexaram. Notavelmente, dada essa incerteza, o baixo custo do armazenamento de dados e a prevalência do que Manovich chama de “complexo de banco de dados” - o desejo irracional de armazenar tudo - muitos são pegos de surpresa pelo desaparecimento de sites que poderiam facilmente ter armazenado em cache localmente. O uso metafórico do lugar nos cega para a fluidez da Web<sup>35</sup> (CHUN, 2006, p. 46, tradução nossa).

Compreendemos outra característica dessa construção verificadora dos serviços da *web* que está na conduta atribuída ao poder de controle. Bloquear e barrar possíveis conexões suspeitas tidas como identificáveis pelo Google, ou, até mesmo, o antivírus, ao informar que proporciona uma

Navegação segura com maior proteção para sua conta. Acesso a app menos seguro: para proteger sua conta, os apps e dispositivos com tecnologias de login menos seguras foram bloqueados. Para manter sua conta segura, o Google desativará essa configuração automaticamente se ela não estiver sendo usada (GOOGLE, 2021).

Esse autoritarismo praticado pelo controle do que o usuário recebe de informação ou encara como uma ameaça, reforça o sentido de Lógica Suspeita que identificamos nas interfaces do FB, mas, também, reflete a vigilância a partir de um monitoramento dos acessos e interações do usuário, mascarada através de escudos e serviços ditos “defensores”.

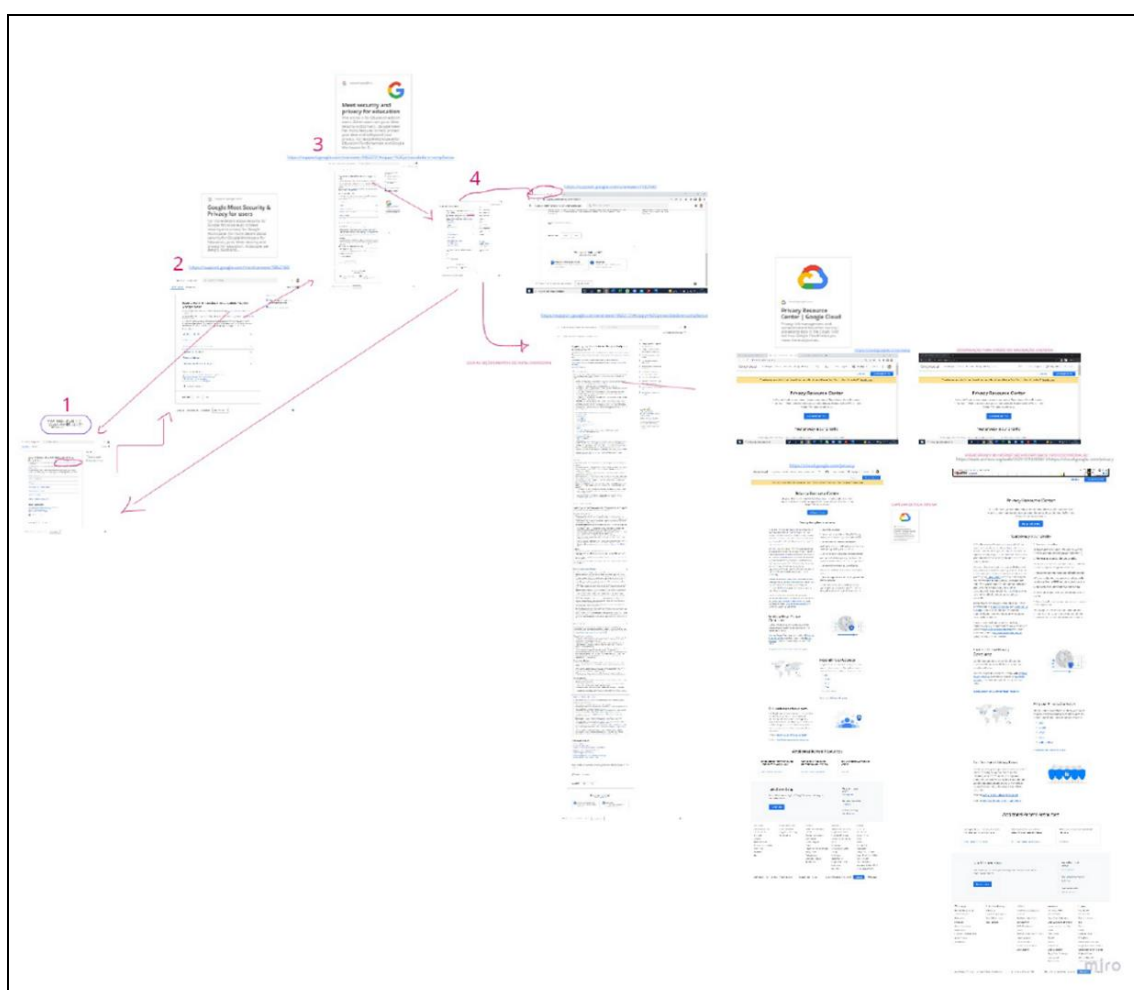
Com o intuito de tentar compreendermos esse movimento de “exército de defesa” no Google, escavamos a seção “Minha conta” que diz realizar um controle sobre a privacidade de

---

<sup>35</sup> “Cyberspace loosens place, for place is no longer stable or proper. Places disappear and/or move rapidly; creators/managers of Web pages often move or erase Web pages with little regard for those who have bookmarked or linked to them, or for search engines that have indexed them. Remarkably, given this uncertainty, the cheapness of data storage, and the prevalence of what Manovich calls ‘database complex’- the irrational desire to store everything-many are caught short by disappearing Web sites they could easily have cached locally. The metaphoric use of place blinds us to the Web’s fluidity.”

acessos reconhecidos pelo próprio serviço como suspeito. Mas, ficamos com a mesma sensação da coleção Políticas de Pergaminho, ou seja, caímos em vários becos sem saída, ou, muitas vezes, um retorno ao conteúdo clicado inicialmente, constituindo um grande labirinto para o usuário. Na Figura 95 tentamos demonstrar o percurso, na tentativa de mapear o processo, numerando as etapas conforme os *links* foram nos direcionando. Porém, nas diversas vezes que tentamos compreender a arquitetura de informação da seção, não tivemos sucesso, fomos voltando em *loop* para os mesmos espaços, sem “avançar” para os conteúdos indicados como o Privacy Resource Center do Google.

Figura 95 - Tentativa de mapear a seção Privacidade da conta do Google

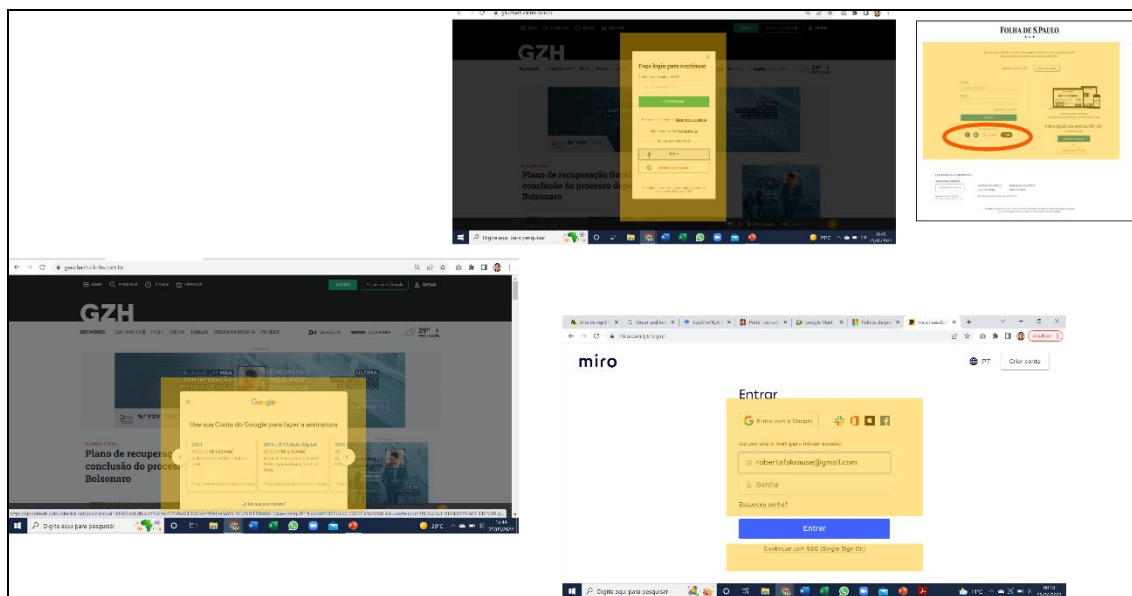


Fonte: Adaptado de Google (2021).

Percebemos que o Google, assim como o FB, apresenta a postura de um serviço que “abre caminhos”, a partir do *login* realizado previamente em suas interfaces, e que alimenta a utopia do acesso livre pelo ciberespaço, mas condicionando a seu “batismo” à liberdade e fluidez. Essa característica pode ser vista no arranjo de interfaces, a seguir, contendo capturas

de telas de notícias *online*, como o *Jornal ZH* e *Folha de São Paulo*, assim como outros serviços de edição de imagens e *design*, como o Miro.

Figura 96 - Dissecação coleção Serviços Autenticadores dos jornais *ZH* e *Folha de São Paulo* e do Miro



Fonte: Elaborado pela autora (2021).

No sentido de o FB ser um espaço que libera e autoriza o direito de “ir e vir” do usuário da internet, Zuboff (2020, p. 528) argumenta sobre a sua construção em também estar associado a essa postura de livre-arbítrio, um “lugar” onde seus usuários têm autonomia para se expressar:

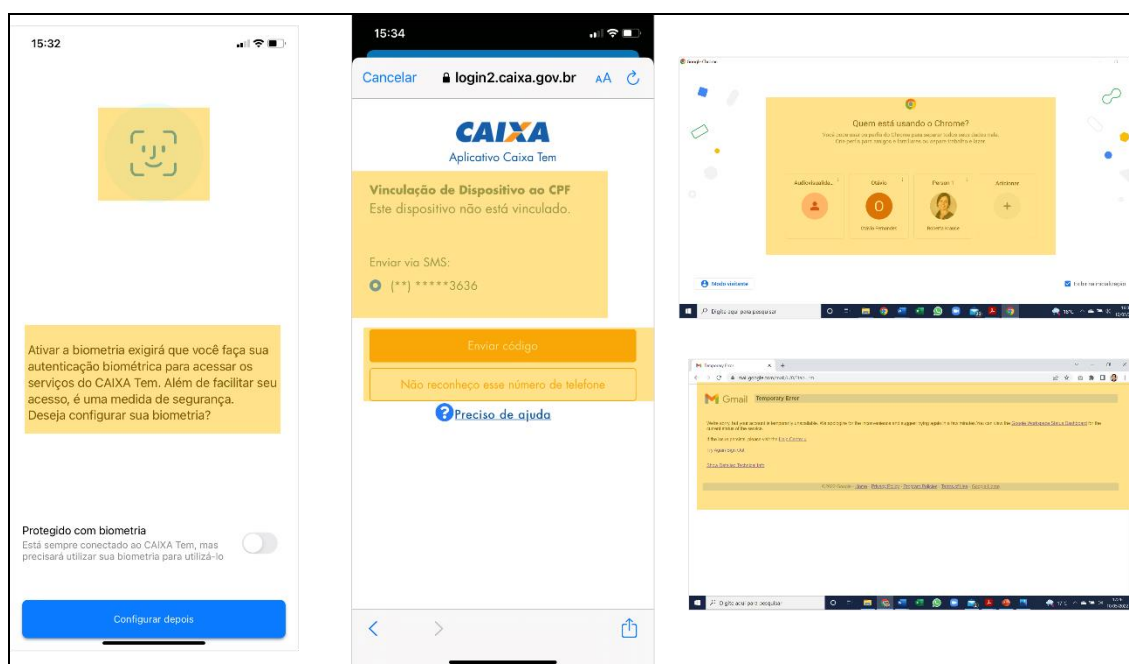
O Facebook veio ao mundo se desviando de antigas fronteiras institucionais oferecendo-nos liberdade para nos conectarmos e nos expressarmos à vontade. É impossível dizer o que a experiência do Facebook poderia ter sido se a companhia tivesse escolhido um caminho que não dependesse das receitas da vigilância. Em vez disso, confrontamos o subido acúmulo de um poder instrumentário que vira a nossa sociedade numa direção imprevista.

Apesar da condição de autenticar os usuários baseada em cadastros associando endereços de *e-mail*, senhas e códigos em contas de grandes empresas de tecnologia ser extremamente comum na *web*, a verificação do usuário também está largamente difundida pela possibilidade de realizar o sistema de reconhecimento facial, condição para acesso a alguma conta ou *software* condicionada à leitura dos traços físicos de um indivíduo, a partir da câmera que alimenta um *software* de inteligência artificial, identificando características do rosto e associando-o a determinada conta cadastrada no banco de dados. Conforme vimos ao longo do capítulo introdutório dessa tese, esse tema hoje é pauta para discussão em relação a



liberdade dos cidadãos, seja pelo uso através da justificativa da segurança pública, seja pelo viés de controle e monitoramento das pessoas em espaços privados, como conta bancária, por exemplo:

Figura 97 - Dissecção da coleção Serviços Autenticadores com biometria, reconhecimento facial e *login* social



Fonte: Elaborado pela autora (2021).

O arranjo de interfaces, acima, apresenta algumas imagens de nosso dispositivo móvel que propõe, em situações diversas, a entrada em algum serviço associada a um *login* cadastrado. Por exemplo, nossa conta bancária, nosso saldo no sistema de Fundo de Garantia por Tempo de Serviço (FGTS), nossa pesquisa na *web* a partir do Google Chrome, e, por fim, uma tentativa de acesso ao endereço de *e-mail* do Google que sinaliza um erro temporário ao compreender nossa falha intencional de senha ao tentarmos acessar a conta. Nas opções sinalizadas, percebemos que a admissão por esses portões de entrada da verificação da conta pode acontecer por algumas autenticações que comprovam que determinado usuário é o “proprietário” daquele *login*. Por exemplo, o reconhecimento facial ou *face ID*, conforme IA que realiza a leitura de nosso rosto e associa ao nosso cadastro realizado, informando que essa forma se trata de garantia maior para o proprietário dos dados da conta, ao dizer que: “ativar a biometria exigirá que faça sua autenticação biométrica para acessar os serviços da Caixa Tem. Além de facilitar seu acesso, é uma medida de segurança. Deseja configurar sua biometria?”.

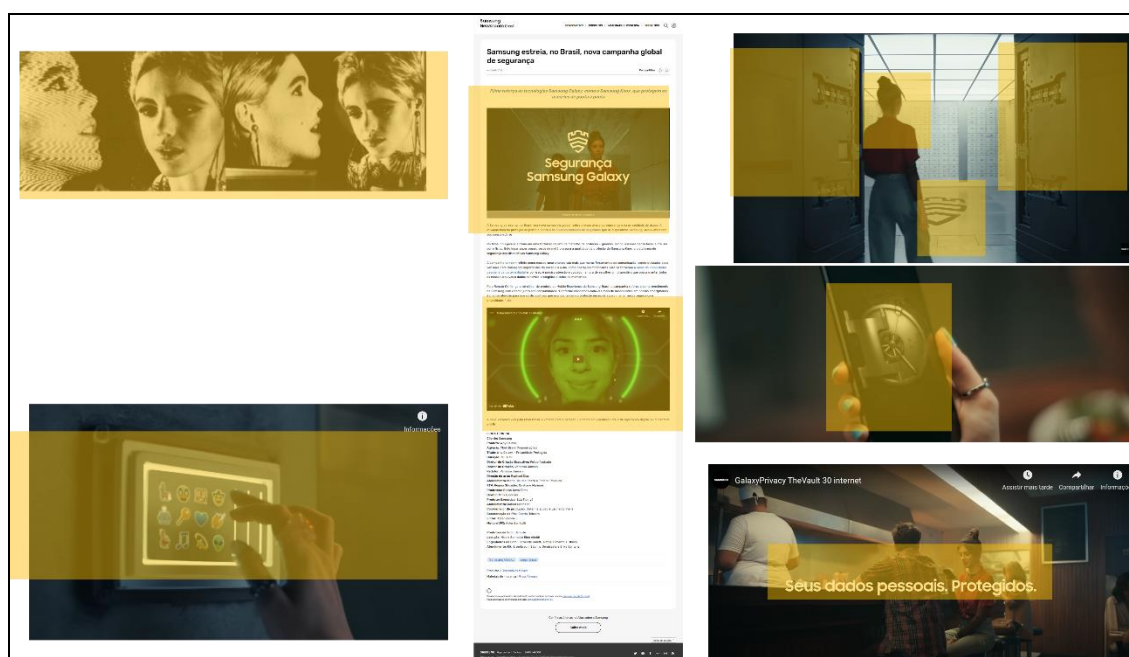
Para complementar esse tópico, Zuboff (2020) comenta sobre a gravidade do acúmulo de dados sobre os usuários, incluindo a biometria e todo histórico de interações, pesquisas e



interesses que demonstramos em “rastros” pela internet, que, em conjunto, acabam por produzir uma análise sobre o perfil emocional dos usuários. Compreendemos que essa construção reforça a *ethicidade* usuário vulnerável, pois alimenta o medo e a incerteza de não permitir a biometria sob risco de violação dos dados lá contidos. Reconhecemos que, justamente, os imaginários que emergem desse espaço, estimulam a *tecnoinsegurança* expondo o usuário na decisão de ceder seu rosto pagando o preço da suposta garantia de proteção da conta.

Para finalizarmos a dissecação das imagens da coleção, apresentamos, a seguir, o último arranjo que contém capturas de telas de duas iniciativas muito associadas às artes, como a produção audiovisual desenvolvida para a campanha publicitária da fabricante de eletroportáteis Samsung, lançada em julho de 2022 nos veículos de comunicação, assim como plataformas digitais no Brasil. E, a segunda iniciativa, trata-se da Vigilância a Arte, projeto que utiliza a tecnologia como forma de observação de indivíduos, e varia por instalações arquitetônicas e audiovisuais, usando como referência o curta-metragem *Outter and inner space*, de Andy Warhol, produzido em 1966. Inferimos tratar-se de uma outra forma de autenticar as pessoas a partir de imposição de controle e poder, algo demonstrado no filme, e que tem a atriz e modelo Edie Sedgwick, que está de frente para um aparelho de televisão que fica reproduzindo uma fita de vídeo pré-gravada dela mesma. “Na fita de vídeo, Edie está posicionada no lado esquerdo do quadro, voltada para a direita; ela está falando com uma pessoa invisível fora da tela à nossa direita.” (INTERALIA MAGAZINE, 2022), autenticando a “verdadeira” atriz e modelo pela reprodução espelhada de sua imagem capturada.

Figura 98 - Dissecação da coleção Serviços Autenticadores do filme *Outter and inner space* e da campanha publicitária da Samsung



Fonte: Elaborado pela autora (2021).

Já a campanha publicitária global, lançada pela fabricante Samsung no Brasil, que contou com veiculação no digital, tv conectada e *Out-Of-Home* (OOH), apresenta a relevância da pauta no imaginário social sobre aspectos associados à privacidade e segurança em dispositivos móveis.

No filme, dois jovens entram em uma fortaleza repleta de métodos de proteção – guardas, senha, escaneamento facial e até um cofre físico. Este lugar super seguro serve de metáfora para a qualidade de proteção do Samsung Knox, a plataforma de segurança dos dispositivos Samsung Galaxy (NEWS SAMSUNG, 2022).

Conforme demonstramos das capturas e na dissecação das imagens que compõem o arranjo, percebemos imaginários que carregam sentidos de *tecnosegurança* apoiados em *eticidades* que verificamos na constelação Confiança Programada, ou seja, o *software* assume a postura de defender, cuidar e proteger, ora salienta constantemente a luta por vigiar, abandonar e controlar os dados os usuários. É construída na campanha e nas imagens que intervimos uma forte dependência do recurso imagético de como a segurança poderia ser reproduzida pela imagem nos sentidos que recorremos na contemporaneidade.

Para Renato Citrini, gerente sênior de produto de Mobile Experience da Samsung Brasil, a campanha reforça o comprometimento da Samsung com o tema junto aos consumidores: “Conforme colocamos cada vez mais de nossas vidas em nossos smartphones, é preciso atenção para que os dispositivos que usamos tenham a

proteção necessária para manter nossa segurança e privacidade.” – diz (NEWS SAMSUNG, 2022).

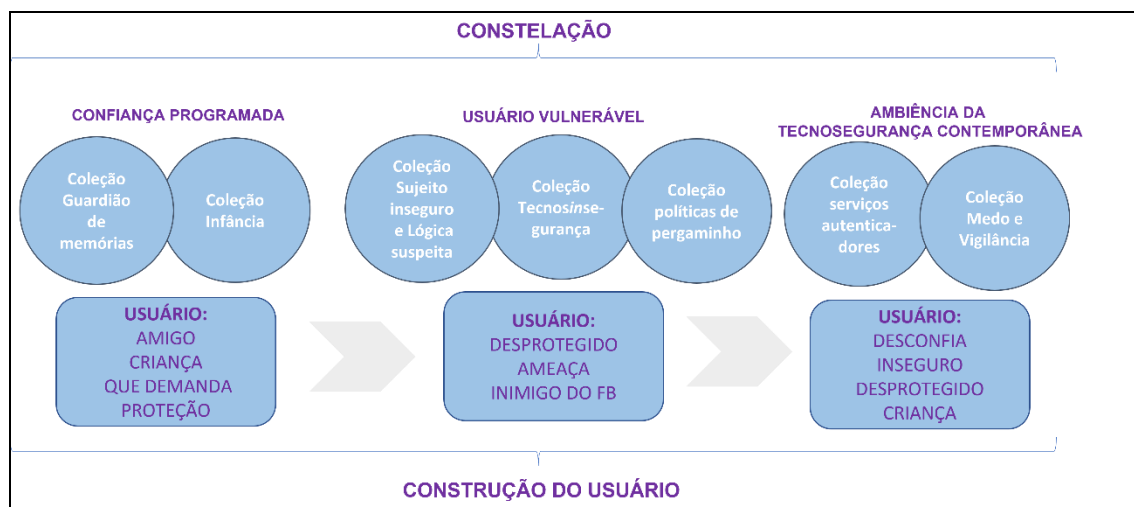
Verificamos que há sentidos sendo produzidos de Sujeito Inseguro e Lógica Suspeita, assim como alimenta a construção de *tecnoinsegurança* social que emerge e é fruto de nossa cultura que estimula a desconfiança nos usuários, pois há a construção extremamente forte em cima do cadeado, das chaves, das senhas (que na campanha é simulada por uma combinação de *emojis* e não pela sequência numérica ou alfabética da personagem). Por fim, percebe-se que há imaginários da confiança programada quando o *software* propõe que a única opção segura para o usuário é confiar, acaba residindo no dispositivo móvel.<sup>36</sup>

Ao longo de nosso exercício de análise apresentado no presente capítulo, verificamos os territórios de identificação que dão a ver imaginários que identificamos como associados a construção da *tecnosegurança* contemporânea. Em um movimento que atravessa aspectos estritamente relacionados à privacidade, proteção, cuidado, segurança de dados, confiança, vigilância, monitoramento e controle. Durante o processo de “sujar as mãos” com as imagens, durante a intervenção cirúrgica da dissecação das interfaces, aliado ao ato de organizar as coleções que dão origem às três constelações, fomos percebendo muita força em um perfil multifacetado do usuário que percorre essa ambiência. Conforme cada uma das constelações que mapeamos, entendemos que poderíamos inferir três “personas” distintas do usuário, a partir dos sentidos que emergem no FB, pois, em determinadas constelações, ele é encarado como frágil que precisa de cuidado, e, em outro momento, ele é construído como um suposto inimigo, no qual o próprio FB precisa criar muros virtuais para se proteger em termos e políticas, e, também, compreendemos que há o usuário amigo, que faz parte da comunidade e deve ser abraçado virtualmente em um parque de diversões:

---

<sup>36</sup> Para que o(a) leitor(a) tenha conhecimento da produção, sugerimos acessar o *link*, a seguir, para assistir ao conteúdo: <https://news.samsung.com/br/samsung-estreia-no-brasil-nova-campanha-global-de-seguranca>.

Figura 99 - Perfis do usuário multifacetado percebidos no mapeamento das constelações



Fonte: Elaborado pela autora (2021).

Por exemplo, a partir da constelação Confiança Programada, percebemos que, na coleção Guardiã de Memórias e coleção Infância, o usuário é compreendido como uma criança, que brinca e se entretém com objetos coloridos e construções divertidas. Como assuntos “negativos” não fazem parte dessa *ethicidade* infantil, então, a melancolia e a tristeza não têm vez nesse espaço. Ou seja, o usuário é cuidado e zelado pelo senso protetor que o FB propõe ao distraí-los da seriedade de suas vidas, numa espécie de escapismo da realidade. Além disso, verificamos *ethicidades* na coleção Guardiã de Memórias, e que imaginários são constantemente tensionados por um papel de Guardiã, na postura que protege e acolhe o usuário.

Já na segunda constelação, vimos que, justamente pela vulnerabilidade que se expõe o usuário, ele se encontra desprotegido. As *ethicidades* que dão a ver sentidos de medo, suspeita e desconfiança colocam o usuário nessa posição. O FB o abandona e encara como possível ameaça à sua comunidade obediente sob os termos de uso. Pelas *ethicidades* atualizadas em diferentes molduras de segredo, e uma paranoia de lógica suspeita ao agir em anonimato, percebemos que há *tecnoinsegurança* construída. Além disso, a judicialização emoldurada pelas políticas de pergaminho enunciam sentidos identitários de legislação e proteção do FB ao se posicionar em constante defesa atrás de suas muralhas encobertas por termos de uso.

Por fim, na terceira constelação, vimos que a ambiência da *tecnosegurança* contemporânea, atualiza diversas personas já identificadas nas constelações anteriores, mas também cria e retroalimenta a cultura da *tecnosegurança* no FB e do FB. Ou seja, percebemos que diversos imaginários acabam por comunicar *ethicidades* que já identificamos nas interfaces no FB, mas que, também, são resultado de toda ambiência na qual ele mesmo faz

parte. Portanto, ora são perfis de usuário encarados como amigo, criança, ora é um usuário que está desconfiando do FB, que pode ser uma possível ameaça à plataforma e à lógica de comunidade que é reforçada pelo FB.

De forma complementar, nossa exploração do objeto, através da dissecação, demonstra que os imaginários reconvocados nas interfaces possibilitam sentidos que constroem a *tecnosegurança* contemporânea, pelas *ethicidades* alicerçadas no uso da *imageria* da segurança tradicional, como chaves e cadeados, mas algo acontece no fundo, apoiado pelo sentido do acolhimento da tecnologia, da vulnerabilidade e do medo do usuário, pela desconfiança e constante vigilância que promove poder e paranoia, pela liberdade, metrificação e a dicotomia entre tornar algo público ou mantê-lo no privado.

## 5 CONSIDERAÇÕES FINAIS

Essa tese buscou responder ao questionamento de como são construídos sentidos durante de *tecnosegurança* pela ambiência Facebook. Para dar conta da construção do problema traçado, foram definidos três objetivos específicos que auxiliaram o desenvolvimento do trabalho, a partir de uma reflexão alicerçada no método da intuição de Bergson (2006), e pelas contribuições deleuzianas (1999) sobre a construção da problematização em relação ao objeto. Julgamos essencial trazermos a contribuição destes autores nessa consideração final sobre o trabalho desenvolvido, pois a forma de refletirmos sobre o próprio tema da pesquisa, sua materialidade e modo de operarmos sobre a empiria selecionada, foi extremamente contagiada pela perspectiva da qualidade durante da virtualidade das coisas, sendo o bergsonismo a base crucial de reflexão sobre tempo que atravessa toda a tese.

Ao termos como objeto da pesquisa as atualizações de *tecnosegurança* pelas interfaces do Facebook, o objetivo geral pretendeu compreender como são construídos sentidos durante de *tecnosegurança* pela ambiência Facebook, numa articulação que deu sustentação para objetivos específicos, que buscaram articular discussões relacionadas à privacidade e à segurança na cultura digital, bem como, à perspectiva das audiovisualidades da tecnocultura; formular o conceito de “*tecnosegurança*” enquanto sintoma da *tecnocultura* contemporânea, que se espalha através e para além das mídias, produzindo ambiência; e, por fim, autenticar sentidos de segurança e de privacidade enunciados pelas interfaces do Facebook.

Conforme comentamos na abertura dessa tese, a relação entre a pesquisadora e o trabalho desenvolvido é extremamente indissociável, pois os aspectos trazidos até aqui, na discussão do tema que nos desconcerta, são resultado de um constante debate teórico que vem sendo feito desde o ingresso no mestrado na UNISINOS, em 2014, no caráter laboratorial produzido nas reuniões do Grupo TCAv e nas realizações do LAR e no conteúdo produzido pelo LabMem. Além disso, nossa sensibilidade para o tema, que emergiu de maneira mais clara ao longo do doutoramento, foi, de certa maneira, fluindo conforme fomos avançando nossa capacidade de tensionamento sobre um olhar crítico ao nosso redor e às mídias. Nesse sentido, entendemos se o(a) leitor(a) pensar ser contraditório desenvolver uma tese sobre segurança estando em um mundo cada vez mais *inseguro*, nós acreditamos ser uma escolha estimulante, foi justamente pelo protagonismo do tema o que nos direcionou o olhar para a investigação pelas audiovisualidades da *tecnocultura*.

Porém, assim como fomos percebendo uma espécie de preocupação do imaginário coletivo associada ao assunto, a proposta da *tecnosegurança* foi emergindo ao compreendermos que diversos aspectos compõem essa discussão, conforme demonstramos na introdução dessa tese, a partir do encontro com as mídias, interfaces e *softwares* que alertam sobre estarmos constantemente protegidos. Portanto, percebemos que a segurança vem tomando uma centralidade na *tecnocultura* contemporânea, mas, ao mesmo tempo, é desconstruída por escândalos envolvendo plataformas, governos e iniciativas privadas que alimentam um cenário de *insegurança* e vulnerabilidade. Verificamos, ao longo do trabalho, que essa discussão acerca da dimensão da segurança está enraizada no mundo *cyber* e na softwarização da cultura, que acompanha desde o nascimento da internet comercial, nos anos 1990, quando aspectos como anonimato e liberdade surgem como uma promessa que se perdeu na atmosfera com a ilusão do ciberespaço.

Outro aspecto essencial ao *boom* da segurança na *tecnocultura* atual, reside no fato de estarmos constantemente conectados em dispositivos e mídias locativas que, em sua essência, são colecionadores de dados associados à nossa performance *online*, assim como informações sobre nossos corpos, faces e expressões a partir de um sistema de IA, como reconhecimento facial e biometria. Essa quantidade gigantesca de informação coletada sobre os indivíduos, que excedem o campo da internet ou da conexão *online*, como câmeras de vigilância urbana, por exemplo, alimentam um sistema que se beneficia sobre a temática da segurança de dados e sobre uma paranoia instaurada lucrativamente pelo poder, ou seja, quanto mais senhas, códigos, cadeados e *logins* criados pela indústria da tecnologia, pela busca em “estar seguro”, mais se estimula a pauta pela promessa da proteção. Nesse sentido, essa tese propõe o conceito de *tecnosegurança* como um sintoma da *tecnocultura* atual, que se espalha por entre as mídias e que as transcende, estabelecendo uma ambiência que apresenta uma característica dinâmica, e provocada, constantemente, pelo imbricamento conjunto de práticas sociais que influenciam o uso da técnica em nossa cultura.

Percebemos, ao longo da pesquisa, que os sentidos de *tecnosegurança* nas mídias se fazem presente em campanhas publicitárias, em sistemas de pagamentos bancários, sempre acompanhados de uma *imageria* associada ao tema da privacidade e do anonimato. Debates que os construtos *tecnoculturais* de segurança e privacidade comparecem nas mídias desde o conceito proposto para o sistema de capitalismo de vigilância até a formulação da LGPD, sigilo, anonimato e ao conceito de *privacy by design*, por exemplo. Paralelamente, dá oportunidade para diversas iniciativas privadas e não governamentais que surgem, justamente, pela demanda da temática em nossa cultura, assim como a DPB e várias *privacy*

*techs*, até produções de entretenimento audiovisuais, cinematográficas, midiáticas e artísticas dedicadas ao assunto.

Portanto, de forma complementar a toda essa discussão produzida nessa tese, nossa empiria, que foi coletada desde o ingresso no doutorado até o encerramento dessa pesquisa, carrega esses aspectos que foram tomando sentido a partir da metodologia utilizada. Chamamos por itinerário metodológico um movimento que conta com iniciativas que foram essenciais pela demanda de compreendermos o objeto e explorarmos a empiria, dando a ver caminhos que flertam com nosso questionamento de pesquisa, ou seja, tensionam aspectos que deram origem ao mapa de nossas constelações. A “fotografia” da *tecnosegurança* caracterizada como um sintoma da tecnocultura, possui *ethicidades* que foram percebidas nas interfaces do FB, mas não restrito a ele, ou seja, há um espalhamento além das mídias, estabelecendo o que chamamos por ambiência.

O desdobramento da cartografia teve como inspiração o movimento do *flâneur*, dando a ver coleções criadas a partir de afinidades eletivas que emergem de nossa observação, indicando que o objeto assume duas ordens: a da materialidade, referente ao percurso pela plataforma e interfaces paralelas, e da ordem das virtualidades, ou as *ethicidades* e os imaginários que emergem, a partir dos emolduramentos agenciados, originando a proposta para as constelações mapeadas. Nesse sentido, assumimos, claramente, que a imagem é protagonista nessa tese, como a materialidade que contém atualizações em seu devir, como portadora de memória, assim como comentamos previamente nessas considerações, o método intuitivo é estruturante na pesquisa.

Na primeira constelação, intitulada por Confiança Programada, organizamos duas coleções de interfaces coletadas no FB, sendo elas, Guardião de Memórias e Infância. Nesses agrupamentos, identificamos a construção de *ethicidades*, a partir da metodologia das molduras, e pela indicação em intervir nas materialidades pelo ato da dissecação, como subjetividades virtuais. Identificamos, também, imaginários que comunicam sentidos de confiança com o usuário, passando pelo alicerce de um espaço de aconchego, conforto e cuidado, apoiados na prerrogativa de fazer parte de uma comunidade segura. Além disso, percebemos que as *ethicidades*, agenciadas por imaginários construídos nessas interfaces, atualizam-se em diferentes molduras, como a construção constante de lembranças felizes, memórias e nostalgia, assim como um universo infantil, colorido e divertido. A *ethicidade* que reconvoca infância, em diversas seções dentro do FB, se estende pela sua Central de Segurança que, também, recorre a recursos da *imageria* da segurança tradicional, tais como



chaves ou fechaduras, mas cria pelo acolhimento, aconchego e sensação de conforto, aspectos associados à proteção do usuário nesse ambiente.

A segunda constelação, Usuário Vulnerável, é composta por três coleções de imagens das interfaces do FB que estimulam uma construção de tensão com o usuário, como Sujeito inseguro e Lógica Suspeita, *Tecnoinsegurança* e Políticas de Pergaminho. Autenticamos algumas *ethicidades* que se atualizam em molduras e moldurações de significação associadas aos imaginários que comunicam sentidos de vigilância, como um modo de ser na contemporaneidade, junto ao medo e ao anonimato. De forma complementar, na coleção *Tecnoinsegurança*, entendemos uma mudança de postura da plataforma ao “zelar” pela proteção, no FB, que acontece pelas molduras e moldurações, pela *imageria* da comunicação “segura”, pelos cadeados, chaves, escudos e conteúdos explicitamente dedicados a contar como aquele espaço se caracteriza por uma comunidade protegida. Já na coleção Políticas de Pergaminho, identificamos a defesa associada a uma judicialização, termos de consentimento e políticas que alertam o usuário para os riscos da plataforma. Porém, fomos compreendendo que estes são recursos de defesa do próprio FB e não do usuário.

E, na última constelação, Ambiência da *Tecnosegurança* Contemporânea, agrupamos capturas de interfaces de iniciativas paralelas ao FB, que entendemos como construções culturais que auxiliam a produzir, e são reflexo da *tecnosegurança* que convive na relação com as tecnologias digitais. Como os serviços autenticadores, que funcionam como uma espécie de “bênção” digital, possibilitando acessos por diversas páginas e serviços *online*, certificados por um registro prévio em contas como Google e FB, ou o uso da IA como garantia de *login* em sistema bancário, pelo reconhecimento facial ou biométrico da conta cadastrada, assumindo a função de verificador de identidades entre as fronteiras das interfaces.

Ao encerrarmos nossas constelações, entendemos como parte da contribuição da pesquisa uma identificação da construção de um perfil multifacetado do usuário que percorre essa ambiência conforme a *ethicidade* circunstanciada pela interface. O lugar de fala do FB e do usuário vão sendo alterados, de acordo com as constelações, passando por “personas” distintas. Por vezes, o usuário é cuidado e zelado pelo senso protetor que o FB propõe como sendo um guardião de carinho e memórias, mas, outras interfaces do FB o expõem ao “abandono” e, por isso, ele se torna vulnerável e é construído como uma possível ameaça à sua comunidade obediente sob os termos de uso e paredes virtuais das políticas de privacidade e segurança. Pelas *ethicidades* atualizadas em diferentes molduras de segredo, e uma paranoia que preconiza o anonimato, percebemos uma *tecnoinsegurança* emergindo nesses ambientes.

Contudo, se desenvolvermos uma tese, sobre um tema que nos desconcerta tanto, carrega aspectos estimulantes, também traz muitos pontos desafiadores, visto que fomos percebendo diversas iniciativas em muitas interfaces, e, nosso hábito de coletar essas manifestações se estende à escrita dessa tese. Ou seja, tivemos dificuldade em “recortar” e limitar o que teria potencialidade de tensionamento para o objetivo da pesquisa, pois selecionarmos as coleções foi um exercício metodológico que nos demandou escolhas e algumas renúncias, conforme a demanda do objeto, assim como constantes questionamentos e incertezas.

Ainda, no aspecto metodológico, tivemos dificuldade em compreender se a proposta da arqueologia da mídia, especificamente, no movimento do agir arqueológico sobre as interfaces, seria a angulação para operar as materialidades. Porém, ao realizarmos o ato de escavarmos as interfaces e irmos em busca de aspectos específicos que tratavam de pontos, conforme o objeto chamava nossa reflexão, compreendemos que a posterior dissecação fez com que fossemos percebendo sentidos comunicados por imaginários que emergiam nas interfaces, e, nesse aspecto, a metodologia das molduras define-se pela demanda do próprio objeto de pesquisa. Porém, assumimos que uma possível fragilidade dessa tese seja certa tendência em trabalharmos com uma proposta arqueológica, já que se trata de um interesse muito forte da autora. Paralelo ao que foi desenvolvido no trabalho, nossas produções acadêmicas e leituras complementares à pesquisa desenvolvida, articulam perspectivas de autores que flertam com essa visão sobre as mídias, então percebemos esse aspecto como ponto de atenção.

Como sugestão de extensão de nossa investigação, pensamos que a proposta desenvolvida sobre o conceito de *tecnosegurança* se expande para outros objetos midiáticos, como tivemos o objetivo de demonstrar em nossas constelações. Por exemplo, enquanto escrevíamos as considerações finais dessa tese, fomos impactados por, pelos menos, duas campanhas publicitárias, uma do Itaú e outra da Meta, com os temas privacidade e proteção sendo centrais na estratégia comunicacional de suas marcas. Ou seja, temos convicção de que a *tecnosegurança* é um sintoma contemporâneo que ultrapassa o estudo de interfaces do FB, como o nosso trabalho demonstrou. Nesse sentido, ficamos interessados em explorarmos, pela perspectiva da arqueologia da mídia, como os sentidos de *tecnosegurança* podem ser percebidos por movimentos de escavação em materialidades, como sistemas operacionais que já foram descartados pela “atualização” dos dispositivos, ou por mídias que caíram em “desuso” pela lógica evolucionista do mercado e da indústria tecnológica, talvez, buscando idealmente refletirmos sobre a genealogia da *tecnosegurança* contemporânea.

Por fim, compreendemos que o FB é um complexo objeto de molduras, *ethicidades* e moldurações que carregam sentidos, dando a ver imaginários do próprio FB, mas não apenas restrito a ele, mas como sintoma da cultura digital contemporânea, a qual ele faz parte constituinte e retroalimenta para permanecer operando, alicerçado em sentidos identitários próprios da *tecnosegurança*. São nesses construtos que se atualizam em virtualidades que compõem uma complexa arquitetura, que o FB reconvoca, constantemente, memórias a partir das imagens de interface criteriosamente desenvolvidas para construir confiança por meio de uma promessa dicotômica entre liberdade e controle.

## REFERÊNCIAS

A AMEAÇA global da China aos direitos humanos. *In*: HUMAN Rights Watch. *S. l.*, 5 jun. 2019. HRW, 2020. Disponível em: <https://www.hrw.org/pt/world-report/2020/country-chapters/337324>. Acesso em: 5 abr. 2021.

A POTENTIAL Privacy Model for the Web. *In*: MICHAELKLEBER. [*S. l.*], 13 fev. 2021. Disponível em: <https://github.com/michaelkleber/privacy-model>. Acesso em: 2 ago. 2022.

ABREU, T.; PELLEGRINI, P. Fake news: o caso Marielle e a manipulação midiática. *In*: CONGRESSO DE CIÊNCIAS DA COMUNICAÇÃO NA REGIÃO NORDESTE, 20, 2018, Juazeiro. *Anais [...]*. Juazeiro: Universidade do Estado da Bahia (UNEB), 2018. Disponível em: <http://portalintercom.org.br/anais/nordeste2018/resumos/R62-0970-1.pdf>. Acesso em: 10 nov. 2018.

ACADEMIA.EDU. Disponível em: <https://www.academia.edu/>. Acesso em: 5 abr. 2021.

ALBUQUERQUE, Luciana Santos Guilhon; PEDRO, Rosa Maria Leite Ribeiro. Facebook como dispositivo de vigilância e visibilidade: algumas controvérsias em questão. **Revista Tecnologia e Sociedade**, Curitiba, v. 9, n. 18, p. 1-14, 2013. Disponível em: <https://www.redalyc.org/pdf/4966/496650340009.pdf>. Acesso em: 26 set. 2020.

ANGWIN, Julia; SINGER-VINE, Jeremy. Selling you on Facebook. **The Wall Street Journal**, [*s. l.*], p. 1-3, April 2012. Disponível em: <https://www.wsj.com/articles/SB10001424052702303302504577327744009046230>. Acesso em: 19 jul. 2021.

ARANTES, Priscila. **Arte e mídia**: perspectivas da estética digital. São Paulo: Senac, 2012.

ASSUMPÇÃO, Fabrício; SANTANA, Ricardo; SANTOS, Plácida. Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais. **Em Questão**, Porto Alegre, v. 21, n. 2, p. 31-48, maio/ago. 2015. Disponível em: <https://seer.ufrgs.br/EmQuestao/article/view/54545>. Acesso em: 2 abr. 2020.

BARBOSA, Flávia. Nos passos de Bush. *O Globo - Mundo*, Rio de Janeiro, p. 31, 7 jun. 2013. *In*: ALBUQUERQUE, Luciana Santos Guilhon; PEDRO, Rosa Maria Leite Ribeiro. **Facebook como dispositivo de vigilância e visibilidade**: algumas controvérsias em questão. Disponível em: <https://www.redalyc.org/pdf/4966/496650340009.pdf>. Acesso em: 7 mar. 2021.

BAUMAN, Zygmunt. **44 cartas do mundo líquido moderno**. Rio de Janeiro: Jorge Zahar Editores, 2011.

BAUMAN, Zygmunt. **Comunidade**: a busca por segurança no mundo atual. Rio de Janeiro: Zahar Editores, 2003.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Jorge Zahar Editores, 2001.

BENJAMIN, Walter. **A obra de arte na era de sua reprodutibilidade técnica**. 1. ed. Porto Alegre: L&PM, 2013.

BENJAMIN, Walter. **Baudelaire e a modernidade**. Edição e tradução de João Barrento. 1. ed. Belo Horizonte: Autêntica, 2015. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788582175859/>. Acesso em: 7 jul. 2022.

BENJAMIN, Walter. **Origem do drama barroco alemão**. Tradução, prefácio e notas de Sérgio Paulo Rouanet. São Paulo: Brasiliense, 1984.

BENJAMIN, Walter. **Passagens**. Tradução de Irene Aron. Belo Horizonte: Editora da UFMG, 2006.

BENJAMIN, Benjamin. **Passagens**. BOLLE, Willi (org.). Tradução de Irene Aron. Belo Horizonte: Editora UFMG, 2018.

BERGSON, Henri. **Duração e simultaneidade**. São Paulo: Martins Fontes, 2006b.

BERGSON, Henri. **Memória e vida**. Tradução de Claudia Berliner. São Paulo: Martins Fontes, 2006a.

BERGSON, Henri. **O pensamento e o movente: ensaios e conferências**. São Paulo: Martins Fontes, 2006c.

BLACK Mirror. Criação: Charlie Brooker. Direção: Dan Trachtenberg, Jakob Verbruggen, James Hawes. [S. l.]: Netflix, 2016. Disponível em: <https://www.netflix.com/br/title/70264888>. Acesso em: 26 abr. 2021

BOLIN, Göran. Surveillance through media, by media, in media. **Northern Lights**, Intellect Ltd Editorial, [s. l.], v. 16, p. 3-21, 2018. Disponível em: <https://www.academia.edu/36872207/Surveillance>. Acesso em: 18 nov. 2020.

BOLIN, Göran; JERSLEV, Anne. In: BOLIN, Göran. Surveillance through media, by media, in media. **Northern Lights**, Intellect Ltd Editorial, [s. l.], v. 16, p. 3-21, 2018. Disponível em: <https://www.academia.edu/36872207/Surveillance>. Acesso em: 18 nov. 2020.

BOLTER, Jay Davis; GRUSIN, Richard. **Remediation: understanding new media**. Cambridge: The MIT Press, 1999.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 19 jul. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Brasília, DF: Presidência da República, 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: 3 abr. 2021.

BRIGHT, Richard. Andy Warhol's outer and inner space. **Interalia Magazine**, [s. l.], 2022. Disponível em: <https://www.interaliomag.org/blog/andy-warhols-outer-and-inner-space/#:~:text=Outer%20and%20Inner%20Space%20is,off%2Dscreen%20to%20our%20right>. Acesso em: 7 jul. 2022.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **Revista Famecos**: mídia, cultura e tecnologia [em linha], Porto Alegre, v. 36, p. 10-16, 2008. Disponível em: <https://www.redalyc.org/articulo.oa?id=495550192002>. Acesso em: 20 jul. 2020.

BRUNO, Fernanda. Rastros digitais sob a perspectiva da teoria do ator-rede. **Revista Famecos**, Porto Alegre, v. 19, n. 3, p. 681-704, 2012. Disponível em: <https://revistaseletronicas.pucrs.br/index.php/revistafamecos/article/view/12893/8601>. Acesso em: 23 jul. 2021.

BRUNO, Fernanda; PEDRO, Rosa. Entre aparecer e ser: tecnologia, espetáculo e subjetividade contemporânea. **Intexto**, Porto Alegre, UFRGS, v. 2, n. 11, p. 1-16, jul./dez. 2004. Disponível em: <https://seer.ufrgs.br/intexto/article/view/4080/4454>. Acesso em: 20 jul. 2020.

BUOLAMWINI, Joy. **Tons de gênero**: disparidades de precisão interseccional em classificação de gênero comercial. 2018. Laboratório de Mídias no Massachusetts Institute of Technology (MIT). Disponível em: <https://www.media.mit.edu/people/joyab/overview/>. Acesso em: 5 abr. 2021.

CANEVACCI, Massimo. **A cidade polifônica**. São Paulo: Studio Nobel, 1997.

CAPURRO, Rafael. Ethical issues of online social networks in Africa. **Innovation: Journal of appropriate librarianship and information work in Southern Africa**, Pretoria, v. 46, p. 161-175, December 2013. Disponível em: <http://www.capurro.de/OSNAfrica2012.html#ftn5>. Acesso em: 5 abr. 2021.

CAPURRO, Rafael. Privacy: an intercultural perspective. **Ethics and Information Technology**, [s. l.], v. 7, p. 37-47, 2005. Disponível em: <http://www.capurro.de/privacy.html>. Acesso em: 21 abr. 2021.

CASTORIADIS, Cornelius. **A instituição imaginária da sociedade**. Rio de Janeiro: Paz e Terra, 1982.

CASTORIADIS, Cornelius. **A instituição imaginária da sociedade**. Rio de Janeiro: Paz e Terra, 1991.

CASTORIADIS, Cornelius. **As encruzilhadas do labirinto I**. Tradução de Carmen Sylvia Guedes. 2. ed. Rio de Janeiro: Paz e Terra, 1997.

CASTORIADIS, Cornelius. **Figuras do pensável**. As encruzilhadas do labirinto VI. Tradução de Eliana Aguiar. Rio de Janeiro: Civilização Brasileira, 2004.

CAVNA, Michael. ‘Nobody knows you’re a dog’: as iconic Internet cartoon turns 20, creator Peter Steiner knows the joke rings as relevant as ever. **Washington Post**, Entertainment, [s. l.], July 31, 2013. Disponível em: [https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb\\_blog.html](https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html). Acesso em: 5 jun. 2022.

CHUN, Wendy Hui Kyong. **Control and Freedom**. Power and Paranoia in the Age of Fiber Optics. Cambridge/Londres: The MIT Press, 2006. Disponível em: [https://www.mondotheque.be/wiki/images/5/54/Wendy\\_Hui\\_Kyong\\_Chun\\_Control\\_and\\_Freedom.pdf](https://www.mondotheque.be/wiki/images/5/54/Wendy_Hui_Kyong_Chun_Control_and_Freedom.pdf). Acesso em: 5 jun. 2021.

CHUN, Wendy Hui Kyong. **Updating to Remain the Same**. Habitual New Media. Cambridge, Massachusetts/London: The MIT Press, 2016.

CHUPAN, Koravin. Factors influencing the decision to repurchase trainer online: case study Facebook. **JISB Journal**, Universidade Thammasat, a. 4, 2. ed., abr.-jun. 2018. Disponível em: [http://www.jisb.tbs.tu.ac.th/wp-content/uploads/2018/06/V.4No2\\_Jisb61\\_3Koravin\\_doi.pdf](http://www.jisb.tbs.tu.ac.th/wp-content/uploads/2018/06/V.4No2_Jisb61_3Koravin_doi.pdf). 2021. Acesso em: 5 abr. 2021.

CIBERIDEA. Núcleo de Pesquisas em Tecnologias da Comunicação, Cultura e Subjetividade. *In*: REVISTA ECO PÓS. Rio de Janeiro, 2020. Disponível em: [http://www.pos.eco.ufrj.br/site/grupos\\_de\\_pesquisa.php](http://www.pos.eco.ufrj.br/site/grupos_de_pesquisa.php). Acesso em: 2 mar. 2021.

CONHEÇA o interior do Data Center do Facebook na Carolina do Norte. *In*: CANALTECH. [S. l.], 11 dez. 2012. Disponível em: <https://canaltech.com.br/redes-sociais/Conheca-o-interior-do-Data-Center-do-Facebook-na-Carolina-do-Norte>. Acesso em: 5 abr. 2021.

CONVENÇÃO SOBRE OS DIREITOS DAS CRIANÇAS. Unicef Brasil, 2022. Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>. Acesso em: 15 jul. 2022.

CUMULATIVE number of monthly Facebook product users as of 2nd quarter 2021. *In*: STATISTA. [S. l.], Aug. 2, 2021. Disponível em: <https://www.statista.com/statistics/947869/facebook-product-mau/>. Acesso em: 20 set. 2021.

DATA PRIVACY BRASIL. Disponível em: <https://www.dataprivacybr.org/>. Acesso em: 25 abr. 2021.

DATA PRIVACY BRASIL. **Já está no ar o episódio de número 50 do #Dadocracia, o nosso podcast!** [S. l.], 7 abr. 2020. Instagram: @dataprivacybrasil. Disponível em: <https://www.instagram.com/p/CNYDWZZDklM/>. Acesso em: 7 abr. 2021.

DEBORD, Guy. **A sociedade do espetáculo**. Rio de Janeiro: Contraponto, 1967.

DELEUZE, Gilles. **Bergsonismo**. São Paulo: Editora 34, 1999.

DELEUZE, Gilles; GUATTARI, Félix. **Mil platôs: capitalismo e esquizofrenia**. Tradução de Aurélio Guerra Neto e Célia Pinto Costa. São Paulo: Editora 34, 1995.

DELEUZE, Gilles; GUATTARI, Félix. **O que é a Filosofia?** São Paulo: Editora 34, 2010.

DIDI-HUBERMAN, Georges. **Diante do tempo**: história da arte e anacronismo das imagens. Belo Horizonte: Editora da UFMG, 2015.

DIDI-HUBERMAN, Georges. **O que vemos, o que nos olha**. São Paulo: Editora 34, 1998.

DIDI-HUBERMAN, Georges; CHÉROUX, Clément; ARNALDO, Javier. **Quando as imagens tocam o real**. Tradução de Patrícia Carmello e Vera Casa Nova. Madrid: Círculo de Bellas Artes, 2013. p. 206-219. Disponível em: <https://periodicos.ufmg.br/index.php/revistapos/article/download/15454/12311/42901>. Acesso em: 2 fev. 2015.

DIGILABOUR. Quem somos. Disponível em: <https://digilabour.com.br/quemsomos/>. Acesso em: 14 abr. 2021.

EDWARD Snowden: the whistleblower behind the NSA surveillance revelations. **The Guardian**, Londres, 2012. Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 14 jun. 2022.

ENTENDA o escândalo de uso político de dados que derrubou valor do facebook e o colocou na mira de autoridades. **BBC News**, G1, [s. l.], 20 mar. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 27 jul. 2021.

ESTADÃO. Captura de tela uso de *cookies*. São Paulo, 2022. Disponível em: <https://www.estadao.com.br/>. Acesso em: 7 jun. 2022.

FACEBOOK completa 10 anos; veja a evolução da rede social. *In*: G1. São Paulo, 4 fev. 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/02/facebook-completa-10-anos-veja-evolucao-da-rede-social.html>. Acesso em: 18 jun. 2021.

FACEBOOK investe US\$ 1 bilhão em seu primeiro data center na Ásia. *In*: OLHAR DIGITAL. [S. l.], 6 set. 2018. Disponível em: <https://olhardigital.com.br/2018/09/06/pro/facebook-investe-us-1-bilhao-em-seu-primeiro-data-center-na-sia/>. Acesso em: 8 abr. 2021.

FACEBOOK, 2021. Feed de Notícias. Disponível em: <https://www.facebook.com/formedia/solutions/news-feed>. Acesso em: 18 jul. 2021.

FACEBOOK. Coleção território do FB – excerto de tela da seção Privacidade. Disponível em: <https://www.facebook.com/privacy/explanation>. Acesso em: 2 abr. 2021.

FACEBOOK. Coleção território do usuário – captura de tela das configurações da conta. Disponível em: <https://www.facebook.com/settings/?tab=account>. Acesso em: 2 jul. 2021.

FACEBOOK. Configurações Gerais da Conta. Disponível em: <https://www.facebook.com/settings/?tab=account>. Acesso em: 4 jul. 2021.

FACEBOOK. Cookies. Disponível em: <https://www.facebook.com/policies/cookies>. Acesso em: 20 out. 2020.



FACEBOOK. Disponível em: <https://www.facebook.com/>. Acesso em: 20 abr. 2021.

FACEBOOK. Nossa missão. Disponível em: <https://about.fb.com/br/company-info/>. Acesso em: 18 jul. 2021.

FACEBOOK. Política de Privacidade. Meta. Disponível em: <https://free.facebook.com/privacy/policy/#>. Acesso em: 5 ago. 2022.

FACEBOOK. Privacy. Disponível em: <https://www.facebook.com/about/privacy>. Acesso em: 20 mar. 2020.

FACEBOOK. Segurança no Facebook. Disponível em: <https://www.facebook.com/safety>. Acesso em: 18 jul. 2021.

FACEBOOK. Termos e Políticas. Disponível em: <https://www.facebook.com/policies>. Acesso em: 8 ago. 2020.

FACEBOOK'S revenue and net income from 2007 to 2020. *In*: STATISTA. [S. l.], 5 fev. 2021. Disponível em: <https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/>. Acesso em: 20 set. 2021.

FACHINI, Tiago. Direito Digital: o que é, importância e áreas de atuação. *In*: PROJURIS. São Paulo, 2022. Disponível em: <https://www.projuris.com.br/direito-digital/#:~:text=O%20direito%20digital%20%C3%A9%20um,espa%C3%A7os%20e%20em%20aparelhos%20eletr%C3%B4nicos>. Acesso em: 7 ago. 2022.

FERREIRA, Lorena de Risse. **A efemeridade na tecnocultura: escavações em aplicativos de imagens feitas para sumir**. 2019. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2019. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/8698>. Acesso em: 2 mar. 2020.

FISCHER, Gustavo Daudt. **As trajetórias e características do YouTube e Globo Media Center/Globo Vídeos: um olhar comunicacional sobre as lógicas operativas de websites de vídeos para compreender a constituição do caráter midiático da web**. 2008. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2008. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/2527>. Acesso em: 5 abr. 2020.

FISCHER, Gustavo Daudt. Desencavando interfaces: reflexões sobre arqueologia da mídia e procedimentos de “resgate” de páginas web. *In*: STEFEN, Cezar; BENVENUTO, Álvaro. (org.). **Tecnologia pra quê?** As reconfigurações no campo da Comunicação Social. Porto Alegre: Armazém Digital, 2012a. Disponível em: [http://www.academia.edu/3356304/Desencavando\\_Interfaces\\_Reflex%C3%B5es\\_Sobre\\_Arqueologia\\_Da\\_M%C3%ADia\\_E\\_Procedimentos\\_De\\_Resgate\\_De\\_P%C3%A1ginas\\_Web](http://www.academia.edu/3356304/Desencavando_Interfaces_Reflex%C3%B5es_Sobre_Arqueologia_Da_M%C3%ADia_E_Procedimentos_De_Resgate_De_P%C3%A1ginas_Web). Acesso em: 1 jun. 2014.

FISCHER, Gustavo Daudt. Do audiovisual confinado às audiovisualidades soterradas em interfaces enunciadoras de memória. *In*: KILPP, Suzana (org). **Tecnocultura audiovisual: temas, metodologias e questões de pesquisa**. Porto Alegre: Sulina, 2015.

FISCHER, Gustavo Daudt. Interfaces culturais e remixibilidade nas lógicas operativas dos websites. *In*: MONTAÑO, Sonia; FISCHER, Gustavo; KILPP, Suzana (org.). **Impacto das novas mídias no estatuto da imagem**. 1. ed. Porto Alegre: Sulina, 2012b, p. 131-148.

FISCHER, Gustavo Daudt. Tecnocultura: aproximações conceituais e pistas para pensar as audiovisualidades. *In*: KILPP, Suzana; FISCHER, Gustavo Daudt (org.). **Para entender as imagens: como ver o que nos olha?** Porto Alegre: Entremeios, 2013, p. 41-54.

FISCHER, Gustavo Daudt. Vida, morte e pós-morte do GeoCities: memória em degeneração/regeneração e nostalgia como crítica no Projeto One Terabyte of Kilobyte Age. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO – INTERCOM, XXXIX, 2016, São Paulo. **Anais [...]**. São Paulo: USP, 2016. p. 1-15. Disponível em: <http://portalintercom.org.br/anais/nacional2016/resumos/R11-2977-1.pdf>. Acesso em: 5 abr. 2020.

FLÔRES, Vinícius dos Santos. **Vigiar e compartilhar**: marcas da violência armada nas redes digitais do Fogo Cruzado. 2021. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2021. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/9761>. Acesso em: 7 abr. 2020.

FLUSSER, Vilém. **Filosofia da caixa preta**: ensaios para uma futura filosofia da fotografia. Rio de Janeiro: Relume Dumará, 2002.

FLUSSER, Vilém. **O universo das imagens técnicas**: elogio da superficialidade. São Paulo: Annablume, 2008.

FLYNN, Kerry. Facebook will share users' political leanings with ABC News, BuzzFeed. **The Huffington Post**, [s. l.], 31 out. 2014. Disponível em: [https://www.huffpost.com/entry/facebook-buzzfeed-politics\\_n\\_6082312](https://www.huffpost.com/entry/facebook-buzzfeed-politics_n_6082312). Acesso em: 18 jul. 2021.

FOUCAULT, Michel. **A arqueologia do saber**. Tradução de Luiz Felipe Baeta Neves, revisão de Ligia Vassalo. Petrópolis: Vozes, Lisboa: Centro do Livro Brasileiro, 1972. Originalmente publicado em 1969.

FOUCAULT, Michel. **Vigiar e punir**. Petrópolis: Vozes, 1983.

FUGAZZA, Grace Quaresma; SALDANHA, Gustavo Silva. A questão do direito à privacidade no Facebook: um estudo à luz da ética da informação. **Revista Informação**, Universidade de Londrina, Paraná, v. 14, n. 2, 2018. Disponível em: <https://www.uel.br/revistas/uel/index>. Acesso em: 21 out. 2020.

GALLOWAY, Scott. **Post Corona**: from crisis to opportunity. Nova Iorque: Portfolio/Penguin, 2020. Disponível em: [https://www.google.com.br/books/edition/Post.\\_Corona/IHr7DwAAQBAJ?hl=pt-BR&gbpv=1&dq=Post+Corona:+From+Crisis+to+Opportunity&printsec=frontcover](https://www.google.com.br/books/edition/Post._Corona/IHr7DwAAQBAJ?hl=pt-BR&gbpv=1&dq=Post+Corona:+From+Crisis+to+Opportunity&printsec=frontcover). Acesso em: 3 set. 2020.

GALVANI, Giovanna. Entenda a Guerra da Ucrânia em 10 pontos. **CNN Brasil**, São Paulo, 25 mar. 2022. Disponível em: <https://www.cnnbrasil.com.br/internacional/entenda-a-guerra-da-ucrania-em-10-pontos>. Acesso em: 5 abr. 2022.

GOMES, Pedro Gilberto A pergunta pela pergunta nos processos midiáticos. *In*: PPGCOM. São Leopoldo, 2011. Ementa da disciplina. São Leopoldo: Unisinos, 2011.

GOOGLE MEET. Segurança nas reuniões por videochamada. Disponível em: <https://meet.google.com/>. Acesso em: 5 jun. 2022.

GOOGLE. Central de Segurança. Disponível em: <https://privacy.google.com/?hl=pt-BR#>. Acesso em: 6 abr. 2021.

GOOGLE. Conta Google. Segurança. Disponível em: <https://myaccount.google.com/security>. Acesso em: 5 ago. 2021.

GOOGLE. Google Conta. Gerencie suas informações, privacidade e segurança para que o Google atenda suas necessidades. Disponível em: [https://myaccount.google.com/?hl=pt\\_BR&utm\\_source=OGB&utm\\_medium=act&pli=1](https://myaccount.google.com/?hl=pt_BR&utm_source=OGB&utm_medium=act&pli=1). Acesso em: 26 maio 2022.

GOOGLE. Think with Google. Disponível em: <https://www.thinkwithgoogle.com/intl/pt-br/tendencias-de-consumo/tendencias-de-comportamento/visual-stories/privacidade-guia-protecao-dados>. Acesso em: 8 ago. 2022.

GROW, Gordon. Understanding privacy. *In*: INTERNATIONAL TELECOMMUNICATION UNION WORKSHOP ON. UNS/05 ITU WUBIQUITOUS NETWORK SOCIETIES, 6-8 abr. 2005, [s. l.]. **Paper** [...]. [S. l.]: Privacy and Ubiquitous Network Societies/English ITU NEW INITIATIVES PROGRAMME, 2005. p. 6-8. Disponível em: [https://www.researchgate.net/publication/227984950\\_Ubiquitous\\_Network\\_Societies\\_Their\\_Impact\\_on\\_the\\_Telecommunication\\_Industry](https://www.researchgate.net/publication/227984950_Ubiquitous_Network_Societies_Their_Impact_on_the_Telecommunication_Industry). Acesso em: 3 set. 2021.

HOFFMAN, Claire. The battle for Facebook: Mark Zuckerberg launched an online empire from his dorm room at Harvard. Now four fellow students say he stole their idea. **The Rolling Stone Magazine**, New York, 15 September 2010. Disponível em: <https://www.rollingstone.com/culture/culture-news/the-battle-for-facebook-242989/>. Acesso em: 16 jul. 2021.

HUHTAMO, Erkki; PARIKKA, Jussi. **Media archeology**: approaches, applications, and Implications. Berkeley, California: University of California Press, 2011.

HUSTINX, Peter. Privacy by design: delivering the promises. **Springer**, [s. l.], v. 3, p. 253-255, 2010. Disponível em: <https://link.springer.com/content/pdf/10.1007/s12394-010-0061-z.pdf>. Acesso em: 26 abr. 2021.

INTERNET Archive. Coleção território do FB – excerto de tela da seção Privacidade de 2004 em The Facebook. Disponível em: <https://web.archive.org/web/20070630042627/http://www.facebook.com/terms.php>. Acesso em: 4 jul. 2021. Acesso em: 7 abr. 2021.

INTERNET Archive. Detalhamento da operação publicitária dentro do Facebook – sob nova nomenclatura. Novembro 2005. Disponível em: <https://web.archive.org/web/20051127050746/http://www.facebook.com/announce.php>. Acesso em: 18 jul. 2021.

INTERNET Archive. Excerto da tela da página inicial do FB quando restrito ao uso entre a comunidade escolar. 19 abr. 2006. Disponível em: <https://web.archive.org/web/20060419184949/https://www.facebook.com/>. Acesso em: 19 jul. 2021.

INTERNET Archive. Página de login da primeira versão da plataforma ainda chamada The Facebook em 2004. Disponível em: <https://web.archive.org/web/20040212031928/http://www.thefacebook.com>. Acesso em: 18 jul. 2021.

INTERNET Archive. Página dentro do The Facebook dedicada a conteúdo publicitário – Announcements. Agosto 2005. Disponível em: <https://web.archive.org/web/20051127050746/http://www.facebook.com/announce.php>. Acesso em: 18 jul. 2021.

INTERNET Archive. Página inicial The Facebook quando aberto para demais comunidades acadêmicas. 16 jul. 2004. Disponível em: <https://web.archive.org/web/20040716021640/http://thefacebook.com/>. Acesso em: 20 abr. 2021.

INTERNET Archive. Primeira versão do site The Facebook. 12 fev. 2004. Disponível em: <https://web.archive.org/web/20040212031928/http://www.thefacebook.com/>. Acesso em: 20 abr. 2021.

INTERNET LAB. Privacy International: a guide for policy engagement on data protection. The keys to data protection. Agosto 2018. Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2018/09/Data-Protection-COMPLETE.pdf>. Acesso em: 18 jul. 2021.

INTERNETLAB. Pesquisa em Direito e Tecnologia. O que é o Internetlab? Disponível em: <https://www.internetlab.org.br/pt/sobre/>. Acesso em: 19 jul. 2021.

ITAÚ é a marca mais valiosa do Brasil em 2020. *In*: INFOMONEY. [S. l.], 3 set. 2020. Disponível: <https://www.infomoney.com.br/negocios/itau-e-a-marca-mais-valiosa-do-brasil-em-2020-segundo-pesquisa/>. Acesso em: 6 abr. 2021.

ITAÚ. Disponível em: <https://www.itau.com.br/>. Acesso em: 21 abr. 2021.

ITAÚ. Privacidade. Disponível em: <https://www.itau.com.br/seguranca/privacidade/>. Acesso em: 21 abr. 2021.

JOHNSON, Steven. **Cultura da interface**: como o computador transforma nossa maneira de criar e comunicar. Rio de Janeiro: Jorge Zahar Editores, 2001.

KAISER, Brittany. **Manipulados**: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. São Paulo: HarperCollins, 2020.

KILPP, Suzana. **A traição das imagens**. Espelhos, câmeras e imagens especulares em *reality shows*. Porto Alegre: Entremeios, 2010.

KILPP, Suzana. Dispersão-convergência: apontamentos para a pesquisa de audiovisualidades. *In*: MONTAÑO, Sonia; FISCHER, Gustavo; KILPP, Suzana (org.). **Impacto das novas mídias no estatuto da imagem**. 1. ed. Porto Alegre: Sulina, 2012. p. 223-238.

KILPP, Suzana. **Ethnicidades televisivas sentidos identitários na tv: moldurações homológicas e tensionamentos**. 2002. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2002a. Disponível em: <https://www.tecnoculturaaudiovisual.com.br/wp-content/uploads/2020/06/Kilpp-Suzana-Ethnicidades-televisivas.pdf>. Acesso em: 5 jun. 2021.

KILPP, Suzana. Ethnicidades televisivas: molduras e moldurações. **Revista Fronteira**, São Leopoldo, UNISINOS, v. IV, p. 209-218, 2002b. Disponível em: <http://suzanakilpp.com.br/artigos/Ethnicidades-televisivas-molduras-molduracoes.pdf>. Acesso em: 5 jun. 2022.

KILPP, Suzana. Imagens conectivas da cultura. **Revista Famecos**, Porto Alegre, v. 17, n. 3, p. 181-189, set./dez. 2010. Disponível em: <https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/8186>. Acesso em: 3 abr. 2020.

KILPP, Suzana. Mundos televisivos, imaginários televisíveis e sociedade imaginada. **Contemporânea**, Salvador, v. 1, n.1, p. 155-180, 2003. Disponível em: [http://www.suzanakilpp.com.br/artigos/Mundos\\_televisivos\\_Imaginarios\\_Televisiveis\\_e\\_Sociedade\\_Imaginada.pdf](http://www.suzanakilpp.com.br/artigos/Mundos_televisivos_Imaginarios_Televisiveis_e_Sociedade_Imaginada.pdf). Acesso em: 5 jun. 2022.

KILPP, Suzana; FISCHER, Gustavo. Janelas de Flusser e Magritte: o que é, afinal, um webvídeo? **Intexto**, Porto Alegre, UFRGS, v. 2, n. 23, p. 36-49, jul./dez. 2010. Disponível em: <http://seer.ufrgs.br/intexto/article/view/11124%3E>. Acesso em: 10 abr. 2021.

KILPP, Suzana; MONTANO, Sonia. Audiovisualidades, tecnocultura e pesquisa em comunicação. In: KILPP, Suzana *et al.* **Tecnocultura audiovisual: temas, metodologias e questões de pesquisa**. Porto Alegre: Sulina, 2015. 207 p.

KIRKPATRICK, David. **O efeito Facebook**. Rio de Janeiro: Intrínseca, 2011.

KITTLER, Friedrich A. **Gramofone, filme typewriter**. Tradução de Guilherme Gontijo Flores e Daniel Martineschen. Belo Horizonte: Editora da UFMG; Rio de Janeiro: EDUERJ, 2019.

KRAPP, Peter. A short media history of influence operations. In: SEMINÁRIO CAPES/PRINT DIGITAL TRANSFORMATION AND THE HUMANITIES: CONTEMPORARY TECHNOCULTURAL DIMENSIONS FOR RESEARCH IN THE SOCIAL AND HUMAN SCIENCES, 2020, São Leopoldo/Brasil. **Comunicação [...]**. São Leopoldo: Unisinos, 2020a. Disponível em: [https://www.dropbox.com/s/53664916whfyq51/Brazil%20slides-Peter\\_Krapp.zip?dl=0&file\\_subpath=%2FBrazil+slides%2Fmemes-brazil.pdf](https://www.dropbox.com/s/53664916whfyq51/Brazil%20slides-Peter_Krapp.zip?dl=0&file_subpath=%2FBrazil+slides%2Fmemes-brazil.pdf). Acesso em: 20 abr. 2020.

KRAPP, Peter. **Beyond schlock on screen: teaching the history of cryptology through media representations of secret communications**. In: INTERNATIONAL CONFERENCE ON HISTORICAL CRYPTOLOGY, 2<sup>nd</sup>, 23-26 June, 2019, Mons, Belgium. **Proceedings [...]**. Mons: Linköping University, 2019. p. 79-85. Disponível em: <https://www.ep.liu.se/ecp/158/009/ecp19158009.pdf>. Acesso em: 20 abr. 2020.

KRAPP, Peter. Comunicação secreta e história da criptologia: um desafio para as Humanidades Digitais. **TECCOGS** – Revista Digital de Tecnologias Cognitivas, São Paulo, n. 21, jan./jun. 2020b, p. 146-165. Tradução de Eduardo Harry Luersen. Disponível em: <https://revistas.pucsp.br/teccogs/article/download/51784/33812>. Acesso em: 5 abr. 2020.

KRAUSE, Roberta Fleck Saibro. [**Timeline**]. [S. l.], Facebook: 29 mar. 2021. Roberta Fleck Saibro Krause. Disponível em: <https://www.facebook.com/robertaflecksaibrokrause>. Acesso em: 29 mar. 2021.

KRAUSE, Roberta Fleck Saibro. **Zelandando o ouro produzido no passado**: escavando construtos de memória da publicidade audiovisual a partir do *site* Propagandas Históricas. 2016. Dissertação (Mestrado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2016. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/5184>. Acesso em: 5 abr. 2021.

KRAUSE, Roberta Fleck Saibro; NESS, Lucas Melo. Construtos de segurança a partir de suas atualizações em imagens técnicas; apontamentos sobre formas de login e serviços autenticadores na web. *In*: INTERCOM – SOCIEDADE BRASILEIRA DE ESTUDOS INTERDISCIPLINARES DA COMUNICAÇÃO/CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 43, 1-10 out. 2020, Virtual. **Anais** [...]. Modalidade Virtual: UFBA, 2020. Disponível em: <https://portalintercom.org.br/anais/nacional2020/resumos/R15-0217-1.pdf>. Acesso em: 5 abr. 2021.

LABMEM. **30 anos do Metaverso**, Brasil, 2022. [S. l.], jun. 2022. Instagram: @LabMem. Disponível em: [https://www.instagram.com/p/CfWzFVRMQUc/?utm\\_source=ig\\_web\\_copy\\_link](https://www.instagram.com/p/CfWzFVRMQUc/?utm_source=ig_web_copy_link). Acesso em: 7 jun. 2022.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). LGPD ESPM. 2022. Disponível: <https://www.espm.br/cursos/pocket-records/protecao-de-dados-com-lei-geral-de-protecao-de-dados-lgpd-e-as-mudancas-com-o-marco-civil-da-internet-mci/>. Acesso em: 2 jun. 2022.

LEMOS, Andre. Mídias locativas e vigilância: sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais. *In*: FIRMINO, Rodrigo; BRUNO, Fernanda; KANASHIRO, Marta (org.). **Vigilância, Segurança e Controle Social na América Latina**, Curitiba, p. 621-648, 2009. Disponível em: [https://www.academia.edu/1771493/M%C3%ADdias\\_locativas\\_e\\_vigil%C3%A2ncia\\_sujeito\\_inseguro\\_bolhas\\_digitais\\_paredes\\_virtuais\\_e\\_territ%C3%B3rios\\_informacionais](https://www.academia.edu/1771493/M%C3%ADdias_locativas_e_vigil%C3%A2ncia_sujeito_inseguro_bolhas_digitais_paredes_virtuais_e_territ%C3%B3rios_informacionais). Acesso em: 5 jul. 2022.

LOPES, Tiago Ricciardi Correa. **Aura e vestígios do audiovisual em experiências estéticas com mídias locativas**: performances algorítmicas do corpo no espaço urbano. 2014. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2014. Disponível em: <http://biblioteca.asav.org.br/vinculos/000012/00001222.pdf>. Acesso em: 5 jun. 2021.

LYON, David. Surveillance culture: engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, Los Angeles, USC Annenberg Press, v. 11, p. 1-18, 2017. In: BRUNO, Fernanda *et al.* (org.) Tradução de Heloísa Cardoso Mourão *et al.*

**Tecnopolíticas da vigilância: perspectivas da margem.** 1. ed. São Paulo: Boitempo, 2018.

MACIEL, Maria Esther. **As ironias da ordem:** coleções, inventários e enciclopédias ficcionais. 1. ed. Belo Horizonte: Editora da UFMG, 2009.

MAINO, Patrícia. **Faces da visibilidade:** a tensão entre publicidade e privacidade. 2010. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2010. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/3990?show=full>. Acesso em: 2 abr. 2020.

MANOVICH, Lev. A era da infoestética. [Entrevista cedida a] Cícero da Silva. **Lumina**, Juiz de Fora, v. 6, n. 1, 22 jun. 2012, p. 1-11. Disponível: <https://periodicos.ufjf.br/index.php/lumina/article/view/21019/11394>. Acesso em: 1 set. 2020.

MANOVICH, Lev. **Instagram and contemporary image.** 2017. All text is available under Attribution-Non Commercial-No Derivatives 4.0 International Creative Commons license. Disponível em: <http://manovich.net/index.php/projects/instagram-and-contemporary-image>. Acesso em: 2 set. 2020.

MANOVICH, Lev. **The language of new media.** Massachusetts: The MIT Press, 2001.

MAYER, William. **Audiovisualidades e construtos de movimento nas imagens e imagétês do Facebook.** 2019. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2019. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/8697>. Acesso em: 20 jun. 2021.

MCCOSKER, Anthony; WILKEN, Rowan. **Automating vision:** the social impact of the new camera consciousness. 1. ed. New York: Routledge, 2020. Disponível em: [https://www.researchgate.net/publication/340275735\\_Automating\\_Vision\\_The\\_Social\\_Impact\\_of\\_the\\_New\\_Camera\\_Consciousness](https://www.researchgate.net/publication/340275735_Automating_Vision_The_Social_Impact_of_the_New_Camera_Consciousness). Acesso em: 21 abr. 2021.

MCLUHAN, Marshall. **Os meios de comunicação como extensões do homem.** São Paulo: Cultrix, 1964.

MCPHERSON, Tara. Capa. In: CHUN, Wendy Hui Kyong. **Control and Freedom.** Power and Paranoia in the Age of Fiber Optics. Cambridge/Londres: The MIT Press, 2006. Disponível em: [https://www.mondothèque.be/wiki/images/5/54/Wendy\\_Hui\\_Kyong\\_Chun\\_Control\\_and\\_Freedom.pdf](https://www.mondothèque.be/wiki/images/5/54/Wendy_Hui_Kyong_Chun_Control_and_Freedom.pdf). Acesso em: 5 jun. 2021.

MELLO, Patricia Campos. Em livro, delatora esmiúça uso de rede social para manipular opinião pública. **Folha de São Paulo**, São Paulo, 25 abr. 2020. Disponível em: [https://www1.folha.uol.com.br/amp/mundo/2020/04/em-livro-delatora-esmiuca-uso-de-rede-social-para-manipular-opinio-publica.shtml?utm\\_source=twitter&utm\\_medium=social&utm\\_campaign=twfolha&\\_\\_twitter\\_impression=true](https://www1.folha.uol.com.br/amp/mundo/2020/04/em-livro-delatora-esmiuca-uso-de-rede-social-para-manipular-opinio-publica.shtml?utm_source=twitter&utm_medium=social&utm_campaign=twfolha&__twitter_impression=true). Acesso em: 28 abr. 2020.

MIRO. Disponível em: [www.miro.com](http://www.miro.com). Acesso em: 20 abr. 2020.

MONTAÑO, Sônia. **Tecnocultura audiovisual**. Temas, metodologias e questões de pesquisa. 1. ed. Porto Alegre: Sulina, 2015. p. 61-111.

MONTAÑO, Sonia; KILPP, Suzana. Trânsitos e conectividades na web: uma ecologia audiovisual. **Revista Matrizes**, São Paulo. v. 6, n. 1-2, p. 129-143, 2012. Disponível em: <https://www.revistas.usp.br/matrizes/article/download/48054/51814/58224>. Acesso em: 8 abr. 2020.

NORA, Pierre. Entre história e memória: a problemática dos lugares. **Revista Projeto História**, São Paulo, v. 10, p. 7-28, 1993. Disponível em: <https://revistas.pucsp.br/revph/article/view/12101>. Acesso em: 6 abr. 2021.

NUMBER of Facebook users in Brazil from 2018 to 2027. *In*: SATISTA. [S. l.], 26 jul. 2022. Disponível em: <https://www.statista.com/statistics/244936/number-of-facebook-users-in-brazil/>. Acesso em: 7 jul. 2022.

NUMBER of monthly active Facebook users worldwide as of 2nd quarter 2022. *In*: STATISTA. [S. l.], 28 jul. 2022. Disponível em: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>. Acesso em: 7 jul. 2022.

OBSERVATÓRIO Covid-19 Brasil. *In*: BIBLIOTECA Virtual em Saúde (BVS), Ministério da Saúde. Brasília, 11 mar. 2020. Disponível em: <https://bvsm.s.saude.gov.br/observatorio-covid-19-brasil/>. Acesso em: 3 jun. 2022.

ORWELL, George. **1984**. Tradução de Alexandre Hubner e Heloísa Jahn. São Paulo: Companhia das Letras, 1989.

OTTE, G; VOLPE, M. Um olhar constelar sobre o pensamento de Walter Benjamin. **Fragmentos**, Florianópolis, n. 18, jan./jun., 2000. Disponível em: <https://periodicos.ufsc.br/index.php/fragmentos/article/viewFile/6415/5984>. Acesso em: 10 jan. 2022.

PARA FACILITAR compreensão, Meta atualiza políticas de privacidade do Facebook e Instagram. *In*: PRIVACY TECH. [S. l.], 14 jun. 2022. Disponível em: [https://www.privacytech.com.br/redes-sociais/pensando-em-facilitar-a-compreensao-dos-usuarios-meta-atualiza-politicas-de-privacidade-do-facebook-e-instagram,415587.jhtml?utm\\_campaign=newsletter\\_113&utm\\_medium=email&utm\\_source=RD+Station](https://www.privacytech.com.br/redes-sociais/pensando-em-facilitar-a-compreensao-dos-usuarios-meta-atualiza-politicas-de-privacidade-do-facebook-e-instagram,415587.jhtml?utm_campaign=newsletter_113&utm_medium=email&utm_source=RD+Station). Acesso em: 5 jun. 2022.

PEREIRA, Gabriel. Automating vision: the social impact of the new camera consciousness (Review). **New Media & Society**, [s. l.], v. 23, n. 5, p. 1332-1334, Fev. 2021. Disponível em: <https://journals.sagepub.com/doi/10.1177/1461444821989639>. Acesso em: 21 abr. 2021.

PEZZI, Ana Paula Jacobus. **A necessidade de proteção de dados pessoais nos arquivos de consumo**: em busca da concretização do Direito à privacidade. 2007. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2007. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/2400>. Acesso em: 8 abr. 2020.



PIRES, Julherme José. **A tecnotropicalidade em Aquarius**. 2021. Tese (Doutorado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2021. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/9714>. Acesso em: 5 jun. 2022.

POLIDORO, Bruno. Cinema, vídeo, digital: a virtualidade do audiovisual. **Revista Famecos**, Porto Alegre, n. 19, p. 1-5, ago. 2008. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/download/4153/3165>. Acesso em: 2 maio 2020.

PORTAL de Periódicos CAPES/MEC. Disponível em: <https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php?>. Acesso em: 2 abr. 2021.

PRIVACIDADE - Autógrafo. [S. l.: s. n.], 10 mar. 2021. 1 vídeo (30 s). Disponível em: [https://www.youtube.com/watch?v=c83z\\_su9Ty4](https://www.youtube.com/watch?v=c83z_su9Ty4). Acesso em: 26 abr. 2021.

PRIVACY TOOLS BR. Sobre. Disponível em: <https://www.privacytools.com.br/sobre/>. Acesso em: 5 jun. 2022.

QUADROS, Ana Maciel de; MARCON, Karina. Os conceitos de público e privado nas redes sociais e suas implicações pedagógicas. **Revista Espaço Acadêmico**, Maringá, Universidade Estadual de Maringá, n. 160, p. 68-77, set. 2014. Disponível em: <https://periodicos.uem.br/ojs/index.php/EspacoAcademico/article/download/24485/13516/>. Acesso em: 3 set. 2020.

RANCIÈRE, Jacques. **O destino das imagens**. Rio de Janeiro: Contraponto, 2013.

RANCIÈRE, Jacques. **O destino das imagens**. Tradução de Mônica Costa Netto. Rio de Janeiro: Contraponto, 2012.

READ, Brock. Have you 'Facebooked' him? **The Chronicle of Higher Education**, [s. l.], May, 28 2004. Disponível em: <https://www.chronicle.com/article/have-you-facebooked-him/>. Acesso em: 5 abr. 2021.

RODRIGUES, Adriano. Experiência, modernidade e campo dos media. In: SANTANA, Raimundo Monteiro (org). **Reflexões sobre mundo contemporâneo**. Teresina: Revan, 2000. p. 189-215.

ROSELLO, Mireille. **Culture de L'insecurité**. Montreal: Université de Montreal, 2008. Disponível em: <http://www.cerium.ca/Insecurite-linguistique-et>. Acesso em: 5 jun. 2022.

ROTHAERMEL, Frank T. Facebook, Inc. **Harvard Business Publishing Education**, Cambridge, p. 1-40, Oct. 6. 2015. Disponível em: <https://hbsp.harvard.edu/product/MH0030-PDF-ENG?Ntt=facebook>. Acesso em: 5 abr. 2020.

SAMSUNG estreia no Brasil nova campanha global de segurança. In: SAMSUNG Newsroom Brasil. [S. l.], 22 jul. 2022. Disponível em: <https://news.samsung.com/br/samsung-estrela-no-brasil-nova-campanha-global-de-seguranca>. Acesso em: 3 jul. 2022.

SANTAELLA, Lucia; RIBEIRO, Daniel Melo. A arqueologia benjaminiana para iluminar o presente midiático. *In*: MUSSE, Cristina Ferraz; VARGAS, Herom; NICOLAU, Marcos (org.). **Comunicação, mídias e temporalidades**. Salvador: EDUFBA, 2017. p. 59-78. Disponível em:

[https://repositorio.ufba.br/bitstream/ri/22861/3/Comunica%C3%A7%C3%A3o%2CM%C3%ADdiaseTemporalidades\\_ChristinaMusse-HeromVargas-MarcosNicolau.pdf](https://repositorio.ufba.br/bitstream/ri/22861/3/Comunica%C3%A7%C3%A3o%2CM%C3%ADdiaseTemporalidades_ChristinaMusse-HeromVargas-MarcosNicolau.pdf). Acesso em: 7 abr. 2022.

SANTOS, Carlos Cesar; SALES, Jefferson David de Araújo. O desafio da privacidade na internet das coisas. **Revista Eletrônica de Gestão Organizacional**, Recife, v. 13, p. 282-289, 2015. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/22115>. Acesso em: 8 abr. 2021.

SANTOS, Myrian Sepúlveda. **Memória coletiva e teoria social**. São Paulo: Annablume, 2003.

SCHAEFFER, Christian Luis. Monitoramento de mídias sociais no processo de análise de percepção dos usuários sobre a segurança de Porto Alegre. **Revista Foco - Interdisciplinary Studies**, Curitiba, v. 9, n. 2, p. 33-53, 2016. Disponível em: <https://revistafoco.emnuvens.com.br/foco/article/view/249>. Acesso em: 2 abr. 2021.

SEGURO. *In*: FERREIRA, Aurelio Buarque de Holanda. **Minidicionário da Língua Portuguesa**. 3. ed. Rio de Janeiro: Nova Fronteira 1993. p. 498.

SEM CÂMERA NA MINHA CARA. Disponível em: <https://www.semcameranaminhacara.meurecife.org.br/>. Acesso em: 16 jun. 2022.

SHAW, Debra Benita. **Technoculture: the key concepts**. New York: Berg, 2008.

SHNAIDER, Amanda. WhatsApp foca na privacidade em sua maior campanha no Brasil. **Meio&Mensagem**, São Paulo, 16 ago. 2021. Disponível em: <https://www.meioemensagem.com.br/home/midia/2021/08/16/whatsapp-foca-na-privacidade-em-sua-maior-campanha-no-brasil.html>. Acesso em: 2 jun. 2022.

SILVA, Julia Dreher Pacheco da. **Internet como dispositivo de vigilância: um estudo sobre geração Y e suas adequações**. 2017. Dissertação (Mestrado em Ciências da Comunicação) - Programa de Pós-Graduação em Ciências da Comunicação, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, 2017. Disponível em: <http://www.repositorio.jesuita.org.br/handle/UNISINOS/7074?locale-attribute=en>. Acesso em: 5 abr. 2020.

SILVA, Sergio Damasceno. WhatsApp lança sua primeira campanha global no Brasil. **Meio&Mensagem**, São Paulo, 13 fev. 2020. Disponível em: <https://www.meioemensagem.com.br/home/comunicacao/2020/02/13/whatsapp-lanca-primeira-campanha-global-no-brasil.html>. Acesso em: 2 abr. 2022.

SIMÕES, Helton Gomes. Em depoimento de 5 horas ao senado americano, Mark Zuckerberg admite erros do Facebook. *In*: G1, Economia. [S. l.], 10 abr. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml>. Acesso em: 18 jul. 2021.

TWITTER. Privacy Policy. Disponível em: <https://twitter.com/en/privacy>. Acesso em: 3 abr. 2021.

TWITTER. Privacy. Disponível em: <https://privacy.twitter.com/pt>. Acesso em: 5 abr. 2021.

UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS). Grupo de Pesquisa TCAv. Audiovisualidades e tecnocultura: comunicação, memória e design. Líderes do grupo: Suzana Kilpp e Gustavo Daudt Fischer. São Leopoldo, 2003. Disponível em: <http://dgp.cnpq.br/dgp/espelhogrupo/3259429458389904>. Acesso em: 5 jan. 2015.

VAN DIJCK, José. Datafication, dataism and dataveillance: big data between scientific paradigm and ideology. **Surveillance & Society**, [s. l.], v. 12, n. 2, p. 197-208, 2014. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication>. Acesso em: 2 abr. 2020.

VAN DIJCK, José; POELL, Thomas; WAAL, Martijn de. **The platform society**. New York: Oxford University Press, 2018.

WEIBEL, Peter. El mundo como interfaz. **Elementos: ciencia y cultura**, Puebla, Benemérita Universidad Autónoma de Puebla, v. 7, n. 40, p. 23-33, 2001. Disponível em: <https://www.redalyc.org/pdf/294/29404005.pdf>. Acesso em: 14 maio 2021.

WERSHLER, Darren; PARIKKA, Jussi; EMERSON, Lori. **What is a Media Lab?** Situated practices in media studies. 2017. Disponível em: <http://whatisamedialab.com/the-authors/>. Acesso em: 22 out. 2019.

WHATSAPP lança no Brasil sua primeira campanha de marca no mundo. *In*: ALMAPBBDO. São Paulo, 13 fev. 2020. Disponível em: <https://www.almapbbdo.com.br/pt/trabalhos/whatsapp-lanca-no-brasil-sua-primeira-campanha-de-marca-do-mundo+382>. Acesso em: 5 jun. 2022.

WOLF, Mauro. **Teorias da Comunicação**. 2. ed. Lisboa: Editorial Presença, 1992.

ZIELINSKI, Siegfried. **Deep time of media: toward an archaeology of hearing and seeing by technical means**. Cambridge, Massachussets: MIT Press, 2006.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2020.