UNIVERSIDADE FEDERAL FLUMINENSE

PATRICK BARRETO DOS SANTOS

Aplicação do Método de Inspeção Semiótica Científico para Avaliação da Interação Humano-Dados

NITERÓI

2019

UNIVERSIDADE FEDERAL FLUMINENSE

PATRICK BARRETO DOS SANTOS

Aplicação do Método de Inspeção Semiótica Científico para Avaliação da Interação Humano-Dados

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Computação Visual

Orientador:
Luciana Cardoso de Castro Salgado

NITERÓI

2019

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

S237a Santos, Patrick Barreto dos
Aplicação do Método de Inspeção Semiótica Científico para Avaliação da Interação Humano-Dados / Patrick Barreto dos Santos ; Luciana Cardoso de Castro Salgado, orientadora. Niterói, 2019.
92 f. : il.

Dissertação (mestrado)-Universidade Federal Fluminense, Niterói, 2019.

DOI: http://dx.doi.org/10.22409/PGC.2019.m.14116052760

1. Human-Data Interaction. 2. Human-Computer Interaction. 3. Semiotic Inspection Method. 4. Produção intelectual. I. Salgado, Luciana Cardoso de Castro, orientadora. II. Universidade Federal Fluminense. Instituto de Computação. III. Título.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

Patrick Barreto dos Santos

Aplicação do Método de Inspeção Semiótica Científico para Avaliação da Interação Humano-Dados

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Computação. Área de concentração: Computação Visual

Aprovada em Abril de 2019 .

BANCA EXAMINADORA

Prof(a). Luciana Salgado - Orientador, UFF

Prof. José Viterbo, UFF

Prof. Flávia Bernadini, UFF

Prof. Roberto Pereira, UFPR

Prof(a). Isabela Gasparini , UDesc

Niterói

2019

"O homem é feito visivelmente para pensar; é toda a sua dignidade e todo o seu mérito, e todo o seu dever é pensar bem." (Blaise Pascal)

Agradecimentos

Nestas palavras, quero expressar a minha profunda gratidão por tudo aquilo que aprendi e vivenciei ao longo de todo esse período riquíssimo enquanto fui mestrando. Primeiramente, sou muito grato a Deus por todas as coisas que passei, pelas pessoas que conheci, pelas grandes oportunidades que a universidade pública me propiciou. Sou muito grato pela nobre orientação da Luciana Salgado, sempre acessível, organizada, sendo fonte de muito conhecimento e sua orientação foi decisiva para a elaboração desta dissertação, bem como das duas publicações, sendo uma internacional. Ao professor José Viterbo, também sou muito grato pelas suas contribuições e ideias! Quero agradecer aos professores Diego Gimenez Passos, Igor Monteiro Moraes, Ricardo Torreão, Célio Albuquerque, Cristina Boeres, Vanessa Murta, Marcos Lage, pela dedicação, comprometimento e pelo ensino de qualidade.

Quero agradecer também a minha mãe, Luzimar Barreto dos Santos, e minha Irmã, Paloma Barreto dos Santos, que me educaram, superando situações adversas.

Ao amigos do Grupo de Interação Humano-Computador, Rômulo Ponciano, Mateus de Souza Monteiro, Emerson Souza, Maria Clara Guimarães, Marcela Ramos, sou grato pelas contribuições a esta dissertação. Agradeço também aos amigos de laboratório e da Superintendência de Tecnologia da Informação (STI), Mônica da Silva, Daniel Pinheiro da Silva Júnior, Diogo Perdomo Castro, Tielle Alexandre, Rosana Petrucio, Bruno dos Santos Silva, Alexandre Gomes, Matheus Bersot, Gabriel Mantini, Fabrício Farias, Thiago Nazareth, Leandro de Cicco, pela troca de experiências, trabalho em equipe e contribuições. Igualmente, agradeço aos amigos que conheci no Grupo de Computação Aplicada à Saúde, Prof. Flávio Luiz Seixas, Érito Marques, Celine Abreu, Caio Serra, pelo trabalho em equipe.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pela bolsa de mestrado que recebi durante todo o curso, bem como pelos demais auxílios.

Por fim, quero agradecer a todos os familiares, amigos e funcionários do Instituto de Computação da Universidade Federal Fluminense que, direta ou indiretamente, ajudaram-me e apoiaram-me em vários momentos durante o curso.

Resumo

A crescente adesão ao uso de redes sociais, bem como a utilização de *smartphones* em diversas tarefas no cotidiano de muitas pessoas, têm possibilitado novas maneiras de gerar dados sobre o usuário. O interesse no processamento desses dados estimula a aplicação de métodos sofisticados de aprendizado de máquina que permitem a extração de inferências como o contexto de uso, condição física ou estados emocionais, por exemplo. Entretanto, a disponibilidade irrestrita desses dados (em grande parte, dados pessoais), pode levar a violações de privacidade, riscos legais e de propriedade intelectual, danos à reputação e outras preocupações éticas e sociais. Tendo em vista essas preocupações que emergem a partir da natureza de tais desenvolvimentos, um campo de estudos denominado Interação Humano-Dados (IHD) propõe *incluir o humano no centro dos fluxos de dados e fornecer mecanismos para os cidadãos interagirem com esses sistemas e dados explicitamente*. Para isso, IHD estabelece três conceitos fundamentais, a saber: Legibilidade, Agência e Negociabilidade. Além da abordagem de IHD, outro campo de estudos, denominado Interação Humano-Computador (IHC), têm expressado tais preocupações refletindo a necessidade em realizar pesquisas considerando uma dimensão mais abrangente, as quais permitam explorar e compreender os fatores envolvidos no uso de sistemas computacionais baseados nas necessidades de indivíduos em termos de valores humanos. Assim, esta dissertação tem como objetivo principal avaliar as oportunidades de Interação Humano-Dados em *Transparency Enhancing Tools - TETs*, explorando as estratégias comunicativas adotadas pelos projetistas de sistemas computacionais para este fim e compreendendo como se dá a percepção de tal comunicação por parte dos usuários, baseando-se nas compreensões da Engenharia Semiótica. Para isso, adotamos um método de avaliação em IHC, denominado Método de Inspeção Semiótica (MIS) para fins científicos. Portanto, espera-se contribuir com a comunidade de pesquisa em IHC e com os projetistas de sistemas computacionais nas questões de avaliação e design considerando a perspectiva de IHD.

Palavras-Chave: Interação Humano-Dados, Privacidade, Dados Pessoais, Engenharia Semiótica, Ferramentas de Apoio à Transparência, Interação Humano-Computador, Valores Humanos, Método de Inspeção Semiótica.

Abstract

The growing adoption of the social networks, as well as the use of smartphones in various tasks in the daily lives of many people, have enabled new ways of generating data about the user. The interest in processing these data promotes the sophisticated machine learning methods that allow the extraction of inferences such as context of use, physical condition or emotional states, for example. However, unrestricted availability of such data (largely personal data) can lead to privacy breach, legal and intellectual property risks, reputation damage, and other ethical and social concerns. In light of these concerns emerging from the nature of such developments, a field of study called Human Data Interaction (HDI) proposes to include the human at the center of data flows and provide mechanisms for citizens to interact with those systems and data explicitly. For this, HDI establishes three fundamental concepts, namely: Legibility, Agency and Negotiability. In addition to the HDI approach, another field of study, called Human-Computer Interteration (HCI), has expressed these concerns reflecting the need to carry out research considering a more comprehensive dimension, which allows us to understand the factors involved in the use of computer systems based on the needs of individuals in terms of human values. Thus, this dissertation has as main objective to evaluate the opportunities of Human-Data Interaction in Transparency Enhancing Tools - TETs, exploring the communicative strategies adopted by the computer system designers for this purpose and understanding the perception of such communication by the users, based on the understanding of Semiotic Engineering. For this purpose, we adopted a method of evaluation in IHC, called Semiotic Inspection Method (SIM) for scientific purposes. Therefore, it is hoped to contribute with the research community in IHC and with the designers of computational systems in the questions of evaluation and design considering the perspective of IHD.

Keywords: Human-Data Interaction, Privacy, Personal Data, Semiotic Engineering, Transparency Enhancing Tools, Human-Computing Interaction, Human Values, Semiotic Inspection Method.

Lista de Figuras

2.1 Visão de IHD proposto por Mortier et. al. em [39] 8

2.2 Exemplificação de conceitos de IHD no aplicativo *Snapchat*. 11

2.3 Metacomunicação entre Design e Usuário - Adaptado de [46] 12

2.4 Exemplos de signos no aplicativo *Snapchat*. 14

2.5 Exemplos de signos dinâmicos no aplicativo *Snapchat*. 15

2.6 Visão geral do Método de Inspeção Semiótica - Adaptado de [46] 16

4.1 Exemplos de signos metalinguísticos na seção de *'Controle de atividade'* do MyActivity. 30

4.2 Designer apresentando informações mais detalhadas, por meio de signos metalinguísticos. 31

4.3 Exemplos de signos metalinguísticos identificados na seção de *'Ajuda'* do MyActivity. 32

4.4 Signos metalinguísticos em seções diversas do MyActivity. 32

4.5 Exemplos de signos estáticos identificados na tela inicial. 34

4.6 Exemplos de signos estáticos identificados, no menu principal e na seção de *'Controles de atividade'*. 34

4.7 Exemplos de signos dinâmicos identificados na interface inicial e seus contextos de aplicação. 36

4.8 Exemplo de interação com signos dinâmicos identificados na seção de *'Controles de atividade'*. 37

4.9 Signo de aviso e resultado de suas interações. 38

4.10 Exemplo de signo de aviso ao excluir um registro de atividade. 38

4.11 Exemplos de signos metalinguísticos na tela inicial do Privacy Badger. . . 45

4.12 Signos que sinalizam opções do tipo *'Saiba mais'*. 46

4.13 Designer comunicando informações detalhadas na seção de *'Ajuda'*. 47

4.14 Designer comunicando sobre como proceder para reportar erros. 48

4.15 Designer comunicando sobre efeitos colaterais. 48

4.16 Exemplo de signos estáticos no Privacy Badger. 49

4.17 Uso de *switch buttons* e contador de possíveis trackers encontrados pelo Privacy Badger. 51

4.18 Signos dinâmicos no Privacy Badger. 51

4.19 Exemplo de *Cards* MyActivity. 56

4.20 Exemplo de *Modal* MyActivity. 56

4.21 Exemplo de Filtros de Busca no Privacy Badger. 57

4.22 Exemplo de *Switch Buttons* no Privacy Badger. 57

Lista de Tabelas

4.1 Sumário das respostas obtidas nos estudos 1 e 2 para as questões de pesquisa definidas. 58

4.2 Sumário dos resultados convergentes e divergentes identificados na triangulação. 59

Lista de Abreviaturas e Siglas

CCPA	:	California Consumer Privacy Act of 2018;
EC	:	Estratégia de Comunicação;
ENGSEM	:	Engenharia Semiótica;
EUDPD	:	European Union Data Protection Directive;
GDPR	:	General Data Protection Regulation;
HDI	:	Human-Data Interaction;
IHC	:	Interação Humano-Computador;
IHD	:	Interação Humano-Dados;
IoT	:	Internet of Things;
LGPDP	:	Lei Geral de Proteção de Dados Pessoais;
MIS	:	Método de Inspeção Semiótca;
PB	:	Privacy Badger;
QP	:	Questão de Pequisa;
TET	:	Transparency Enhancing Tools;
TIC	:	Tecnologia da Informação e Comunicação;
UI	:	User Interface;
UX	:	User eXperience;

Sumário

1 Introdução **1**

1.1 Motivação e Definição do Problema 3

1.2 Objetivos 5

1.3 Metodologia 5

1.4 Organização 6

2 Fundamentação Teórica **7**

2.1 Interação Humano-Dados 7

2.2 Engenharia Semiótica 11

2.3 Método de Inspeção Semiótica 15

3 Trabalhos Relacionados **18**

3.1 Estudos com Foco na Usabilidade 18

3.2 Estudos com Abordagens Teóricas, Requisitos de Design e/ou Diretrizes . . 20

3.3 Consideração Sobre os Trabalhos Relacionados 25

4 Estudos Empíricos **26**

4.1 Metodologia 26

4.2 Estudo I: My Activity 29

4.2.1 Signos Metalinguísticos 30

4.2.2 Reconstrução da Metamensagem dos Signos Metalinguísticos. . . . 33

4.2.3 Signos Estáticos 33

4.2.4 Reconstrução da Metamensagem dos Signos Estáticos 35

4.2.5 Signos Dinâmicos 35
4.2.6 Reconstrução da Metamensagem dos Signos Dinâmicos 39
4.2.7 Reconstrução da Metamensagem Designer-Usuário 39
4.2.8 Consistência das Metamensagens 40
4.2.9 Resultados 41
4.3 Estudo II: Privacy Badger 43
4.3.1 Signos Metalinguísticos 44
4.3.2 Reconstrução da Metamensagem dos Signos Metalinguísticos 44
4.3.3 Signos Estáticos 49
4.3.4 Reconstrução da Metamensagem dos Signos Estáticos 50
4.3.5 Signos Dinâmicos 50
4.3.6 Reconstrução da Metamensagem dos Signos Dinâmicos 51
4.3.7 Reconstrução da Metamensagem Designer-Usuário 52
4.3.8 Consistência das Metamensagens 53
4.3.9 Resultados 54
4.4 Classes de Signos 55
4.5 Análise Comparativa Entre os Resultados de Estudo 1 e Estudo 2 56
4.6 Estudo 3: Triangulação 58
4.6.1 Convergências 59
4.6.2 Divergências 63

5 Conclusões e Contribuições 65

5.1 Principais Conclusões da Pesquisa 66
5.2 Contribuições 68
5.3 Trabalhos Futuros 68
5.4 Publicações Realizadas 69

Referências **70**

Apêndice A – TERMO DE CONSENTIMENTO **74**

Apêndice B – QUESTIONÁRIO PRÉ-TESTE **75**

Apêndice C – CENÁRIOS E TAREFAS **76**

Apêndice D – QUESTIONÁRIO PÓS-TESTE **77**

Capítulo 1

Introdução

Com a crescente adesão ao uso de redes sociais, as pessoas passaram produzir uma quantidade significativa de dados a seu próprio respeito, despertando o interesse tanto da indústria, quanto da academia em estabelecer metodologias de pesquisa e análises diversas a partir desses dados. Podemos citar, como exemplo, o processamento dos registros de interação nas redes sociais, a fim de identificar e estabelecer padrões do comportamento humano relacionados a hábitos de consumo ou ligados a problemas psicológicos [2, 48, 21, 34, 10, 40]. Isso têm impulsionado também o interesse em identificar oportunidades para gerar novos serviços que permitam, por exemplo, ações personalizadas para clientes, tais como publicidade ou serviços de recomendação [2, 27, 7].

Nesse mesmo cenário, os *smartphones* se tornaram indispensáveis para o cotidiano de muitas pessoas, sendo usados como o principal dispositivo para a realização de atividades, seja profissionais, recreativas, até mesmo como ferramenta para cuidados de saúde, por meio do uso de aplicativos [35]. Esse crescente uso dos *smartphones*, em grande parte como um dos principais meios de acesso a serviços na internet, têm possibilitado novas maneiras de gerar dados sobre o usuário graças aos recursos computacionais embarcados, tais como GPS, bússola, acelerômetro, leitor de digital, RFID, dentre outros. Dessa forma, o crescente interesse no processamento desses dados têm estimulado a aplicação de métodos sofisticados de aprendizado de máquina que permitam extrair inferências sensíveis, como o contexto de uso do usuário, atividades físicas realizadas ou estados emocionais, por exemplo [35, 45]. A presença e o uso contínuo permitem a vinculação dos dados (coletados a partir de sensores embarcados) ao proprietário do dispositivo, de modo que esses dados podem refletir os hábitos, as atividades e as rotinas do seu dono [35].

Tendo em vista a natureza desses desenvolvimentos, portanto, é notório afirmar que

produtos e serviços computacionais estão se tornando mais presentes no cotidiano das pessoas. Inegavelmente, o avanço de tecnologias emergentes, tais como Internet das Coisas (*Internet of Things - IoT*), Computação Ubíqua e Aprendizado de Máquina, têm proporcionando benefícios diversos à sociedade em diferentes aspectos como ganho de agilidade, produtividade e organização, bem como em algumas áreas como saúde e educação. Porém, a disponibilidade irrestrita desses dados (em grande parte, dados pessoais), pode levar a violações de privacidade, riscos legais e de propriedade intelectual, danos à reputação e outras preocupações éticas e sociais.

A área de Interação Humano-Computador (IHC), um subcampo da Ciência da Computação, têm expressado tais preocupações refletindo a necessidade em realizar pesquisas considerando uma dimensão mais abrangente, as quais permitam explorar e compreender os fatores envolvidos no uso de sistemas computacionais baseados nas necessidades de indivíduos em termos de valores humanos [36, 43, 44]. A medida que os dispositivos computacionais foram se desenvolvendo, as contribuições de IHC se pautaram em compreender os fenômenos relacionados no uso dessas tecnologias. Hornung et al. [29] ponderam que, embora essas preocupações não sejam um objeto de pesquisa novo em IHC, é perceptível que tais questões ainda não recebem a importância devida em projetos de sistemas computacionais, mesmo aqueles que apresentem grande impacto social, sugerindo, assim um atraso entre pesquisas e práticas acadêmicas e na indústria.

Em 2012, a comunidade brasileira de pesquisadores em IHC prospectou grandes desafios de pesquisa para IHC no Brasil, no período entre 2012 à 2022 [8], sendo um deles a formulação de iniciativas que atentem para a inclusão de valores humanos em IHC. Em [37], os autores aprofundam as discussões com enfoque nesse desafio sob a perspectiva de temas centrais, como privacidade, ética e *design*, relacionadas à avaliação e uso de tecnologias de computação. Tais iniciativas encontram apoio em outros trabalhos científicos [1, 3, 6] que apresentam uma tendência crescente sobre a percepção do usuário em relação a sua privacidade como um fator-chave que afeta a aceitação e a adoção de novas tecnologias. Além disso, tais preocupações podem ser evidenciadas a partir dos desdobramentos importantes que têm ocorrido em relação à privacidade de dados pessoais, por meio da criação de regulamentações de proteção a dados, tais como *EU General Data Protection Regulation (GDPR)*[1], *California Consumer Privacy Act of 2018 (CCPA)*[2], bem como a brasileira *Lei Geral de Proteção de Dados Pessoais (LGPDP)*[3].

[1] https://eugdpr.org/
[2] https://www.ccpa-2018.com
[3] http://www.planalto.gov.br/ccivil$_0$3/$_A$to2015 − 2018/2018/Lei/L13709.htm

Perante o exposto, observamos a necessidade em se aprofundar sobre a centralidade do papel dos dados neste trabalho. Assim, recorremos à abordagem de Interação Humano-Dados - IHD (do inglês, *Human-Data Interaction - HDI*) em busca de uma perspectiva mais ampla ligada às preocupações sobre a interação de sistemas computacionais (que em grande medida, dar-se por meio do uso de dados pessoais), associadas à importância em considerar valores humanos.

O campo emergente de IHD, com base nas contribuições de Mortier et al. [39], propõe *incluir o humano no centro dos fluxos de dados e fornecer mecanismos para os cidadãos interagirem com esses sistemas e dados explicitamente.* Seu objetivo é viabilizar a compreensão pelo usuário sobre as formas em que e por quem seus dados são utilizados, e como as pessoas podem desejar agir ou influenciar, bem como, idealmente, beneficiar-se dos dados e seu uso.

O enfoque deste trabalho recai sobre a ótica de IHD no contexto de gerenciamento de dados pessoais, mais especificamente em explorar rastros pelos quais projetistas de sistemas interativos utilizam para comunicar aos usuários suas decisões de design, associadas a tais aspectos propostos em IHD. Para isso, adotamos a teoria de Engenharia Semiótica [18] a qual considera, como um caso particular de comunicação, a interação dos seres humanos com interfaces de sistemas computacionais, a fim de orientá-lo na execução de suas tarefas. Em outras palavras, a Engenharia Semiótica é uma teoria explicativa sobre os fenômenos envolvidos em IHC segundo a perspectiva comunicativa (i.e. entre o projetista e o usuário por meio da interface de um sistema interativo) tendo como objetivo investigar e esclarecer a natureza e os aspectos inerentes do processo de design, uso e avaliação nesses sistemas [18].

1.1 Motivação e Definição do Problema

Atualmente, existe uma ampla disponibilidade de aplicativos para apoiar as pessoas em suas tarefas do dia a dia. Ao utilizarmos essas ferramentas, somos capazes, por exemplo, de saber as condições do trânsito em tempo real para obter um caminho mais apropriado, estimar o tempo de chegada do ônibus, descobrir interesses e gostos de um grupo, criar uma conta bancária, monitorar a qualidade da nossa alimentação ou do nosso sono em detalhes. A implementação de algumas tecnologias de aprendizado de máquina, computação ubíqua e internet das coisas têm por objetivo o processamento de dados, em grande parte dados pessoais, possibilitando a criação de novos produtos e serviços computacionais com

o objetivo de viabilizar avanços importantes, por exemplo, na geração de novas formas de diagnóstico precoce de doenças, identificação de padrões de comportamento de pessoas em contextos variados, identificação de hábitos de consumo e monitoramento de pacientes à distância. Assim, a sociedade está se tornando cada vez mais orientada a dados.

Dessa forma, novos desafios emergem a respeito de questões éticas, legais e de responsabilização, transparência no uso de dados, a participação de pessoas por meio da consideração de seus valores, avaliações e decisão. Podemos levantar um exemplo: por quais meios o usuário poderá preservar sua privacidade em quaisquer contextos de uso, de modo a torna-se mais ciente sobre a utilização de serviços a fim de alcançar seus objetivos?

A exposição de casos de violação de privacidade ou de disponibilização indevida de dados pessoais por plataformas de serviços online destacam a deficiência de mecanismos de privacidade e de transparência. Outro grande desafio, por parte dos designers de sistemas, é encontrar orientações claras que lhes permitam implementar soluções que não apenas considerem metas de usabilidade, como facilidade de uso, aprendizado, eficiência e consistência de suas soluções, mas também legislações vigentes, conhecimento cultural, foco no usuário e em seus valores. Por exemplo, um sistema pode ter uma ótima usabilidade, mas ser socialmente rejeitado por não respeitar a privacidade dos usuários ou por não explicar claramente como obtém e usa as informações do usuário. Neste exemplo, se as pessoas não se sentirem seguras ou se sentirem livres para fazer escolhas, as chances de adotar o sistema são mínimas.

Na literatura de computação, existem trabalhos que fomentam a necessidade de pesquisas com enfoque na avaliação ou criação de sistemas interativos que considerem valores humanos [42, 8, 5, 6, 33]. Outros trabalhos [12, 25, 30, 41] propõem diretrizes, requisitos ou recomendações de design gerais ou relacionadas a domínios específicos tais como uso de dispositivos móveis, computação em nuvem e políticas de privacidade, com enfoque em privacidade e transparência. Essas propostas baseiam-se na avaliação de regulamentações de proteção a dados vigentes ou pela declarações de especialistas. Existem trabalhos que propõem recomendações de design, porém específicas de suas ferramentas avaliadas. Em [28], os autores realizam avaliação de design para uma ferramenta de privacidade, mas buscando identificar problemas de usabilidade e propor melhorias. Já em [4], os autores avaliam um conjunto de ferramentas, tendo em vista questões de usabilidade que apoiem a privacidade para os mecanismos utilizados por essas ferramentas.

Ainda existem poucos trabalhos que se utilizam de abordagens, como a de Interação Humano-Dados, que ofereçam uma perspectiva sobre questões de uso de dados pesso-

ais, valores humanos e de privacidade de forma integrada e analítica, em conjunto com teorias de IHC que permitam extrair interpretações, com validade científica, sobre fenômenos interativos envolvendo àquelas questões citadas. Esta problemática, portanto, é um dos principais elementos motivadores para a pesquisa apresentada nesse trabalho, constituindo-se uma das contribuições dessa dissertação.

1.2 Objetivos

Este trabalho tem como objetivo principal avaliar as oportunidades de Interação Humano-Dados no domínio de gerenciamento de dados pessoais, explorando as estratégias comunicativas adotadas pelos projetistas para este fim e compreendendo como se dá a percepção de tal comunicação por parte dos usuários, baseando-se nas compreensões da Engenharia Semiótica a respeito dos fenômenos interativos que ocorrem no processo de IHC.

A partir dos resultados obtidos nesta pesquisa, objetivamos identificar as principais consistências e inconsistências de comunicação dos aspectos de IHD. Para alcançar tais objetivos, definimos as seguintes questões de pesquisa:

QP1) Quais estratégias de comunicação (ECs) que potencialmente viabilizam a Interação Humano-Dados?

QP2) Qual é a relação entre as ECs encontradas na QP1 com os principais conceitos de IHD?

1.3 Metodologia

Para responder nossas questões de pesquisa, conduzimos uma pesquisa qualitativa [14, 22] baseados em conceitos e métodos da Engenharia Semiótica [18]. Utilizamos o Método de Inspeção Semiótica (MIS) para avaliar a comunicabilidade dos conceitos de IHD em duas ferramentas de apoio à transparência, tendo em vista responder às duas questões de pesquisa. Por fim, foi executada a etapa de Triangulação para validar os resultados obtidos pela aplicação do MIS. Esta última etapa foi realizada por meio de testes de observação com a participação de pessoas.

1.4 Organização

Esta dissertação está estruturada da seguinte forma: o Capítulo 2 apresenta o referencial teórico que fundamentou esta pesquisa. O Capítulo 3 apresenta os trabalhos relacionados ao tema da presente dissertação. Na sequência, o Capítulo 4 descreve os estudos empíricos, a metodologia adotada nesta pesquisa, a etapa de triangulação para validação dos resultados encontrados, a resposta para as questões de pesquisa e a síntese dos resultados. Por fim, no Capítulo 5, são apresentadas as conclusões e as oportunidades para trabalhos futuros.

Capítulo 2

Fundamentação Teórica

A pesquisa apresentada nesta dissertação enfatiza a exploração de estratégias de design no processo de comunicação dos conceitos de Interação Humano-Dados (IHD). Além disso, baseia-se na perspectiva da Engenharia Semiótica sobre os fenômenos envolvidos em IHC. Este capítulo, portanto, discorre sobre essas perspectivas e conceitos que permeiam nossas investigações.

2.1 Interação Humano-Dados

A área de Interação Humano-Dados é um campo emergente de estudos, sendo cunhado pela primeira vez em 2011 por Elqmvist [23]. Desde então, observamos que a literatura de IHD têm apresentado contribuições que, embora não sigam um consenso sobre uma definição canônica para IHD, desdobram-se em duas vertentes, as quais citamos:

A primeira vertente, IHD está relacionada à aplicação de aspectos interativos de visualização na exploração (fazer sentido) ou análise (atingir um objetivo) sobre grandes conjuntos de dados complexos e desestruturados. Algumas contribuições se enquadram nessa vertente, dentre as quais citamos: Elqmvist [23] associa IHD com a *manipulação humana, a análise e fazer coesão de sentido de grandes conjuntos de dados complexos e desestruturados*; Cafaro [11] relaciona IHD com a *criação de um contexto para compreensão de grandes conjuntos de dados*; Widjojo et al. [50] entende IHD a partir da *necessidade de envolver os humanos com grandes conjuntos de dados e de fornecer uma experiência de usuário altamente envolvente na exploração de dados*, e define IHD como *a interface interativa entre uma representação visual dos dados*. Dessa forma, essas propostas consideram IHD para o design de visualizações que permitam gerar *insights* sobre grandes volumes de dados analisados.

A segunda vertente, fundamentada pelas propostas de Mortier et al. [39], difere de questões sobre IHC, considerando aspectos ou dimensões mais abrangentes da interação de pessoas com sistemas computacionais que, normalmente, não são abordadas em IHC [49], como o uso ou interação de dados na sociedade em geral [13], além do gerenciamento desses dados em tais sistemas computacionais com enfoque em fatores humanos [39].

Essa última vertente, empregada neste trabalho, está relacionada ao cenário em que o desenvolvimento de tecnologias e serviços de geração, compartilhamento e manipulação de dados têm permitido que as pessoas estejam a todo momento em contato com ferramentas e artefatos digitais para consumo ou produção de informações. Assim, pessoas podem produzir dados tanto de forma consciente (dados de perfil em redes sociais, uso de ferramentas de atividade física, por exemplo), quanto de forma inconsciente (monitoramento de robôs sobre nosso histórico de pesquisas ou *cookies* que armazenam nosso rastro de atividades, por exemplo) [39, 28].

Esses dados podem ser acumulados por diferentes organizações interessadas em inferir sobre questões sensíveis a respeito de nossas vidas (estado de saúde ou emocional, hábitos de consumo ou preferências políticas, por exemplo) [39], de modo que essas diferentes análises possibilitam influenciar o comportamento das pessoas de diversas maneiras [28]. Mortier et al. [39] propõem um modelo que estrutura essa visão de IHD, apresentando os elementos chaves, conforme ilustrado na Figura 2.1.

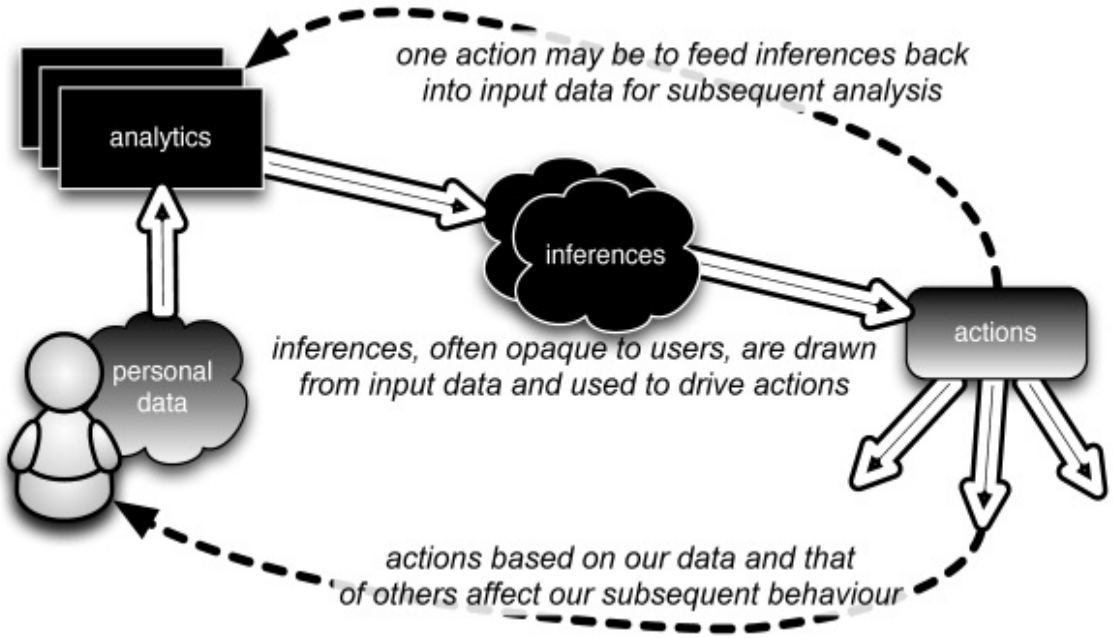


Figura 2.1: Visão de IHD proposto por Mortier et. al. em [39]

Com base nesse modelo, dados pessoais são coletados e analisados com ou sem consentimento prévio (geralmente o usuário participa de forma passiva na disponibilização de seus dados), servindo de *input* para a realização de inferências sobre nós (tais informações ainda opacas para o usuário). As inferências obtidas podem servir tanto para realimentar o sistema para análises posteriores, gerando *loops* de *feedback*, quanto para desencadear ações que influenciem nosso comportamento (por exemplo, sugestão de consumo de produtos específicos). Consequentemente, nosso comportamento subsequente altera os dados que produzimos, sendo novamente coletados, realimentando outro ciclo de análises.

Portanto, buscando tratar as novas questões que emergem a partir dessa percepção, ecossistema de dados pessoais entre diferentes entidades interessadas e de seus impactos nas ações de indivíduos e na sociedade, IHD propõe *colocar o Humano no centro do fluxo de dados e prover mecanismos aos cidadãos para interagirem com esses sistemas de forma explícita* [38, 39], fomentando a participação mais ativa e consciente de usuários nas decisões sobre gerenciamento de seus dados pessoais. Assim, Mortier e colegas defendem que *as pessoas, em última análise, devem ser capazes de utilizar suas informações analisando sua privacidade e, como provedoras de serviço, assumir um controle mais explícito sobre o consumo de seus dados e as informações que fornecem* [26].

Outro campo intimamente relacionado ao de IHD é o estudo da privacidade. Embora IHD seja um campo de estudos distinto, sua abordagem sobrepõe a de privacidade [26]. A privacidade é uma preocupação especial que pode ser levantada aqui com base no que os dados são e como são usados. O IHD é mais amplo e baseia-se na compreensão dos dados disponíveis sobre os indivíduos, as formas e por quem é utilizado e como as pessoas podem desejar e agir para influenciar e, idealmente, beneficiar-se dos dados e seu uso [26].

Mortier e co-autores estabelecem três princípios fundamentais os quais endereçam desafios abordados em Interação Humano-Dados, sendo estes: a Legibilidade, Agência e Negociabilidade [39].

A Legibilidade preocupa-se em tornar a obtenção de dados e os algoritmos analíticos mais transparentes e compreensíveis para os usuários, já que, em geral, as interações com fluxos e processos de dados são muitas vezes obscuras às pessoas.

A Agência visa permitir aos indivíduos meios para gerir seus dados e seu acesso por terceiros, além de buscar formas de atuação eficazes nesses sistemas. Isso não inclui apenas a capacidade de optar por permitir ou cancelar a coleta e processamento de dados, mas de se envolver de forma mais ampla em relação às decisões sobre seus dados, como a modificação dados e de inferências obtidas, armazenamento e acesso.

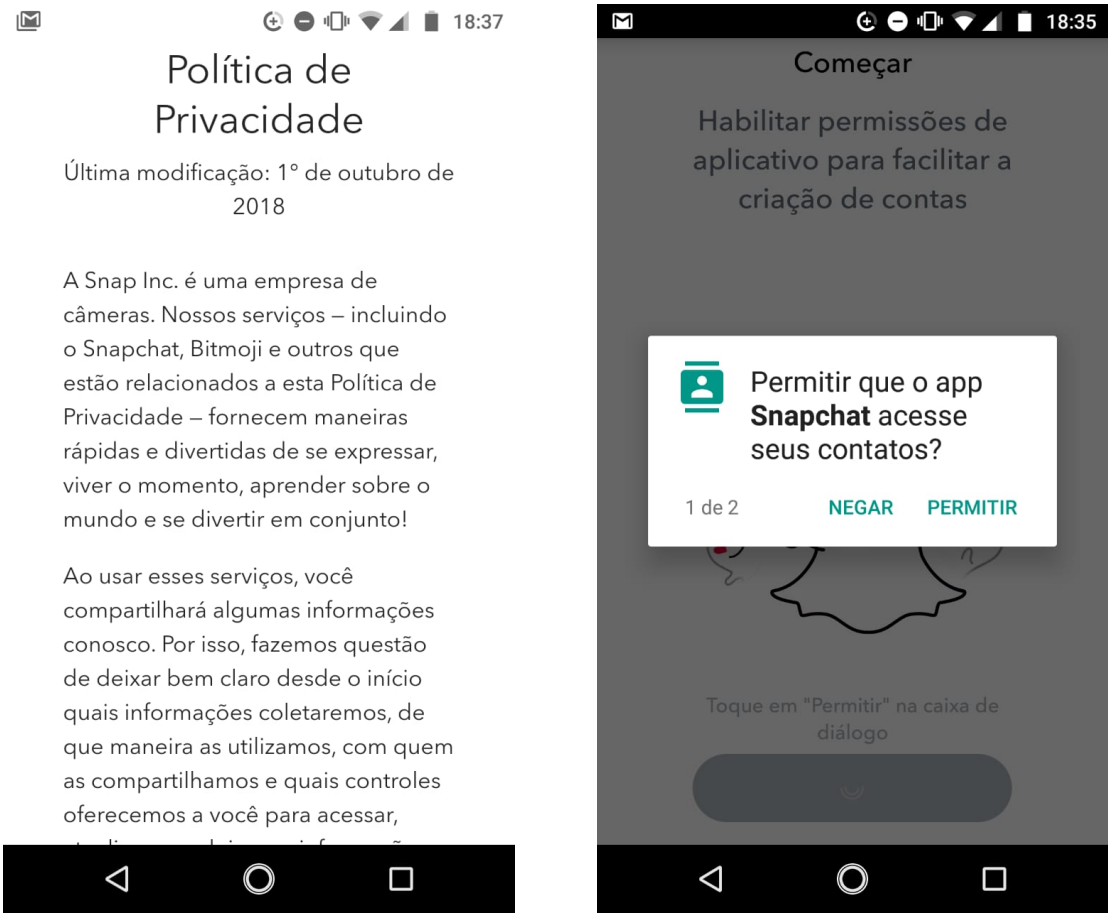
Por fim, a Negociabilidade se refere à re-avaliação de decisões tomadas pelos titulares de dados em relação a manipulação de seus dados, estimulando o seu engajamento de forma contínua. Em IHD, esse conceito se associada como um meio de equilibrar o relacionamento desproporcional de poder dos agregadores de dados sobre o usuário individual.

Para melhor entendimento sobre os conceitos de IHD descritos, refletimos sobre um cenário de uso para exemplificação:

Joana gostaria de conhecer um aplicativo muito utilizado por seus amigos: o *Snapchat*[1]. Para isso, ela recorre a sua loja de aplicativos e realiza a instalação do *App* em seu *smartphone*. Ao começar o procedimento de cadastro, o aplicativo pede para que Joana aceite algumas solicitações de acesso à dados, a fim de facilitar o procedimento de cadastro. Entretanto, desconfiada em permitir tais acessos, Joana opta por negar todas as solicitações, conforme ilustra a Figura 2.2b. Neste ponto, podemos perceber o conceito de Agência a partir da oportunidade dada à Joana em decidir sobre o acesso aos seus dados pessoais. Antes de finalizar o cadastro, Joana deseja consultar as políticas de privacidade do aplicativo em relação ao uso de seus dados pessoais, explorando informações sobre quais dados podem ser coletados, como são utilizados e se há a disponibilização de tais dados à terceiros, conforme ilustra a Figura 2.2a. Ao conseguir obter essas informações, podemos dizer que Joana pôde extrair Legibilidade sobre seus dados pessoais em relação ao Snapchat. Após a utilização do aplicativo durante alguns meses, Joana percebeu que o Snapchat não mais a interessava, e gostaria de excluir sua conta, bem como remover todos os seus dados da plataforma. Entretanto, o aplicativo não oferecia essa opção e Joana apenas o desinstalou de seu *smartphone*. Caso o Snapchat permitisse à Joana que reavaliasse o valor de manter (ou não) seus dados armazenados na plataforma, o aplicativo estaria oferecendo um exemplo de Negociabilidade.

Considerando o exemplo acima, em relação ao que mencionamos no início desse capítulo, enxergamos a necessidade de compreender como o *design* de sistemas computacionais pode permitir aos usuários finais a apropriação clara de tais conceitos de IHD em seu contexto de gerenciamento de dados pessoais no âmbito digital. Para isso, adotamos uma teoria que fundamenta a nossa visão a respeito do design de interfaces e os fenômenos envolvidos em IHC, conforme descrevemos na seção abaixo.

[1]https://www.snapchat.com



(a) Legibilidade (b) Agência

Figura 2.2: Exemplificação de conceitos de IHD no aplicativo *Snapchat*.

2.2 Engenharia Semiótica

A Engenharia Semiótica foi proposta originalmente como uma abordagem para o design de linguagens de interface [15]. Gradativamente, esse campo de estudos foi evoluindo para uma teoria explicativa sobre os fenômenos envolvidos na Interação Humano-Computador segundo uma perspectiva comunicativa, tendo como objetivo investigar e esclarecer a natureza e os aspectos inerentes do processo de design, uso e avaliação de um sistema interativo [46]. Assim, a Engenharia Semiótica define um conjunto de conceitos e propõe métodos que viabilizem tais objetivos.

Segundo a Engenharia Semiótica, um sistema interativo é um artefato intelectual cuja definição é a de um produto gerado a partir da interpretação de um projetista sobre um problema e sua concepção de solução, que é então apresentada em uma codificação linguística [46]. Este artefato só irá atingir o seu objetivo se o usuário for capaz de utilizar o sistema linguístico empregado na interface para decodificar as mensagens enviadas pelo designer, desse modo, estabelecendo um diálogo comunicativo [17].

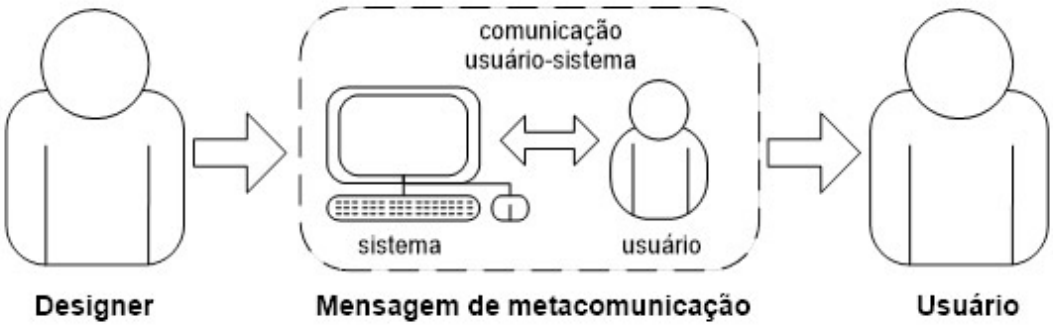


Figura 2.3: Metacomunicação entre Design e Usuário - Adaptado de [46]

A caracterização do diálogo comunicativo pode ser entendida a partir do processo de Interação Humano-Computador que, sob a ótica da Engenharia Semiótica, pode ser considerado como um caso particular de metacomunicação mediada pela interface de um sistema interativo, de modo que os seus projetistas informam suas intenções de design ao usuário a fim de orientá-lo na execução de suas tarefas [18]. Essa comunicação é feita por meio dos diversos elementos de interface e, segundo a Engenharia Semiótica, a interface de um sistema interativo assume o papel de seu representante (o designer) em tempo de interação, constituindo-se, desse modo, como o preposto do designer [9], conforme ilustrado na Figura 2.3. Em outras palavras, a interface de um sistema é uma mensagem do designer para o usuário cujo conteúdo é:

"Esta é a minha interpretação sobre quem você é, o que eu entendi que você quer ou precisa fazer, de que formas prefere fazê-lo e por quê. Eis, portanto, o sistema que consequentemente concebi para você, o qual você pode ou deve usar assim, a fim de realizar uma série de objetivos associados com esta (minha) visão." [16]

A teoria de Engenharia Semiótica é fundamentada na Semiótica, uma disciplina que estuda fenômenos de significação e comunicação, tendo como um dos principais conceitos o de signo. Segundo [17], um signo é tudo aquilo que significa algo para alguém, e possui uma estrutura triádica: Objeto, *Representamen* e Interpretante.

Objeto: é aquilo que signo busca referenciar, sendo a causa e justifica para a existência de um signo.

Representamen: é a representação do signo, que se torna possível pela existência de "algo a representar" (que é o objeto).

Interpretante: refere-se ao processo mental que permite a associação entre o signo e

o seu objeto (significado).

A partir desses conceitos semióticos, a Engenharia Semiótica entende que a Significação é o processo através do qual a expressão e conteúdo de signos são estabelecidos com base em convenções sociais e culturais conhecidas das pessoas que vão utilizá-los, produzindo e interpretando signos [46]. Assim, os processos comunicativos entre usuários e designers são, portanto, sempre únicos, singulares, imprevisíveis. Entretanto, a Engenharia Semiótica se atém ao estudo da metacomunicação através de artefatos baseados em sistemas computacionais e não uma Semiótica geral, para quaisquer signos, naturais ou artificiais [17]. Por isto, estabelece classes de signos envolvidas no processo de significação da IHC: signos metalinguísticos, estáticos e dinâmicos [19].

Os signos metalinguísticos são aqueles usados pelo designer para comunicar explicitamente aos usuários os significados que ele atribuiu para os demais signos codificados na interface e como eles devem ser usados. O sistema de ajuda, mensagens de erro, avisos, diálogos explicativos e dicas são exemplos de signos metalinguísticos.

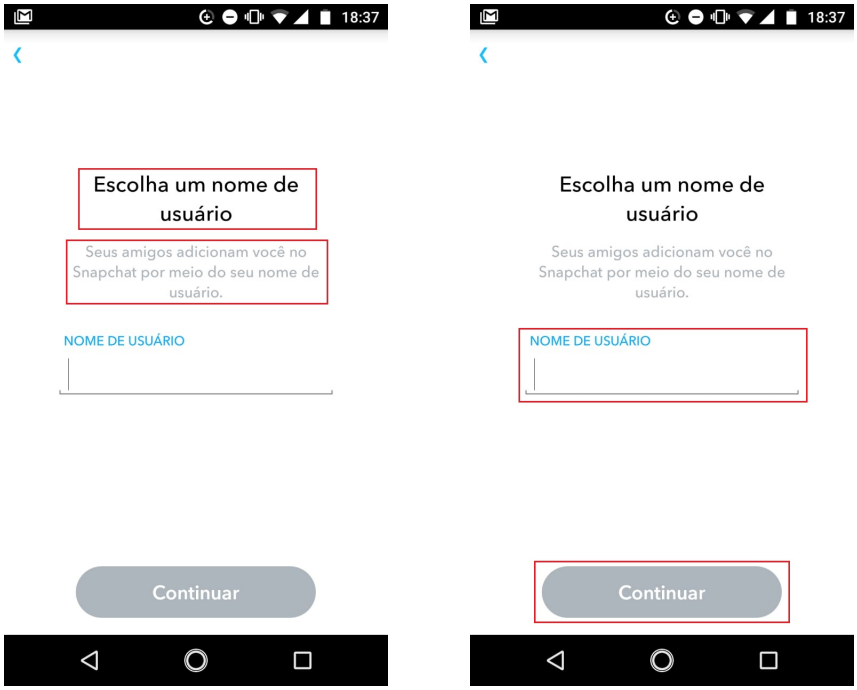
Os signos estáticos, por sua vez, são aqueles cujos significados são interpretados independentemente das relações causais e temporais que permeiam a interação. Assim, sua interpretação é limitada pelos elementos visíveis na interface em um determinado momento [18]. Ou seja, signos estáticos são interpretados na dimensão espacial. Alguns exemplos de signos estáticos são: opções de um menu ou botões em uma barra de ferramentas.

Já os signos dinâmicos, por fim, são aqueles cuja interpretação está sujeita às relações causais e temporais, ou seja, a interação em si. A sua identificação é mais sutil, pois não há necessariamente um elemento visível que o represente. Por exemplo, a relação causal entre a seleção de um botão na barra de ferramentas e o diálogo que se segue a esta ação é um signo dinâmico, que só pode ser identificado com a interação [18]. Os signos dinâmicos devem ser interpretados na dimensão temporal.

Para melhor compreensão dos conceitos mencionados até aqui, tomemos como exemplo algumas telas que foram exibidas à Joana durante o seu processo de cadastro no Snapchat. Primeiramente, podemos apontar como signos metalinguísticos o título e o subtítulo, já que estes explicam o que o usuário deve inserir, bem como sobre a finalidade do campo *'Nome de Usuário'*, conforme ilustra a Figura 2.4a. Já com relação aos signos estáticos, podemos destacar o próprio campo *'Nome de Usuário'* e o botão *'Continuar'*, conforme mostra a Figura 2.4b . Por fim, os exemplos de signos dinâmicos presentes na interface são o *loader* acompanhado da palavra *'Verificando'*, que surge em resposta ao ato de digitar no campo *'Nome do Usuário'*, bem como a mensagem em vermelho *'Nome já está*

sendo usado!', que é exibida como resposta do *App* em relação a indisponibilidade de uso para o nome digitado. Os *'Nomes de Usuário Sugeridos'* também são signos dinâmicos e aparecem como alternativas disponíveis para uso, similares ao que foi digitado. As Figuras 2.5a, 2.5b, 2.5c ilustram os signos dinâmicos, resultantes da sequência de interações nessa interface.

Em relação a este último signo, o seu Objeto é a alternativa disponível de *'Nome de Usuário'*. Seu *Representamen* é o *'Nomes de Usuário Sugeridos'* como sendo sua representação. Por fim, seu Interpretante consideramos como sendo a percepção de similaridade entre o que foi digitado e o que foi sugerido, que neste caso é o primeiro nome do usuário e uma sequência numérica, o que pode permitir ao usuário compreender as variações válidas de *'Nome de Usuário'* que podem ser escolhidas.

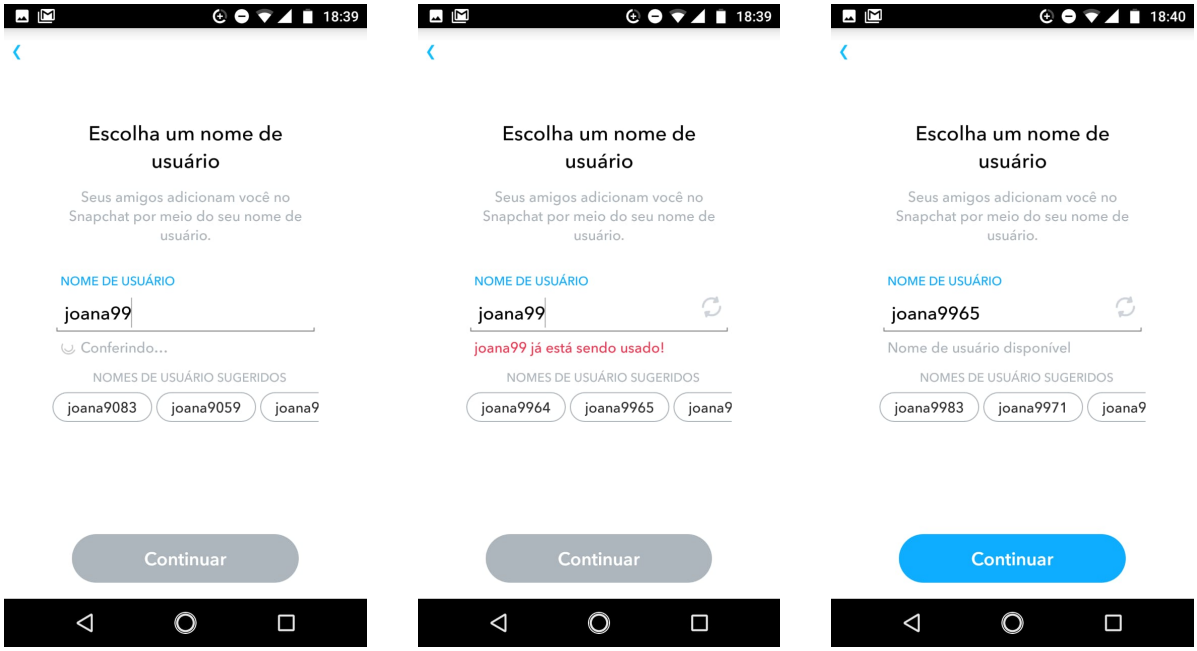


(a) Metalinguísticos (b) Estáticos

Figura 2.4: Exemplos de signos no aplicativo *Snapchat*.

O propósito das classes de signos utilizadas é fornecer ao projetista subsídios para analisar a natureza, a estrutura, o processo, os efeitos e as condições em que a comunicação, mediada por artefatos computacionais, ocorre entre o designer e o usuário [17].

Do ponto de vista da Engenharia Semiótica, o conteúdo da mensagem elaborada pelo designer deve ser não ambíguo e compreensível para que usuário tenha condições de realizar seus objetivos ao receber a mensagem. Portanto, a Comunicabilidade é um dos principais fatores de qualidade de um sistema interativo, sendo a propriedade de um sistema interativo transmitir ao usuário, de forma eficaz e eficiente, as intenções e



(a) Após digitação no campo *Nome do Usuário*

(b) Após a verificação da disponibilidade do nome digitado

(c) Após a escolha de um *Nome de Usuário Sugerido*.

Figura 2.5: Exemplos de signos dinâmicos no aplicativo *Snapchat*.

princípios de interação que guiaram o seu *design*, fomentando o uso criativo, eficiente e produtivo da aplicação.

2.3 Método de Inspeção Semiótica

O Método de Inspeção Semiótica (MIS) [20] é um método de avaliação qualitativa em IHC, baseado na Engenharia Semiótica [16]. Com este método, os avaliadores podem analisar a comunicabilidade dos artefatos interativos [20], sem o envolvimento de usuários, permitindo avaliar a qualidade da emissão da metacomunicação do designer através da interface do sistema. Assim, o foco do MIS é inspecionar a metacomunicação do designer para usuário com o objetivo de identificar possíveis rupturas na comunicação. Primeiramente, na etapa de preparação, são definidos o foco de avaliação, o perfil do usuário e o cenário de inspeção. No processo de avaliação, o avaliador examina a interface e classifica os signos como metalinguístico, estático ou dinâmico, seguindo a proposta de classes de signos da Engenharia Semiótica.

Os signos metalinguísticos são os primeiros a serem analisados, uma vez que expressam e explicam outras partes da metacomunicação do designer. Na sequência, os signos estáticos são analisados, considerando apenas os elementos de interface apresentados em cada tela em um instante de tempo, sem examinar o comportamento do sistema, nem as

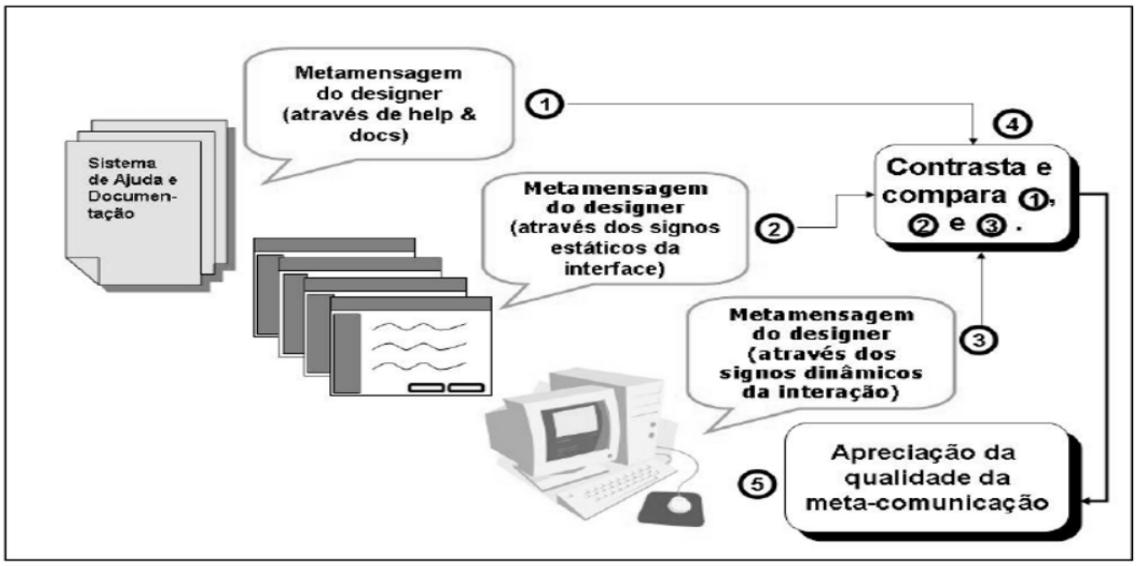


Figura 2.6: Visão geral do Método de Inspeção Semiótica - Adaptado de [46]

relações temporais e causais entre elementos de interface [19]. Por fim, a inspeção dos signos dinâmicos exige que, na análise, o avaliador inspecione o processo de interação que o usuário pode experimentar através da interface. Esses signos são percebidos através de mudanças na interface que comunicam ao usuário o comportamento do sistema como resultado de ações do usuário (clicando no mouse, pressionando enter, alterando o foco de um campo de formulário para outro, etc.) por eventos externos (recebendo *email*, a conexão à Internet falha, etc.) ou ao longo do tempo.

Para inspecionar a interface, o MIS propõe 5 etapas a serem seguidas pelo avaliador [47]. Nas três primeiras etapas, o principal objetivo é reconstruir a metacomunicação do designer, usando o seguinte modelo da metacomunicação do designer [47] para cada categoria de signos (metalinguística, estática e dinâmica): *"Aqui está a minha compreensão, de quem você são, o que eu aprendi que você quer ou precisa fazer, em que maneiras preferidas e por quê. Este é o sistema que eu, portanto, criei para você, e é assim que você pode ou deve usá-lo para atender a uma variedade de propósitos que se enquadram nesta versão"*.

As etapas de inspeção são:

Passo 1: inspeção de signos metalinguísticos. Nesta fase, o avaliador explora o documentação e sistema de ajuda.
Passo 2: inspeção de signos estáticos. Nesta fase, o avaliador inspeciona os signos estáticos da interface.

Passo 3: Inspeção de signos dinâmicos. Nesta fase, o avaliador inspeciona os signos que emergem da interação.
Passo 4: Nesta fase, o avaliador contrasta e compara a metacomunicação das etapas 1, 2 e 3 e registra as possíveis interpretações problemáticas que podem ocorrer no tempo de interação pelos usuários.
Passo 5: Apreciando a qualidade da metacomunicação, nesta etapa, o avaliador produz um relatório contendo os problemas de comunicabilidade encontrados, que podem frustrar ou impedir que o usuário compreenda a mensagem pretendida pelo designer, afetando sua produtividade. Neste método, o avaliador é o "advogado" do usuário, isto é, ele se põe no papel do usuário e o representa interagindo com o sistema a fim de representá-lo. A Figura 2.6 ilustra as etapas do MIS.

O MIS pode ser aplicado para fins técnicos ou científicos. Quando usado para fins de pesquisa, um passo deve ser acrescentado à sua execução: a triangulação dos resultados [18].

A triangulação visa gerar diferentes perspectivas sobre a questão de estudo, checando a consistência entre elas, e não sua homogeneidade e replicabilidade. O produto da triangulação, quando consistente, é um conjunto de significados e categorias interpretativas capazes de gerar uma compreensão profunda do contexto pesquisado e, além disso, um *framework* interpretativo que pode ser (re)aplicado em outros contextos de investigação [46].

Segundo [18], existem dois tipos de triangulação: Endógena e Exógena. Na triangulação Endógena, realiza-se a comparação dos resultados gerados pela aplicação, por um mesmo pesquisador, de diferentes métodos para analisar o mesmo problema de estudo, isto é, o domínio e a questão de estudo são estáveis, havendo a variação do método ou do sujeito que o executa. Um exemplo deste tipo de triangulação é a validação dos resultados coletados pela aplicação do MIS, comparando-os com os resultados de um conjunto de entrevistas com usuários [46]. A triangulação Exógena ocorre quando o mesmo método é aplicado em domínios distintos para a análise comparativa de seus resultados. Neste caso, o problema e o método de investigação são estáveis, variando o domínio no qual é aplicado [46].

Capítulo 3

Trabalhos Relacionados

Este capítulo descreve os trabalhos selecionados por apresentarem a mesma temática de nosso estudo, servindo de base para o amadurecimento desta dissertação e verificando as principais lacunas encontradas na literatura referentes ao presente tema. A análise destes trabalhos permitiu identificação de aspectos, sob do ponto de vista de outros autores, relativos a compreensão do envolvimento de usuários no exercício do controle da privacidade sobre seus dados em face ao cenário de extração e manipulação de dados por parte de entidades interessadas.

Para fins de organização, definimos duas categorias para apresentação dos trabalhos relacionados, sendo estas: (i) estudos que realizam avaliações de usabilidade em ferramentas no contexto de privacidade; (ii) estudos que realizam discussões teóricas sobre problemas de privacidade em sistemas computacionais, bem como propõem diretrizes para o amadurecimento de propostas de privacidade centradas no usuário.

3.1 Estudos com Foco na Usabilidade

Em [32], os autores realizaram estudos sobre uma ferramenta denominada *DataTrack*. O objetivo dessa ferramenta é fornecer uma ampla visualização ao usuário geral sobre seus dados pessoais que foram disponibilizados à provedores de serviços, bem como tornar claro como esses dados foram processados. Assim, um aspecto primordial é permitir que o usuário seja capaz de navegar pelos seus dados e compreender como estes estão sendo utilizados. Tendo isso em vista, os autores definiram 6 questões de pesquisas a serem respondidas por meio de avaliações de usabilidade com a participação de pessoas. Para capturar todas as considerações dos participantes a respeito dos elementos de interface do DataTrack, os avaliadores priorizaram a coleta de comentários verbais ao longo de toda a

interação. Outras formas de coleta de dados foram utilizadas, tais como questionário pré-teste, entrevista semi-estruturada, questionário pós-teste e capturas de tela. Anotações sobre dificuldades percebidas e reações dos participantes no ato da interação também foram registradas por um observador.

Os resultados apontados mostram que os usuários, de modo geral, não conseguiram entender claramente o significado de alguns conceitos relacionados, por exemplo, às possibilidades de ações sobre os dados, como a "Portabilidade de dados", ou ainda compreender em quais situações em que a Portabilidade seria útil. Além disso, questões sobre segurança e privacidade de dados pessoais, importação e exportação (ou a transferência) de dados de/para diferentes serviços geraram dúvidas sobre onde, como e por quem os dados são acessados e controlados. Os autores também constataram que, de modo geral, apesar de muitos provedores de serviços, tais como o *Google*, *Facebook* e *Linkedn* fornecerem certa transparência e mecanismos de controle, as pessoas raramente têm ciência ou se utilizam desses mecanismos para exercerem seus direitos. Dessa forma, os autores concluem que faz-se necessário o aperfeiçoamento de mecanismos de transparência, controle e portabilidade de dados, de modo a serem usufruídos de forma eficaz e permitam ao usuário alcançar seus objetivos.

Em [4], os autores apresentam um conjunto de estudos que abordam questões relacionadas à privacidade no contexto *mobile*, tendo como principal objetivo avaliar a qualidade da usabilidade (com foco em privacidade) em aplicativos de proteção à dados pessoais, identificando possíveis problemas e gerar recomendações de *design* para melhoria no uso e adoção de tais ferramentas. Tais avaliações foram conduzidas por meio de estudos com usuários e especialistas, baseado-se nos princípios de *Whitten and Tygar's*.

Os autores selecionaram as ferramentas *ChatSecure*, *ObscureCam* e dois aplicativos de *proxy* baseado na rede *Tor*: o *Orbot* e *ProxyMob*. O ChatSecure permite criptografar a conversa entre dois usuários usando o algoritmo OTR (*Off-the-Record*). O ObscureCam visa agregar maior segurança no compartilhamento de imagem e vídeos, removendo dados identificadores tais como localização e informações sobre o dispositivo do usuário. Por fim, o Orbot e ProxyMob permitem que os dispositivos móveis acessem a rede Tor.

O resultado das avaliações de usabilidade mostram que os aplicativos não fornecem orientação adequada para que os usuários concluam suas tarefas planejadas, às vezes levando a erros. Além disso, as interfaces dos aplicativos foram consideradas pouco intuitivas, não apresentando detalhes apropriados, além de fazer uso de terminologias complexas. Por fim, muitos usuários não puderam determinar se suas ações foram bem-sucedidas, carac-

terizando a falta de *feedback* adequado de suas ações realizadas. Assim, tais problemas afetam a capacidade dos usuários de compreenderem os estados da aplicação em tempo de interação, podendo causar enganos ao usuário quanto à sua utilização dos recursos de forma apropriada e segura.

Além dos estudos de avaliação de interfaces, os autores agregam uma visão abrangente sobre os fatores relacionados à percepção, preferências e hábitos de usuários em relação à privacidade, por meio da realização de um *survey*, com a participação de 258 pessoas. Os resultados mostram que 83% dos entrevistados estão preocupados com a privacidade de suas informações pessoais em dispositivos móveis, sendo 72% os que de fato tomam medidas para preservarem sua privacidade sem o auxílio de aplicativos de terceiros para este fim. As medidas mais comuns adotadas pelos participantes para proteger sua privacidade em seus dispositivos móveis são bloquear o dispositivo (73%), excluir o histórico de navegação (56%) e atentar as permissões antes da instalação de aplicativos (53%). Os participantes também responderam sobre a probabilidade de instalar um aplicativo de proteção à privacidade em seus dispositivos móveis e 77% deles disseram que tinham um grande interesse de fazê-lo. No entanto, menos de 20% dos participantes relataram ter usado tais aplicativos. Por fim, o *survey* permitiu que os participantes classificassem a importância de algumas características em aplicativos de proteção à privacidade, sendo a facilidade de uso, a facilidade de aprendizado e a facilidade de compreensão sobre o *status* de proteção tidas como as mais importantes.

3.2 Estudos com Abordagens Teóricas, Requisitos de Design e/ou Diretrizes

Em [25], os autores apresentam questões relacionadas ao processamento de dados em nuvem à luz de regulamentações como a *EU General Data Protection Regulation (GDPR)*[1], bem como o importância das ferramentas de apoio à transparência no suporte ao usuário no controle de seus dados pessoais registrados em serviços *online*. Para isso, foi realizado um *workshop* para identificar problemas encontrados por usuários finais relativos às políticas de privacidade e ao direito de exercer o controle sobre seus dados, dentre os quais, destacam-se: (i) pouca clareza sobre a definição da responsabilidade de provedores de serviços em nuvem; (ii) dificuldades para identificar formas de reparação dos danos causados por problemas de manipulação de dados pessoais e as leis aplicáveis; (iii) encerramento de contrato, deleção ou transferência dos dados para outro servidor, mesmo sendo os donos

[1] https://eugdpr.org/

de seus dados. De modo geral, questões relativas à privacidade são frequentemente ilegíveis e de difícil compreensão para as pessoas, de modo que conceitos de IHC adequados devem ser escolhidos para tornar essas questões facilmente perceptíveis e compreensíveis. Por fim, os autores propuseram requisitos de privacidade e transparência, derivados a partir dos resultados obtidos no *workshop* e de análises dos princípios legais de privacidade, baseados na legislação GDPR, com foco na transparência e responsabilização de serviços em nuvem, dentre os quais, destacam-se: (1) Exibição de informações pertinentes ao processamento de dados pessoais aos seus donos, a partir do momento em que tais dados sejam alvos de coleta ou de processamento. Estas informações são: a identidade de entidades interessadas, suas propostas e objetivos de manipulação de dados, bem como seus destinatários. (2) Os donos de dados também devem obter informações sobre períodos de retenção de dados, bem como o nível de proteção de dados de um país terceiro ou organização internacional para o qual o responsável pelo processamento deseja transferir os dados. (3) Uso de de políticas de privacidade que apresente informações padrões, as quais citam-se: tempo mínimo para cada propósito específico de processamento, a intenção de utilizar os dados pessoais para outros fins, além daqueles para os quais foram coletados (caso exista tal pretensão), bem como se há o interesse na divulgação ou venda de dados a terceiros comerciais.

Ainda no âmbito dos provedores de serviços em nuvem, em [30] os autores exploram o conceito de prestação de contas (*Accountability*) em relação ao tratamento de dados pessoais e confidenciais na nuvem. Os autores consideram que uma organização responsável é transparente ao tornar suas políticas de proteção de dados conhecidas pelas partes interessadas, demonstrando como elas são implementadas, fornecendo notificações apropriadas em caso de violação de alguma política, além de respostas adequadas às solicitações de acesso dos titulares de dados. Partindo dessas considerações, os autores propõem um conjunto de requisitos de transparência, os quais foram elicitados por meio de entrevistas realizadas com voluntários especialistas da área de Segurança da Informação que atuam em projetos de sistemas em nuvem. As questões levantadas buscaram identificar requisitos que permitissem considerar, por exemplo, quais informações mais importantes que devem ser apresentadas ao usuário, o envolvimento do usuário na tomada de decisões e os aspectos que contribuem para o aumento da confiabilidade em relação à segurança de dados.

Em [41], os autores exploram técnicas de IHC que possibilitem a criação de Políticas de Privacidade com foco na melhoria da aplicação de aspectos da compreensão do usuário e de usabilidade. Assim, os autores, primeiramente, analisam e discutem fatores que afe-

tam a confiança do usuário sobre um sistema em relação ao gerenciamento da privacidade. Frequentemente, os usuários precisam compartilhar informações pessoais para acessar os serviços *online*, entretanto, o objetivo desse armazenamento nem sempre fica claro, trazendo à tona algumas indagações, tais como se as informações são ou não criptografadas, quem possui acesso às informações, o tempo de armazenamento se é indefinidamente ou por um período de tempo especificado. Além das preocupações com o armazenamento, outros questionamentos levantados por usuários abrangem o monitoramento de atividades realizados pelo usuário e a disponibilização e uso de tais dados por terceiros.

De outro lado, as políticas de privacidade, por vezes, também são incoerentes com os mecanismos de gerenciamento da privacidade, de modo que os usuários não possuem controle sobre o compartilhamento de seus dados à outras entidades. Os selos de privacidade não garantem a transparência da política de privacidade de um site, e os propósitos para os quais as empresas utilizam dados pessoais não são adequadamente comunicados aos usuários.

Esses fatores permitem a extração de alguns pontos chave que podem ajudar na maturidade relacionada a manipulação de dados pessoais, dentre as quais, citam-se: (i) prática e política de armazenamento do cliente, (ii) prática e política de manipulação de dados, (iii) acessibilidade e legibilidade do documento de privacidade, (iv) oportunidade de personalização das configurações de privacidade do usuário.

Tendo essas declarações em vista, a criação de políticas de privacidade deve prezar pela transparência de todas as considerações complexas ao uso de dados, sem abrir mão de meios para viabilizar a facilidade de compreensão por parte dos usuários. Assim, os autores defendem a incorporação de metodologias de *design*, técnicas de análise e fatores humanos, por parte dos projetistas, para melhorar a acessibilidade das políticas de privacidade. As metodologias de *design*, baseadas na literatura de IHC, como *Design* Interativo, *Design* Centrado no Usuário e *Design* Participativo, podem ser úteis na criação de controles de privacidade mais eficazes e tornar as políticas de privacidade mais compreensíveis ao usuário, de modo que podem permitir a extração de informações sobre as necessidades e habilidades dos usuários, dentre outras.

Em [12], os autores também defendem que interfaces de usuário eficazes são essenciais para a incorporação da privacidade e, por isso, a aplicação de princípios de *design* UI/UX (*User Interface/User eXperience*) à experiência de privacidade do usuário representa um importante campo de pesquisa. A partir dessa motivação, os autores apresentam um estudo que explora questões de design da privacidade no contexto móvel, destacando como

as escolhas de UI/UX podem afetar a transparência e a confiabilidade. Com isso, o estudo busca adaptar alguns princípios gerais, tais como Consciência (*Awareness*), Descoberta (*Discoverability*) e Compreensão (*Comprehension*), sob a ótica de UI/UX, estendendo-os no campo da privacidade móvel para, em última análise, sugerir *insights* para apoiar a solução de tais problemas.

No campo da Consciência, o objetivo é trazer ao usuário o entendimento sobre os efeitos de suas ações relacionadas à sua privacidade. De modo geral, a ideia é oferecer aos usuários a oportunidade de realizar escolhas de privacidade no momento em que estiverem realizando uma ação que envolva suas informações pessoais. Esse tipo de comunicação em processo esclarece o alcance efetivo de suas escolha e respectivas implicações, funcionando como um suplemento para adicionar significado às decisões que já possam ter sido estabelecidas em outras experiências, ou sob os termos gerais da política de privacidade.

Pensar como um usuário ao projetar experiências de privacidade também levantará questões sobre por quanto tempo uma permissão permanece em vigor, uma vez que tenha sido concedida. Segundo os estudos apresentados, considerando o contexto mobile, os consumidores, geralmente não tinham certeza, por exemplo, se concordavam em fornecer seus dados de localização apenas uma vez ou de forma contínua, embora tais dados estivessem disponíveis para os seus aplicativos. Portanto, é essencial que a linguagem usada para explicar proposições de valor e obter permissões seja clara e concisa, sem assumir que o usuário tenha conhecimento profundo de como uma aplicação ou função funciona.

A conscientização também pode ser viabilizada através de opções de design que destaquem as informações mais essenciais. Uma consideração importante na abordagem de tais exercícios de design é se o foco está na informação (explicando as políticas de privacidade) ou na ação (permitindo que os usuários façam escolhas de privacidade).

No campo da Descoberta, o objetivo é considerar a facilidade de acesso às políticas de privacidade pertinentes, bem como às opções de configuração de privacidade.

Ainda no contexto móvel, por exemplo, exigir excessiva rolagem ou toque frustram os usuários que tentam acessar informações e / ou opções. O mesmo pode ser verdade para ícones desconhecidos ou inconsistentes, o que podem provocar a desorientação do usuário. Uma opção de *design* que permite atenuar esse problema é o emprego de auxílios de navegação. Um exemplo prático é o uso de *jump links*, que podem ajudar a orientação e a capacitação dos usuários que acessam páginas e documentos mais longos. A sinalização em documentos para ajudar na orientação, complementada por sugestões de opções orientadas para a ação, quando apropriado, é uma prática recomendada para textos legais ou de

privacidade obrigatórios. Por fim, estratégias de *design* para dar destaque a um conteúdo importante ou para sinalizar a atualização de termos de uso aos usuários, por exemplo, por meio da manipulação de cores ou pelo emprego de mensagens de alertas podem ser eficazes para proporcionar a melhoria na aplicação do aspecto de descoberta.

No campo da compreensão, o objetivo é considerar se o entendimento que os termos de uso e os mecanismos de privacidade desejam comunicar realmente fazem sentido ao usuário. Tendo em vista que termos de consentimento longos e legalistas tendem a desencorajar usuários, busca-se propiciar formas comunicativas que transmitam transparência em relação às práticas realizadas com os dados disponibilizados pelos usuários, que por sua vez, façam um consentimento verdadeiramente ciente, bem como outras decisões sobre privacidade.

Uma abordagem para isso é comunicar as informações essenciais sobre privacidade. Outra abordagem possível é a utilização de avisos "em camadas", que fornecem subconjuntos curtos de informações sobre as políticas (uma classificação em tópicos de interesse, por exemplo), por meio de navegação simples, opção para detalhar sobre áreas mais específicas e questões para mais informações.

Uma das formas de implementação da abordagem em camada é o conceito de um Centro de Privacidade, que já é adotado por empresas como a Google e o Yahoo, dentre outras. De modo geral, esse conceito reúne informações sobre políticas de privacidade em relação aos produtos e serviços disponibilizados, como sendo um balcão único em que o usuário aprende sobre como seus dados são utilizados, bem como editar suas preferências de configuração. O *design* é fortemente centrado na interação do usuário, de modo que a estrutura de navegação (ícones, *labels*, botões, ajuda, dentre outros) define as expectativas e a compreensão dos usuários sobre como se envolver com o volume inevitável de informações e recursos disponibilizados - tais informações que seriam demais para qualquer usuário consumir de uma só vez. Assim, o processo iterativo relacionado ao bom *design* também pode ajudar a melhorar a abordagem das divulgações baseadas em texto.

Por fim, outro ponto que ajuda na melhoria da compreensão do usuário é o emprego adequado de terminologias. É preciso considerar que nem sempre se deve presumir que termos como 'domínios de terceiros' ou 'local atual' sejam claros aos usuários e em seus contextos locais da mesma maneira. Portanto, o uso de uma linguagem clara é essencial. Em termos de interação,por exemplo, o uso consistente de ícones também pode ser útil para introduzir ou comunicar um novo conceito ao usuário.

3.3 Consideração Sobre os Trabalhos Relacionados

Os trabalhos descritos na seção 3.1 apresentam avaliações de *design* com a participação de pessoas, permitindo compreender os problemas que interferem na aceitabilidade, facilidade de aprendizagem, eficiência e satisfação do usuário, tendo com resultado, sugestões de melhorias de *design*. Em [32] o estudo é direcionado a tratar desses aspectos relacionados à uma ferramenta em específico. Já em [4], a avaliação desses aspectos é centrada na privacidade, baseadas em um conjunto de ferramentas mobile de contexto de uso diferentes. Além disso, essas considerações são derivadas unicamente a partir do foco na qualidade de usabilidade, limitando-se realizar considerações de *design* específicas para cada ferramenta.

Em relação aos trabalhos apresentados na seção 3.2, são apresentados amplas discussões teóricas sobre problemas relativos aos diferentes aspectos satélites à privacidade de usuários em sistemas de computação, tais como confiabilidade e transparência, extraídos a partir do foco no usuário em sua interação nos contextos de computação em nuvem, políticas de privacidade e no contexto móvel. A partir desses pontos, esses trabalhos apresentam diretrizes ou abordagens, i.e., requisitos e recomendações gerais ou específicas de *design* à luz de regulamentações de proteção à privacidade vigentes ou pela declarações de especialistas, tendo em vista o amadurecimento das propostas de privacidade centradas no usuário. Entretanto, suas considerações de privacidade não são baseadas em teorias, nem suas contribuições acompanhadas de validações científicas.

O presente trabalho, por sua vez, se propõe a explorar questões de *design* em uma perspectiva mais ampla, integrando questões sobre o uso de dados pessoais, valores humanos e de privacidade por meio dos conceitos propostos em Interação Humano-Dados. A partir das compreensões de IHD, este trabalho investiga os rastros da adoção desses conceitos em ferramentas no contexto de gerenciamento de dados pessoais. Para isso, utiliza-se metodologias de avaliação com foco na comunicabilidade (e não na usabilidade), baseadas em uma teoria de IHC, Engenharia Semiótica, que considera os fenômenos de interação como um caso de metacomunicação entre Designer e Usuário através de um sistema. Tendo em vista a validade científica dos resultados obtidos, foi realizada uma etapa de validação.

Capítulo 4

Estudos Empíricos

Este capítulo descreve as etapas realizadas para a execução dos estudos empíricos desenvolvidos nesta dissertação. Portanto, na seção 4.1 apresentamos a metodologia adotada nesses estudos. As seções 4.2 e 4.3 apresentam os estudos e seus respectivos resultados. A seção 4.4 apresenta as classes de signos. Na sequência, a seção 4.5 apresenta uma análise comparativa entre os resultados obtidos nos dois estudos anteriores. Por fim, a etapa de Triangulação, i.e. validação dos resultados, é apresentada na seção 4.6.

4.1 Metodologia

A metodologia empregada neste trabalho tem como base a aplicação do Método de Inspeção Semiótica (MIS) para fins científicos, com o foco na avaliação da Comunicabilidade, considerando os conceitos propostos em Interação Humano-Dados (IHD). As inspeções foram realizadas por dois avaliadores em conjunto, sendo um avaliador de nível júnior e um avaliador de nível sênior (especialista). O avaliador júnior foi responsável pela execução do MIS em ambas as ferramentas e o avaliador especialista foi responsável por depurar a inspeção realizada pelo avaliador júnior, a fim de asseverar os resultados obtidos.

Na etapa de Preparação, conforme o MIS, procedemos com a definição do objetivo das inspeções, a escolha dos sistemas a serem avaliados, a avaliação informal nos sistemas escolhidos, além da identificação do perfil dos usuários e descrição do cenário de inspeção para os sistemas escolhidos.

Durante o processo de escolha dos sistemas, recorremos à literatura de Ferramentas de Apoio à Transparência (do inglês, *Transparency Enhancing Tools - TETs*), a fim de descobrir ferramentas existentes relacionadas ao domínio de gerenciamento de dados pessoais.

Avaliando as ferramentas elencadas em *surveys* [24, 31], identificamos que muitas delas não recebem atualizações há alguns anos, sendo o caso de *PrivacyBird, Firesheep, Adnostic, MyTrackingChoices, AdReveal*, o que pode sinalizar a descontinuidade de tais sistemas. Outras ferramentas se atém a um caráter informativo, não considerando a participação do usuário, sendo o caso de *Collusion ou Lightbeam*. Dentre as ferramentas restantes, considerando sua abrangência em termos quantidade de usuários atendidos, documentação (i.e, descrições detalhadas sobre o que é e como a ferramenta funciona, mecanismos de controle empregados), histórico recente de atualizações de sistema, disponibilização de recursos e funcionalidades com foco na participação do usuário no gerenciamento de seus dados pessoais, optamos por duas ferramentas, a saber: *Google MyActivity*[1] e *Privacy Badger*[2]. O Google MyActivity é uma ferramenta de transparência que permite a revisão, de forma cronológica, de todo o histórico de atividades realizadas pelo usuário em que algum dos produtos e serviços da Google estejam envolvidos. A ferramenta oferece formas de controle ao usuário, sendo possível deletar tais registros, por exemplo. Além disso, o MyActivity, vinculado ao *Google MyAccount*, permite que o usuário opte por ter ou não suas atividades monitoradas e registradas nos servidores da Google. O Privacy Badger é um *Add-on* para navegadores criado pela *Electronic Frontier Foundation*, e tem como objetivo bloquear o rastreamento não autorizado de domínios de terceiros sobre a navegação do usuário. Assim, é possível gerenciar os rastreadores e demais serviços que coletam dados durante o acesso de *sites*.

A inspeção informal, na sequência, teve como objetivo identificar os trechos dessas ferramentas potencialmente mais relevantes para esta pesquisa, i.e, um conjunto de elementos e funcionalidades relacionados ao domínio de gerenciamento de dados pessoais. Em seguida, procedemos com a definição do perfil de usuário para ambos os sistemas, com base no entendimento de que "as pessoas, de modo geral, podem ser movidas a exercer o controle de seus dados não de forma contínua ou detalhada, mas de forma esporádica, por curiosidade ou em resposta ao potencial ou risco percebido inerente à manipulação de seus dados pessoais" [39]. Além disso, IHD fomenta que seus princípios possam ser apropriados por qualquer pessoa a fim de engajá-las nas decisões sobre o uso de seus dados, respeitando os objetivos a serem almejados por cada um [39]. A partir da definição do perfil de usuário, um cenário de inspeção foi descrito para cada ferramenta, tendo em vista os trechos-alvos a serem avaliados durante a etapa de Execução. Assim, uma persona foi criada de modo a condensar o perfil de usuário e os cenários de inspeção, a fim de servir

[1] myactivity.google.com, acessado em Jan/2018
[2] www.eff.org/privacybadger, versão 2017.11.20, acessado em Jan/2018

como um guia para as inspeções durante a etapa de Execução.

Não há registros de que essas ferramentas foram concebidas baseadas nos conceitos que nós adotamos como fundamentos de IHD. Para isso, formulamos duas questões de pesquisa, conforme descrevemos a seguir:

(QP1) Quais estratégias de comunicação (ECs) que potencialmente viabilizam a Interação Humano-Dados?

(QP2) Qual é a relação entre as ECs encontradas na QP1 com os principais conceitos de IHD propostos por Mortier et al. [39], i.e. Legibilidade, Agência e Negociabilidade?

Ao final da etapa de Preparação, procedemos com a execução da etapa de Execução para ambos os sistemas escolhidos, culminando no desenvolvimento de dois estudos de avaliação, os quais denominamos como Estudo 1 (seção 3.2) e Estudo 2 (seção 3.3). Nesta etapa, realizamos a inspeção dos signos metalinguísticos, estáticos e dinâmicos, considerando apenas os elementos de interface que apresentassem algum aspecto relacionado aos três conceitos de IHD propostos por Mortier et al.[39]. Em seguida, realizamos a reconstrução da meta-mensagem de cada tipo de signo, além da comparação e contraste entre elas. Por fim, chegou-se ao entendimento sobre quem era o usuário e seus interesses, ao passo que também foi possível caracterizar a intenção de comunicação relacionada a cada elemento de interface. Dessa forma, identificamos possíveis estratégias comunicativas e traçamos um paralelo com os conceitos de IHD por meio daquelas questões de pesquisa apresentadas no início desta seção.

Com os dois estudos realizados, o próximo passo foi comparar minuciosamente ambos os resultados e identificar categorias em comum e divergentes, buscando conhecer as estratégias comunicativas adotadas pelos mesmos sistemas, relacionadas aos três principais conceitos de IHD.

Por fim, para validar cientificamente a pesquisa qualitativa realizada nos Estudo 1 e Estudo 2, realizamos a triangulação endógena (Estudo 3), considerando a participação de pessoas por meio de entrevistas. Os participantes foram recrutados de forma aleatória e aceitaram o convite para participar dos testes, totalizando 5 voluntários. Os participantes, até então, não tinham conhecimento sobre IHD ou de TETs, mas expressaram certa preocupação com sua privacidade ao utilizar sistemas computacionais.

A triangulação foi executada respeitando as seguintes etapas: Primeiramente, um termo de consentimento (ver Apêndice A) foi entregue e assinado pelo participante antes do início do teste. Dado o aceite, o participante preencheu um questionário pré-teste (ver

Apêndice B) e, na sequência, uma apresentação sobre os fundamentos de IHD foi realizada a fim de tornar o participante ciente sobre tais conceitos necessários para a realização do teste. Após essas etapas, o teste foi aplicado por meio de tarefas (ver Apêndice C) a serem realizadas utilizando as mesmas TETs avaliadas em Estudo 1 e Estudo 2 (MyActivity e Privacy Badger), nessa ordem. Uma persona (ver Apêndice C) foi utilizada para gerar empatia por parte do participante com o objetivo almejado pelo teste. Ao término do teste, os participantes foram entrevistados, com base em um questionário pós-teste (ver Apêndice D), sobre as tarefas realizadas. O áudio do participante foi registrado ao longo de todo o teste e entrevista, permitindo gerar dados empíricos sobre percepção pelos usuários quanto aos fundamentos de IHD comunicados pela interface das TETs utilizadas. Por fim, foram identificadas e destacadas convergências e divergências a partir da análise dos dados obtidos nos discursos de cada participante.

4.2 Estudo I: My Activity

Ao longo desta seção, será apresentado o primeiro estudo exploratório desta pesquisa, com o detalhamento dos procedimentos adotados e os resultados encontrados.

O objetivo deste estudo foi o de identificar de que maneiras o MyActivity comunica os conceitos de IHD através de seus elementos de interface e, também, quais os conceitos de IHD propostos por Mortier et al.[39] estão envolvidos nessa comunicação. Um cenário de inspeção foi elaborado para guiar tal inspeção, conforme apresentado a seguir:

"*Ane realiza várias tarefas pelo smartphone. Todos os dias, ela acessa o noticiário, redes sociais, realiza pesquisas de interesse profissional e pessoal e busca encontrar o melhor caminho no trânsito. Ane sempre optou em permitir disponibilizar seus dados pessoais aos seus aplicativos e serviços provenientes de grandes empresas como a Google. Com isso, Ane busca experimentar uma navegação baseada nos seus gostos, interesses e em tipos de conteúdo consumido, evitando assim, receber notificações ou conteúdo desnecessários. Recentemente, Ane foi notificada pelo Google a conhecer sua ferramenta de gerenciamento de dados, o MyActivity. Segundo a proposta do MyActivity, Ane descobriu que pode gerenciar os serviços da empresa de modo que estes sejam mais úteis. Ane ficou surpresa em saber que pode exercer controle sobre seus dados ou atividades realizadas por meio do seu smartphone. Dessa forma, Ane ao acessar o Google MyActivity, quer realizar as seguintes tarefas: (1) Descobrir que tipos de dados estão sendo armazenados ou monitorados pela Google, ao utilizar seus produtos ou serviços.; (2) Deseja exercer alguma intervenção na*

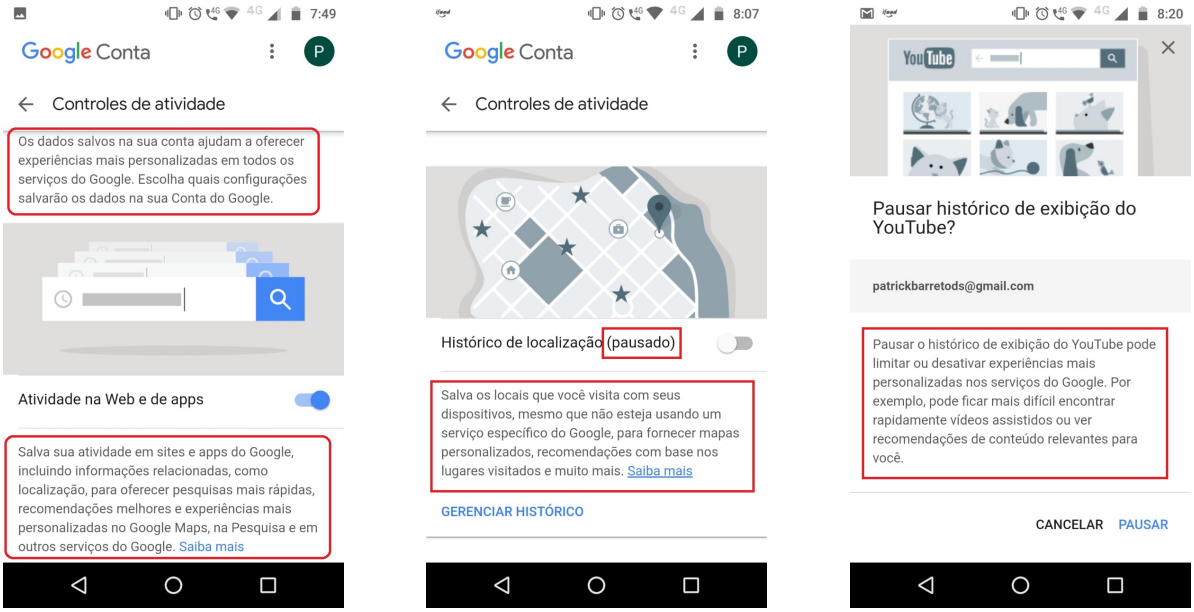
disponibilização e acesso aos seus dados."

A inspeção foi realizada de acordo com as tarefas apresentadas no cenário de inspeção acima e o seu resultado foi organizado de acordo com a classificação de signos, i.e., em Metalinguísticos, Estáticos e Dinâmicos. A seguir, serão apresentados os principais signos encontrados e que estão relacionados aos conceitos de IHD, bem como suas interpretações, de acordo com o entendimento dos avaliadores, sobre a intenção do designer.

4.2.1 Signos Metalinguísticos

Primeiramente, o usuário recorre ao menu de principal para conhecer as opções que o MyActivity oferece. Assim, ao acessar a seção de *'Controles de atividades'*, o designer apresenta ao usuário, inicialmente, uma explicação sobre a finalidade do uso de seus dados, bem como sobre a possibilidade de realizar ações sobre configurações de armazenamento de seus dados. O designer também informa o que será monitorado e quais tipos de dados serão obtidos, complementando a explicação dada anteriormente. Em ambos os casos, o designer utiliza signos metalinguísticos, conforme ilustra a Figura 4.1a.

Na mesma interface, o designer busca reforçar o conteúdo de sua mensagem em vários momentos. A Figura 4.1b, por exemplo, ilustra o uso do signo metalinguístico *'pausado'*, reforçando ao usuário que tal configuração se encontra *'desabilitada'*, como tal é informado



(a) (b) (c)

Figura 4.1: Exemplos de signos metalinguísticos na seção de *'Controle de atividade'* do MyActivity.

pelo botão à sua direita. Ao clicar nesse botão, seja para *'Habilitar'* ou para *'Pausar'* a coleta de dados sobre suas atividades, o designer se utiliza de avisos para acrescentar novas explicações sobre possíveis implicações de tal ação, esforçando-se para tornar esse entendimento claro por meio de exemplos, conforme ilustra a Figura 4.1c, caracterizando um signo metalinguístico. Essa estrutura comunicativa se repete para cada tipo de atividade informados. Além disso, a opção *'Saiba mais'* está disponível em todas as atividades para esclarecer possíveis dúvidas sobre as explicações apresentadas pelo designer, por meio de signos metalinguísticos que fornecem informações mais detalhadas. Assim, o designer sinaliza o seu esforço em se comunicar de forma mais clara ao usuário, buscando diminuir possíveis rupturas comunicativas. A Figura 4.2 ilustra esse esforço por meio de informações detalhadas sobre uma atividade registrada.

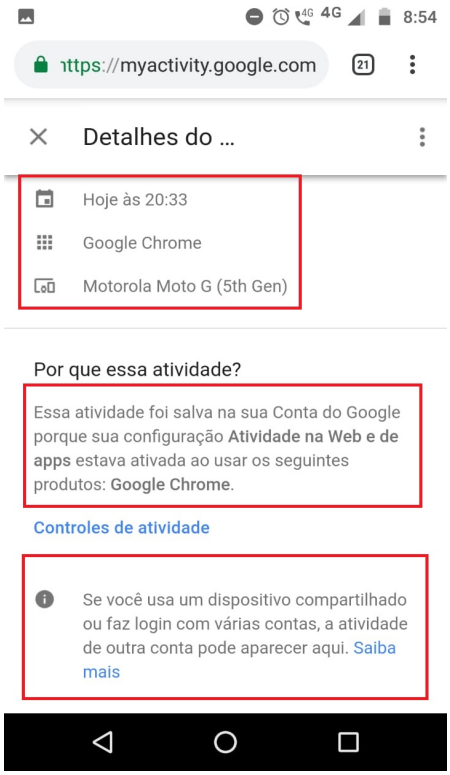


Figura 4.2: Designer apresentando informações mais detalhadas, por meio de signos metalinguísticos.

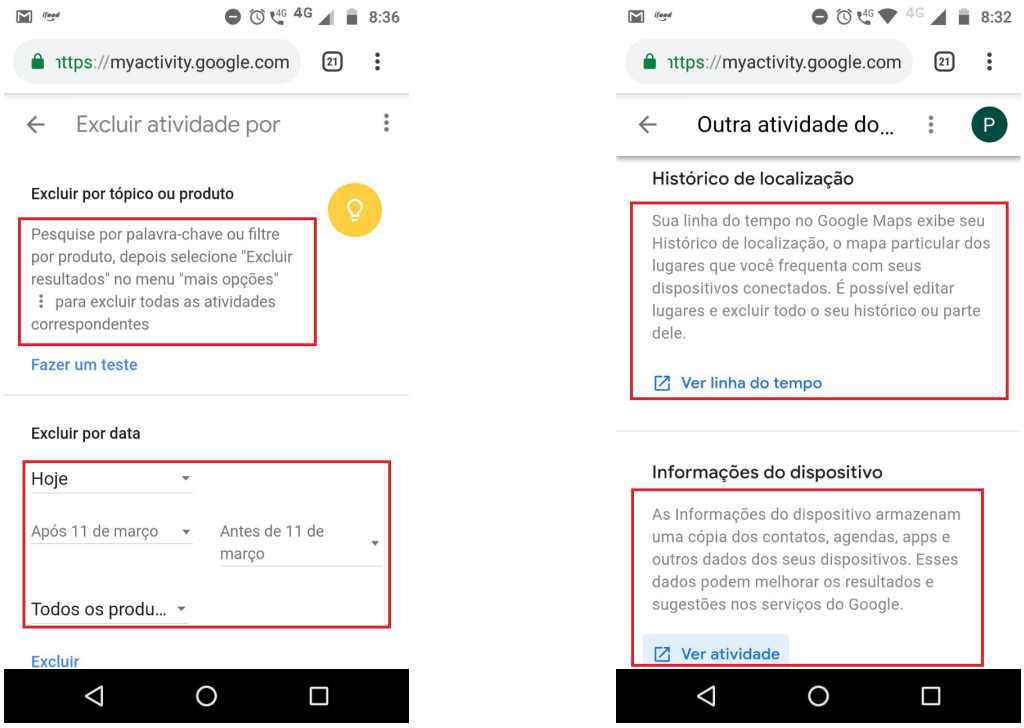
Na seção de *'Ajuda'*, o designer descreve as funcionalidades existentes no MyActivity bem como informações sobre o monitoramento de atividades do usuário. As Figuras 4.3a e 4.3b apresentam exemplos de signos utilizados nessa seção do MyActivity.

Na seção *'Excluir atividade por'*, o designer apresenta algumas opções de filtros que permitem selecionar os registros de interesse do usuário a fim de excluí-los. Tais opções são explicadas por meio do signos metalinguísticos ilustrados na Figura 4.4a, que informam

ao usuário como utilizar as opções oferecidas.

(a) (b)

Figura 4.3: Exemplos de signos metalinguísticos identificados na seção de *'Ajuda'* do MyActivity.



(a) (b)

Figura 4.4: Signos metalinguísticos em seções diversas do MyActivity.

Por fim, na seção *'Outra atividade do Google'*, o designer busca oferecer um panorama abrangente sobre os tipos de atividades que são monitoradas e ações que o usuário pode realizar sobre o que foi registrado sobre as mesmas. Para isso, o designer faz uso de signos metalinguísticos conforme ilustra a Figura 4.4b.

4.2.2 Reconstrução da Metamensagem dos Signos Metalinguísticos.

Com base na identificação dos signos metalinguísticos, faremos a reconstrução da metamensagem do designer para o usuário:

Você, usuário, é uma pessoa que se preocupa com seus dados pessoais ou o que pode ser visto sobre você. Você é um usuário que deseja ter confiança na hospedagem onde suas informações estão armazenadas, buscando informações a esse respeito. Por outro lado, pelo fato de ser um usuário que frequentemente utiliza alguns serviços como *Youtube* e *Google Maps*, busca entender como tirar proveito para obter uma experiência mais útil e eficaz desses serviços, por meio do monitoramento consciente de suas atividades.

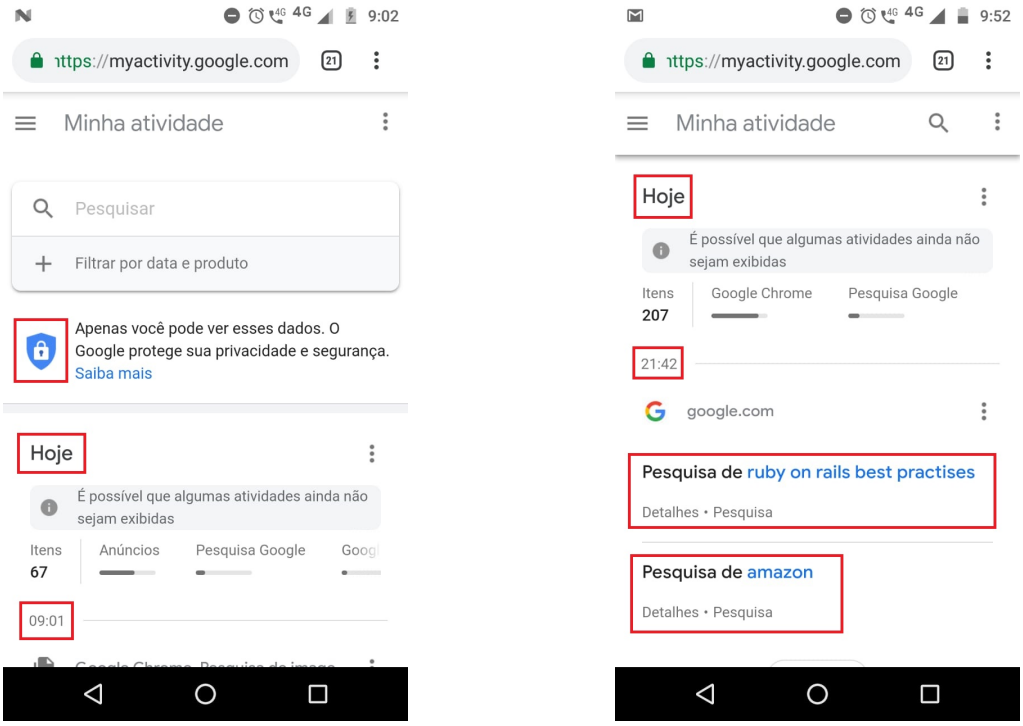
Você, usuário, quer ou precisa ver quais são os tipos de atividades monitoradas pelo Google, acessar detalhes de uma atividade e decidir quais atividades serão armazenadas/coletadas pela empresa. Você também quer controlar atividades em sua conta, optando por excluir ou por permitir (ou não) que alguns tipos de atividade sejam registrados.

Você prefere consultar suas atividades fazendo uso de filtros por período de tempo ou por tipo de serviço utilizado, e também de uma classificação que o ajudará a se manter mais organizado ao revisar suas atividades, sendo esta classificação por itens ou por pacotes. Mas se contenta em visualizar todas as atividades em ordem cronológica inversa.

4.2.3 Signos Estáticos

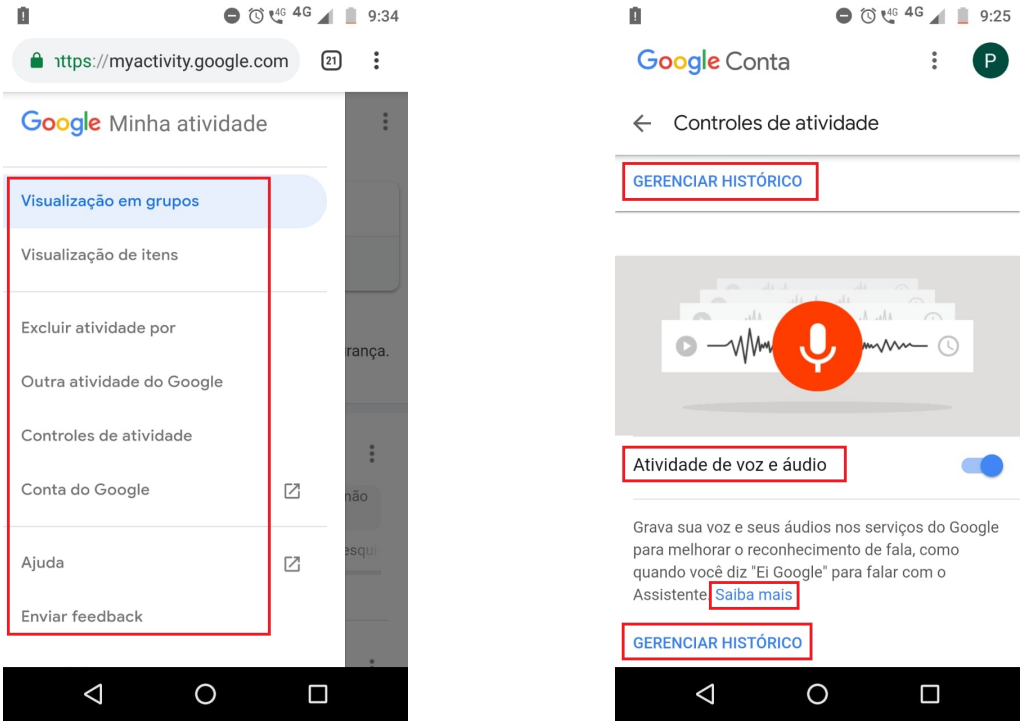
Na tela inicial, o designer se utiliza de signos estáticos para comunicar confiabilidade e proteção das informações exibidas ao usuário. Para isso, o designer apresenta um ícone *'cadeado fechado a frente de um escudo'* para remeter a ideia de restrição de acesso. O designer também apresenta alguns atributos relevantes ao que foi registrado sobre a atividade do usuário, como datas, horários, conteúdo acessado, o produto ou serviço da Google que foi utilizado, além de opções como *'Detalhes'* e *'Saiba mais'*. Assim, percebe-se que o designer objetiva comunicar transparência sobre aquilo que o usuário realizou enquanto utilizava tais serviços. As Figuras 4.5a e 4.5b ilustram os exemplos de signos

estáticos utilizados nessa comunicação.



(a) (b)

Figura 4.5: Exemplos de signos estáticos identificados na tela inicial.



(a) No Menu Principal (b) Em Registro Específico

Figura 4.6: Exemplos de signos estáticos identificados, no menu principal e na seção de *'Controles de atividade'*.

Ainda na tela Inicial, o designer oferece algumas ações que podem ser realizadas pelo usuário, como *'Controle de atividades'* ou *'Excluir atividades'*, por meio do seu menu principal, conforme ilustrado na Figura 4.6a.

Na seção de *'Controles de atividade'*, o designer informa ao usuário quais são os tipos de atividades que podem ser monitoradas, bem como possibilidade de gerenciar o seu histórico de atividades registradas. Em caso de dúvidas, o designer acrescenta uma abertura para descrição mais detalhada pelo link *'Saiba mais'*. A Figura 4.6b ilustra os signos estáticos usados nessa comunicação.

4.2.4 Reconstrução da Metamensagem dos Signos Estáticos

Com base na identificação dos signos estáticos, faremos a reconstrução da metamensagem do designer para o usuário:

Você, usuário, entende o conceito de 'atividade' no contexto da aplicação, portanto possui algum conhecimento sobre formas de interagir com serviços e produtos da internet. Deseja revisar seu histórico de atividades realizadas (assistiu, pesquisou ou visitou alguma determinada página de serviço ou produto).

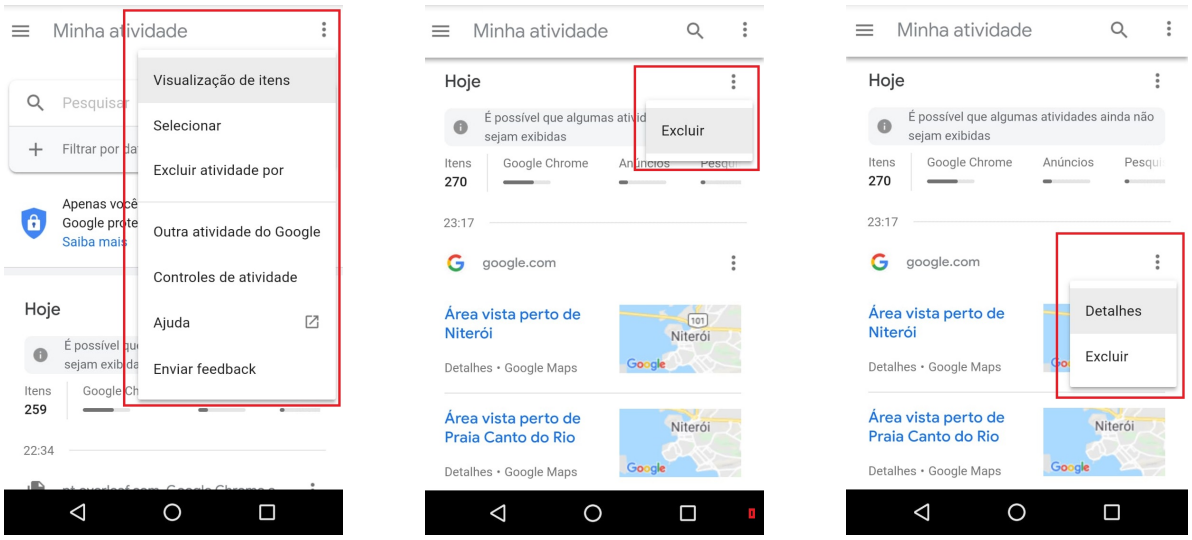
Você, usuário, quer ou precisa acessar suas atividade, controlar quais tipos de atividades o Google pode ou não monitorar/armazenar. Além disso, quer revisar seu histórico de atividades realizadas e ter a possibilidade de excluir tais atividades.

Você prefere visualizar algumas atividades rapidamente, em uma lista em ordem cronológica inversa (da mais recente para a mais antiga), categorizada por serviços ou produtos, conferindo detalhes caso tenha maior interesse em alguma atividade em específico. Além disso, prefere categorizações por data, por serviço ou produto acessado, podendo optar por visualizar todas as atividades relativos a uma data, serviço ou produto. Para gerenciar os tipos de atividades que o Google pode monitorar, prefere uma lista com todas as atividades possíveis e uma opção de *'Habilitar'* ou *'Desabilitar'* tal monitoramento. Prefere optar por excluir atividades por período de data e/ou tipo de produto.

4.2.5 Signos Dinâmicos

Para apresentar ações que podem ser realizadas pelo usuário, o designer se utiliza de vários signos dinâmicos. No primeiro exemplo, o designer apresenta o signo de *'três pontos na vertical'* o qual denota a existência de um conjunto de opções que podem ser diferentes

a medida que é acessado em contextos de aplicação distintos. Por exemplo, a Figura 4.7a mostra o signo sendo aplicado no contexto do menu principal, apresentando várias opções, como *'Excluir atividade por'* e *'Enviar feedback'*. A Figura 4.7b mostra o mesmo signo sendo aplicado no contexto relacionado a todos os registros do dia em questão, com apenas a opção *'Excluir'*. Por fim, a Figura 4.7c mostra o signo no contexto relacionado a um registro específico, com as opções *'Detalhes'* e *'Excluir'*.



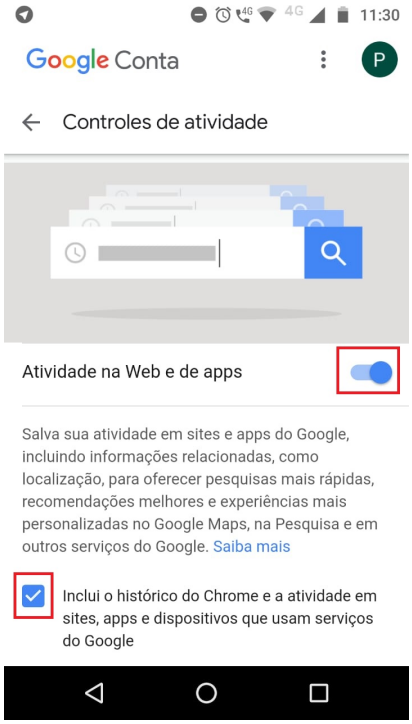
(a) No Menu Principal (b) Em Registros do Dia (c) Em Registro Específico

Figura 4.7: Exemplos de signos dinâmicos identificados na interface inicial e seus contextos de aplicação.

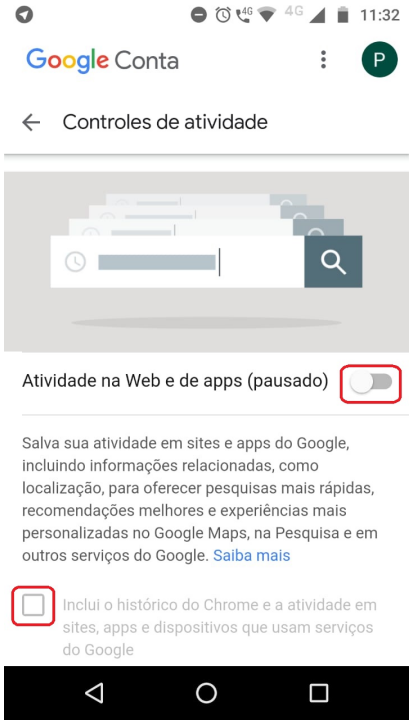
Na seção *'Controle de atividade'*, o designer aplica signos dinâmicos para comunicar ao usuário sobre ações importantes, tal como a de *'Habilitar'* ou *'Pausar'* o monitoramento de atividades. Neste caso, *switch buttons* e *checkbox* que ao serem marcados ou desmarcados, refletem nas interações ilustradas nas Figuras 4.8a e 4.8b, respectivamente. O resultado dessas ações pode ser reforçado pelo uso da mesma imagem em escala de cinza (Figura 4.8d) ou colorida (Figura 4.8c), o que evidencia a preocupação do designer em manter uma comunicação clara a respeito do uso (ou não) de dados pessoais relacionadas ao tipo de atividade em questão. Essa preocupação também é percebida pelo fato do designer emitir um aviso, alertando sobre os efeitos de tal ação antes da sua finalização. Além disso, tal ação só poderá ser concluída quando o usuário observar todo o conteúdo explicativo dado pelo designer. As Figuras 4.9a, 4.9b e 4.9c ilustram um exemplo de aviso e da interação que ocorre ao clicar sobre o botão *'Pausar'*. Dessa forma, as Figuras 4.8a, 4.9a, 4.9b, 4.9c e 4.8b ilustram um exemplo de interação com objetivo de pausar um monitoramento.

Outro exemplo em que o designer utiliza avisos ao realizar uma ação, é durante a exclusão de um registro de atividade. Neste caso, as Figuras 4.10a e 4.10b ilustram os

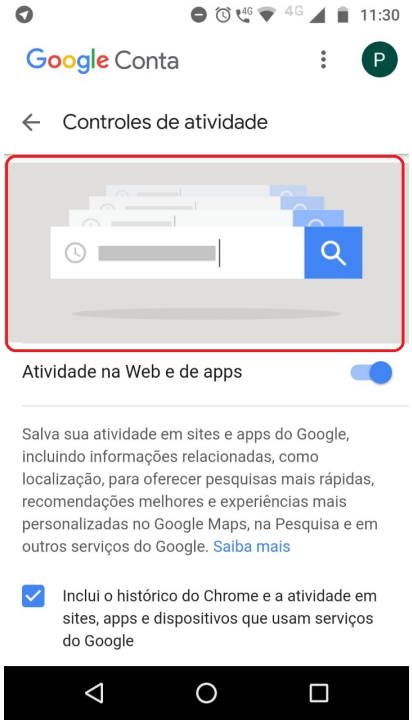
signos dinâmicos usados. Assim como no exemplo anterior, o designer apresenta as opções somente ao final do texto explicativo, de modo que o usuário precise 'rolar' completamente



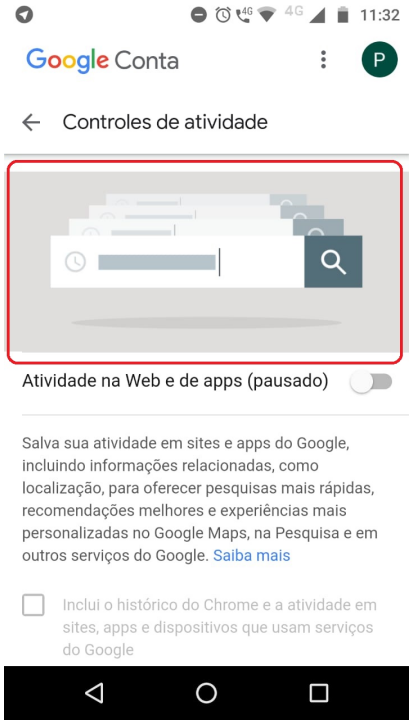
(a) Opções selecionadas



(b) Opções não selecionadas



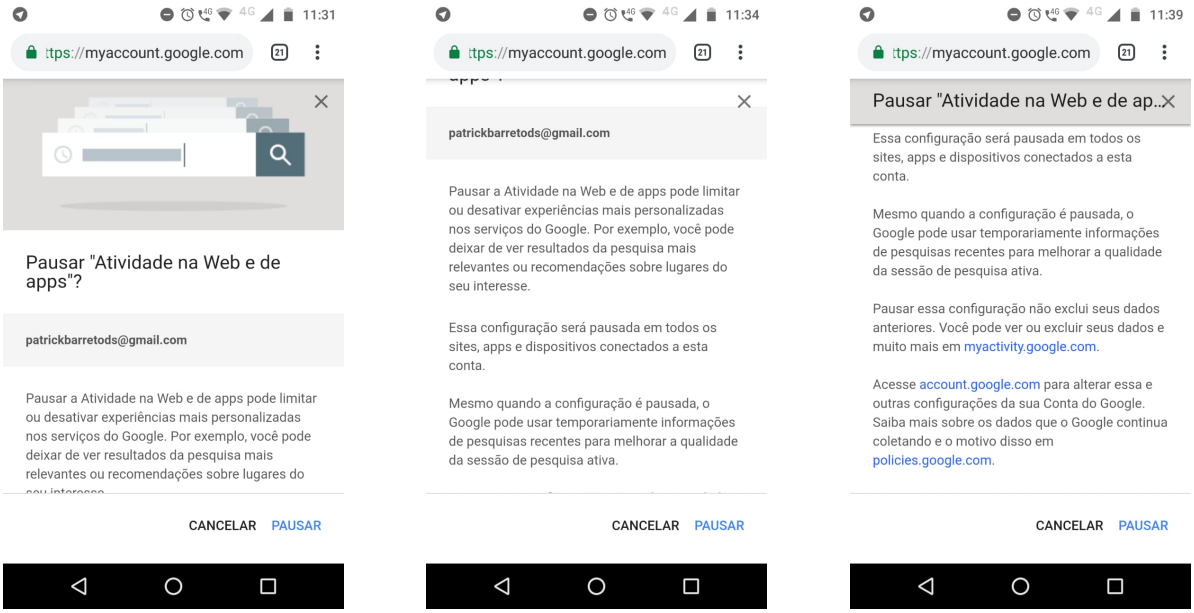
(c) Signo que sinaliza monitoramento ativado



(d) Signo que sinaliza monitoramento pausado

Figura 4.8: Exemplo de interação com signos dinâmicos identificados na seção de *'Controles de atividade'*.

o referido texto para acessar tais opções, caracterizando outro exemplo de signo dinâmico.

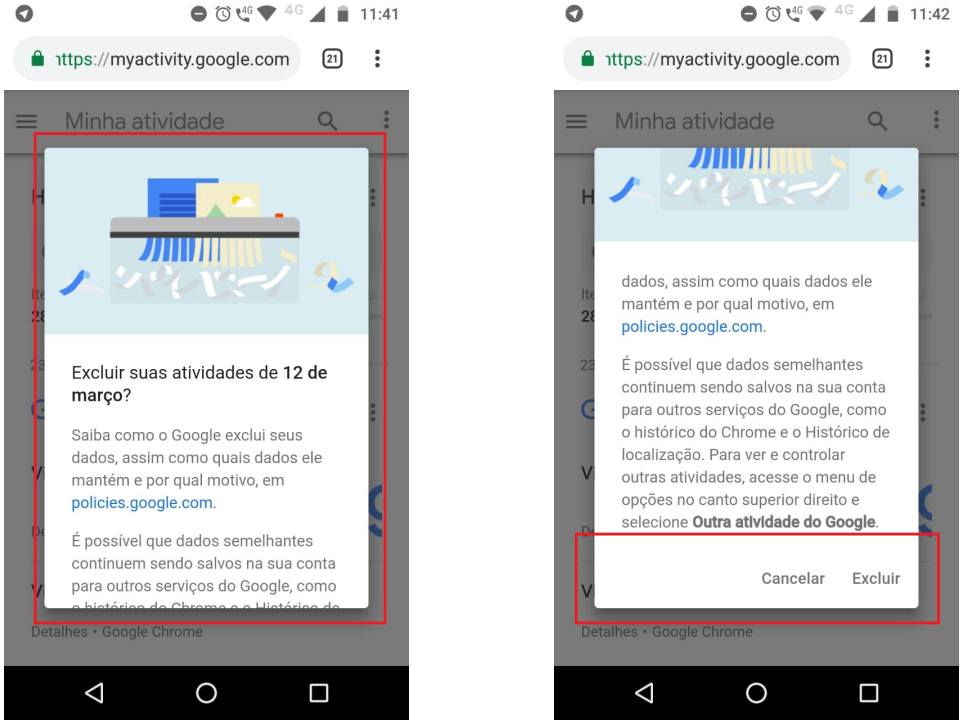


(a) Interação inicial ao acessar o aviso.

(b) Interação após o primeiro clique em *'Pausar'*

(c) Interação após o segundo clique em *'Pausar'*

Figura 4.9: Signo de aviso e resultado de suas interações.



(a) Interação Inicial

(b) Interação Final

Figura 4.10: Exemplo de signo de aviso ao excluir um registro de atividade.

4.2.6 Reconstrução da Metamensagem dos Signos Dinâmicos

Com base na identificação dos signos dinâmicos, faremos a reconstrução da metamensagem do designer para o usuário:

Você, usuário, é uma pessoa que usará o MyActivity provavelmente em dispositivos móveis, em um contexto variado ou não. É um usuário com experiência intermediária em navegação ou interfaces móveis.

Você, usuário, quer ou precisa consultar e excluir e intervir no monitoramento de suas atividades pelo Google, bem como descobrir quais tipos de atividades estão sendo monitoradas.

Você prefere intervir no monitoramento de atividades do Google, escolhendo entre *'habilitado'* ou *'pausado'*. Por padrão, prefere ser avisado sobre possíveis impactos ao realizar algumas ações como *'Excluir'*, *'Habilitar'* ou *'Pausar'*. Além disso, deseja acessar, primeiramente, o seu histórico de atividades ao entrar na aplicação.

4.2.7 Reconstrução da Metamensagem Designer-Usuário

A reconstrução da metamensagem do MyActivity, com base na análise de signos, revela a seguinte intenção comunicativa designer-usuário: "Este é o meu entendimento, como designer, de quem você é: uma pessoa que, em certa medida, preocupa-se com seus dados pessoais ou com o que pode ser visto sobre você. Você é um usuário que deseja ter confiança na hospedagem onde suas informações estão armazenadas. Entretanto, pelo fato de ser um usuário que frequentemente interage com alguns serviços ou produtos do Google, tais como Youtube, Maps e Chrome, busca entender como obter uma experiência mais útil e eficaz dessas ferramentas que utiliza por meio do monitoramento de alguns de seus dados. Dessa forma, eu acho que você possui algum conhecimento sobre formas de interagir com serviços e produtos da internet, provavelmente em dispositivos móveis, em um contexto variado ou não, estando ambientado com sistemas de busca e classificação de categorias. Por isso, mostra-se como um usuário que entende o conceito de 'atividade' no contexto da aplicação."

"Este é o meu entendimento, como designer, do que você quer: você quer consultar quais tipos de atividades são passíveis de monitoramento, revisar seu histórico atividades realizadas, pesquisar atividades por meio de uma busca com palavras e filtros, bem como acessar detalhes de atividades específicas. Você também quer intervir no monitoramento

das atividades, decidindo controlar quais tipos de atividades podem (ou não) ser monitoradas ou armazenadas nos servidores da Google, podendo assim, realizar exclusões de atividades registradas. Diante desses recursos que ofereço, você pode querer opinar ou expressar suas impressões sobre essa plataforma, fornecendo *feedbacks* de sua experiência, seja reportando problemas, respondendo questionários de pesquisa ou compartilhando suas ideias."

"Este é o meu entendimento, como designer, das maneiras que prefere fazer suas atividades e o porquê: você quer visualizar novas atividades rapidamente ao acessar a ferramenta, podendo fazer consultas em seu histórico por uma data, serviço ou produto que utilizou. Além disso, você pode optar entre duas formas de visualização as quais permitem classificar suas atividades registradas em itens avulsos ou agrupá-los em pacote, podendo ser por produto ou serviço. Por padrão, prefere visualizar todas as atividades em ordem cronológica inversa (da mais recente para a mais antiga), conferindo detalhes caso tenha maior interesse em alguma atividade em específico. Ao gerenciar suas atividades, prefere entender como o registro de suas atividades influencia a sua experiência ao fazer uso dos serviços da Google. Para gerenciar os tipos de atividades que a empresa pode monitorar, prefere consultar uma lista com todas os tipos atividades existentes, bem como a descrição de cada. Além disso, aproveitando o entendimento obtido nessa mesma lista, deseja intervir no monitoramento de suas atividades, escolhendo entre *'habilitado'* ou *'pausado'*. Ademais, prefere, por padrão, ser alertado todas as vezes que realizar a exclusão de registros de atividades, pausar ou habilitar o registro de suas atividades."

4.2.8 Consistência das Metamensagens

A comunicação entre designer-usuário se mostra abrangente e clara, as vezes até de forma redundante, mas apresentando explicações consistentes nas três classes de signos tais como, informações sobre o uso de manipulação de dados pessoais, oferta de mecanismos de controle que permitam a tomada de decisão pelo usuário. Essa comunicação se dá em diferentes seções do sistema, permitindo deduzir uma outra característica do usuário: ele prefere estar ciente a todo tempo sobre questões de transparência e privacidade quanto a manipulação dos registros pessoais.

Por outro lado, o designer comunica alguns aspectos de forma objetiva, por exemplo, aqueles relativos à visualização de registros de atividades, utilizando-se de signos estáticos para comunicar tais aspectos. Assim, observa-se a maioria das ocorrências desse signo apenas na visualização do histórico de atividades, causando certo desbalanceamento na

metacomunicação entre designer-usuário.

A preocupação do designer em deixar claro as informações pertinentes à coleta e sobre os objetivos do uso de dados pela Google foi uma constante e praticamente todo o sistema, bem como sua proposta de prover níveis de detalhamento para muito do que é informado ao usuário, evidenciado pela opções de *'Saiba mais'* e *'Detalhes'*.

4.2.9 Resultados

Com base no mapeamento dos signos metalinguísticos, estáticos e dinâmicos, e suas respectivas meta-mensagens, as estratégias de comunicação identificadas na ferramenta MyActivity são:

(EC1) Prover diferentes categorizações de dados coletados.

(EC2) Exibir atividades monitoradas e o nível de uso de produtos/serviços.

(EC3) Oferecer formas de intervenção sobre a coleta de dados.

(EC4) Prover alertas de ações executadas pelo usuário.

(EC5) Disponibilizar ao usuários meios de reportar problemas ou colaborar com ideias.

Sobre a Estratégia (EC1), o MyActivity, vinculado ao MyAccount, oferece ao usuário uma lista das categorias de dados que podem ser coletados a seu respeito, como *'Histórico de localização'* ou *'Informações do dispositivo'*. Para cada categoria, é apresentada uma breve descrição sobre a finalidade da coleta realizada. Caso o usuário queira obter mais informações a esse respeito, o link *'Saiba mais'* o direcionará para página de *'Ajuda'*. A partir dessa categorização, o MyActivity disponibiliza, também, categorias mais específicas das atividades realizadas pelo usuário nos serviços do Google, tais como *'Feedback sem interesse do YouTube'* e *'Respostas sobre o lugar'*. Com isso, acreditamos que a intenção de design seja oferecer meios para que usuário tenha uma visão abrangente sobre quais tipos de dados podem ser coletados pelo Google, bem como entender os objetivos da empresa em adquirir os dados de seus usuários. Em nossa interpretação, avaliamos que esta estratégia aponta para alguns aspectos do conceito de Legibilidade em IHD, pois a ferramenta disponibiliza ao usuário informações sobre quem está o monitorando, os meios usados para realizar a coleta de dados, quais tipos de dados serão coletados, bem como o interesse pretendido nesse processo. No entanto, não encontramos explicações sobre os algoritmos e métodos empregados na geração de inferências a partir dos dados do usuário.

Sobre a Estratégia (EC2), o MyActivity permite ao usuário consultar e revisar o seu

histórico de atividades realizadas. Por padrão, as atividades mais recentes são exibidas no início do histórico, i.e. em ordem cronológica inversa. Além disso, o usuário tem acesso à opção *'Detalhes'* que fornece explicações sobre como o monitoramento é realizado. O mecanismo de busca ajuda o usuário a encontrar um conjunto ou uma atividade específica em seu histórico de atividades, proporcionando ao usuário melhor navegabilidade, já que se espera uma grande quantidade de registros. O MyActivity oferece, ainda, dois tipos de visualização de atividades: baseada em pacotes (os registros são listados individualmente), ou baseada em produto/serviço (agrupa uma sequência de registros por seu respectivo produto/serviço). É possível, ainda, consultar a frequência de utilização dos serviços em cada dia. A consulta ao histórico de atividades deve ser feita com base na sua categoria. Entretanto, inicialmente, isso pode não ser comunicado de forma apropriada ao usuário, já que, por padrão, ao acessar o MyActivity, são listadas as atividades relacionadas a uma categoria, geralmente a de *'Atividade na Web e de Apps'*. Diante do exposto, podemos observar indícios do conceito de Legibilidade nesta estratégia, tendo em vista que a ferramenta disponibiliza recursos que informam ao usuário sobre a captura realizada sobre suas atividades nos serviços e produtos da Google.

Sobre a Estratégia (EC3), o MyActivity, vinculado ao *MyAccount*, oferece ao usuário formas de intervenção sobre os dados coletados ao seu respeito. Para cada categoria de coleta de dados, é possível definir se o monitoramento está habilitado ou não. Por padrão, alguns tipos de monitoramento já se encontram habilitados e outros desabilitados (pausados). Entretanto, o usuário tem o direito de intervir, a qualquer tempo, sobre o tipo de monitoramento que desejar pausar ou habilitar. A ferramenta faz uso de cores para distinguir o status do monitoramento, aplicando escala de cinza para o monitoramento com *status 'pausado'*, e colorido para o monitoramento com *status 'habilitado'*. Neste caso, entendemos uma possível intenção ao uso de cores é comunicar ao usuário sobre possíveis benefícios provenientes da coleta de seus dados. O MyActivity também permite a exclusão de registros de atividades. Neste caso, a exclusão de registros implica na desconsideração desses dados na agregação e processamento feitos pela Google. Logo, podemos perceber nesta estratégia a perspectiva abordada pelo conceito de Agência, de modo que o usuário dispõe de mecanismos para determinar quais tipos de dados poderão ser acessados e coletados, bem como gerar e excluir seus registros.

Sobre a Estratégia (EC4), o MyActivity oferece alertas quando o usuário quer realizar alguma ação sobre seus dados, tal como pausar/habilitar um tipo de monitoramento ou excluir uma atividade, por exemplo. Essas notificações comunicam ao usuário sobre as implicações da ação pretendida, geralmente buscando incentivá-lo a disponibilizar seus

dados para o Google, mostrando como isso reflete em benefícios na entrega de serviços ou produtos. Além disso, esclarecimentos sobre formas de coleta e armazenamento de tais dados também são comunicados, propondo, assim, clareza e transparência, almejando a confiança do usuário. Com isso, podemos atentar para um vínculo com o conceito de Legibilidade, pois esta estratégia busca lidar com as preocupações do usuário em relação aos seus dados e o processamento que é realizado a partir deles.

Sobre a Estratégia (EC5), o MyActivity apresenta um espaço que oferece ao usuário um recurso para reportar problemas de utilização ou erros no registro de atividades. Dessa forma, no entanto, é necessário aguardar a análise da solicitação para ter o pedido atendido. Esse mecanismo também funciona como um canal para compartilhar ideias ou sugestões. Assim, podemos estabelecer um vínculo com o conceito de Agência, pois esta estratégia possibilita ao usuário meios para informar e corrigir os dados fornecidos.

4.3 Estudo II: Privacy Badger

Esta seção apresenta o segundo estudo de avaliação pelo MIS realizado nesta pesquisa, apresentando os detalhes dos procedimentos adotados e os resultados encontrados. O objetivo deste estudo foi o de identificar de que maneiras o Privacy Badger comunica aspectos de IHD através de seus elementos de interface, bem como observar quais os conceitos de IHD propostos por Mortier et al. [39] estão envolvidos nessa comunicação. Um cenário de inspeção foi elaborado para guiar tal inspeção, conforme apresentado a seguir:

"*Bob usa seu computador pessoal frequentemente para ler notícias, emails, pesquisar produtos, realizar compras online, acessar o internet banking e redes sociais. Bob faz uso de suas informações pessoais para realizar boa parte dessas ações. Assim, preocupado com o risco de invasão de privacidade por robôs de monitoramento (trackers), recorreu à algumas ferramentas, dentre elas, o Privacy Badger. Assim, Bob quer realizar as seguintes tarefas ao usar esta ferramenta: (1) Identificar todos os possíveis sistemas de rastreamento (trackers) que podem monitorar sua atividade ao usar a internet; (2) Bloquear o monitoramento de trackers*"

A inspeção foi realizada de acordo com as tarefas apresentadas no cenário de inspeção acima e o seu resultado foi organizado de acordo com a classificação de signos, i.e., em Metalinguísticos, Estáticos e Dinâmicos. A seguir, serão apresentados os principais signos encontrados e que estão relacionados aos conceitos de IHD, bem como suas interpretações,

de acordo com o entendimento dos avaliadores sobre a intenção do designer.

4.3.1 Signos Metalinguísticos

O usuário, ao acessar o Privacy Badger, é comunicado sobre possíveis *trackers*, que estejam o monitorando indevidamente, além de informar o nível de acesso aplicado em cada um deles. Para isso, o designer recorre ao uso de signos metalinguísticos para ajuda-lo a explicar tais informações. As Figuras 4.11a, 4.11b, 4.11c e 4.11d mostram os exemplos de signos utilizados pelo designer.

Entretanto, tais informações podem ainda não serem claras ao usuário, apontando para a necessidade de detalhes, em especial, a respeito do que são *trackers* ou de como funciona o seu processo de identificação e de possíveis bloqueios. Desse modo, o designer se utiliza de signos metalinguísticos que comunicam a existência de opções as quais o usuário pode recorrer para buscar mais detalhes, conforme ilustram as Figuras 4.12a e 4.12b. Ao acessar informações sobre *trackers*, o designer encaminha o usuário para uma seção de *'Ajuda'*, onde comunica detalhes a respeito de *trackers* e dos mecanismos utilizados pelo Privacy Badger para identificar e atribuir níveis de acesso aos domínios de terceiros, conforme ilustram as Figuras 4.13a e 4.13b.

O designer também comunica de que está ciente que o Privacy Badger pode interferir na exibição do conteúdo de uma página Web, oferecendo um espaço para o usuário relatar a ocorrência desses tipos de problemas ou erros. A Figura 4.14 mostra o signo metalinguístico utilizado pelo designer para realizar tal comunicação.

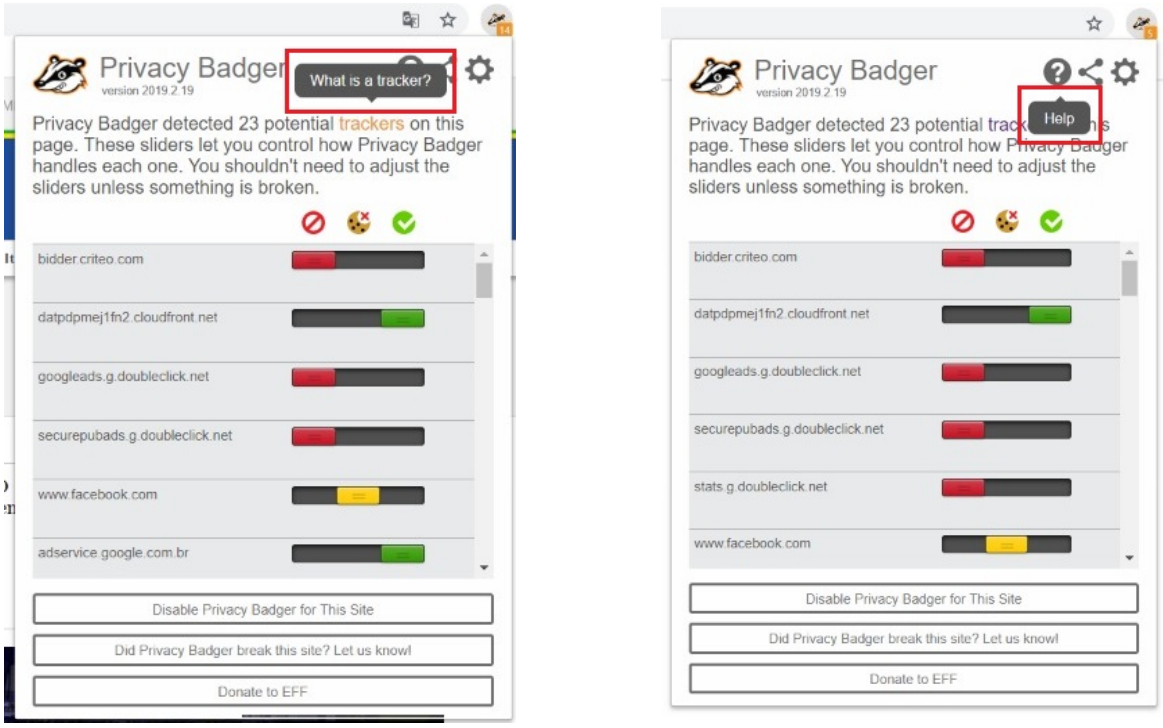
Na seção de *'Configurações'*, o designer descreve alguns aspectos importantes quanto aos efeitos colaterais relacionados mecanismos de proteção, bem como dos recursos de intervenção que são oferecidos ao seu usuário, conforme ilustrado pela Figura 4.15.

4.3.2 Reconstrução da Metamensagem dos Signos Metalinguísticos

Você, usuário, compreende o idioma inglês. Possui pouca familiaridade com sistemas TET, mas parece já ter ouvido falar sobre 'Rastreadores' ou '*trackers*', além do termo 'Domínio de terceiro'. Portanto, parece possuir familiaridade em identificar esses domínios pelo seu endereço, bem como seus objetivos de operação. Por outro lado, pode querer saber de mais detalhes sobre essas questões. Além disso, você se preocupa com seus dados ou com o que pode ser monitorado ao usar serviços na web, desejando ter maior

Figura 4.11: Exemplos de signos metalinguísticos na tela inicial do Privacy Badger.

privacidade ao navegar por sites da web. Já possui algum conhecimento sobre formas de monitoramento não consensual que são realizados por terceiros e parece ser um usuário que busca compreender formas de resguardar sua privacidade ao navegar pela web, mas sem ser impedido de acessar o que realmente deseja acessar, a menos que isso ponha sua



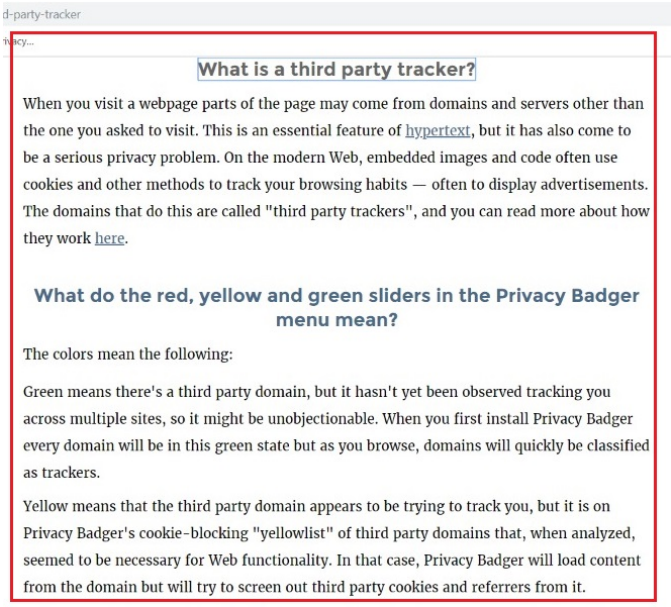
(a) (b)

Figura 4.12: Signos que sinalizam opções do tipo *'Saiba mais'*.

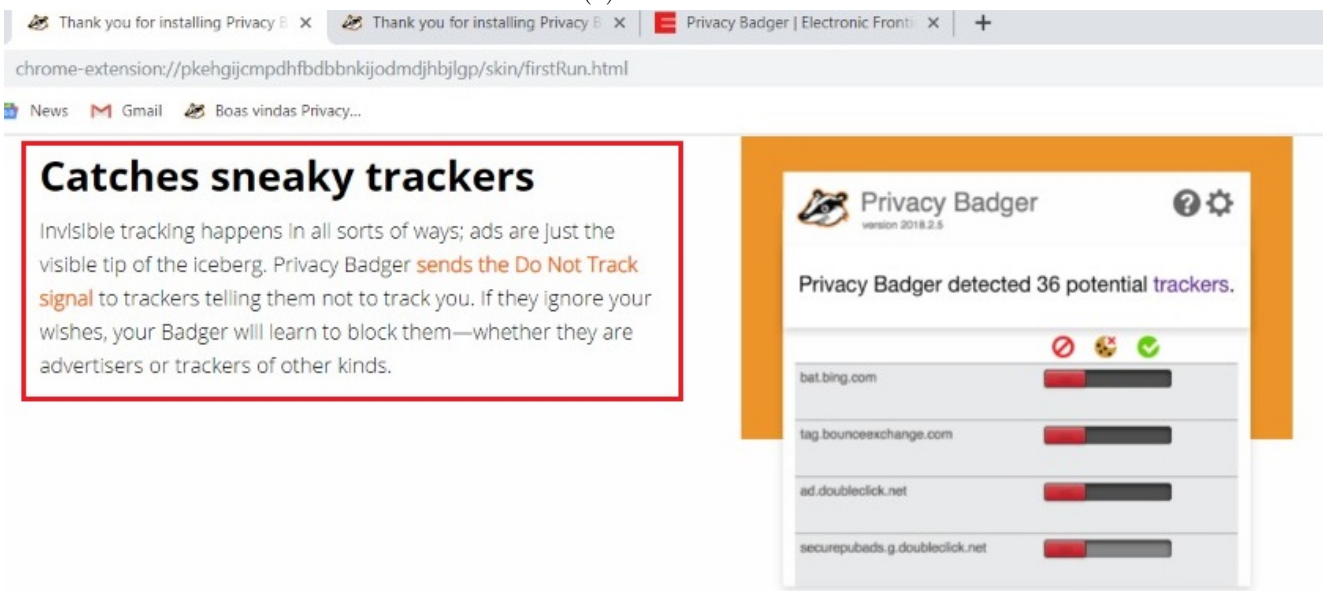
privacidade em risco.

Você, usuário, quer bloquear todo rastreamento não consensual que é feito secretamente por domínios de terceiros à medida que navega na Web. Isto é, impedir que anunciantes ou rastreadores o monitorem para obter seus hábitos ou realize inferências sobre seu comportamento que são geradas pelo simples uso da web. Quer também tomar decisões no controle mais efetivo sobre sua privacidade, não desejando compartilhar seus dados de navegação com entidades terceiras de forma passiva e sem seu consentimento. Também gostaria de reportar problemas de uso decorrentes do Privacy Badger.

Prefere fazer uso de diferentes classificações para mensurar o seu nível de risco, optando por três níveis de controle: 'Domínio liberado' (Verde) , '*Cookie* Bloqueado' (Amarelo) e 'Domínio Bloqueado' (Vermelho). Prefere que o bloqueio de possíveis rastreadores seja de forma automática, embora opte por intervir na decisão final do algoritmo, definindo o nível de risco para domínios de terceiros específicos, caso tenha necessidade, com o mínimo de interação possível no sistema. Deseja ter acesso a detalhes sobre os mecanismos de privacidade implementados pelo Privacy Badger por meio de ilustrações e textos explicativos em uma seção apropriada.



(a)



(b)

Figura 4.13: Designer comunicando informações detalhadas na seção de *'Ajuda'*.

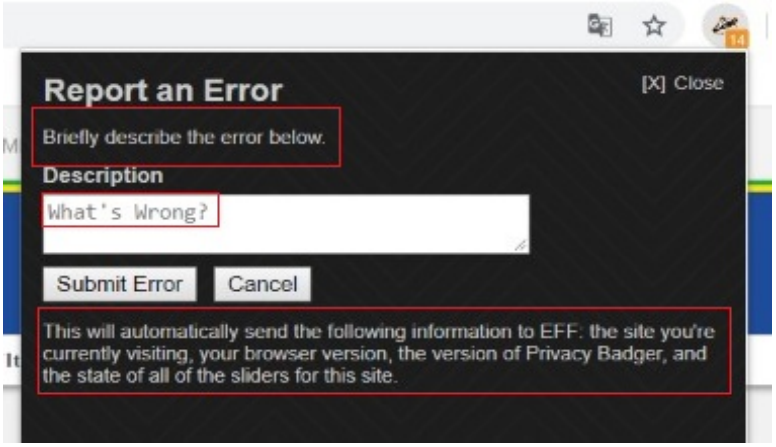


Figura 4.14: Designer comunicando sobre como proceder para reportar erros.

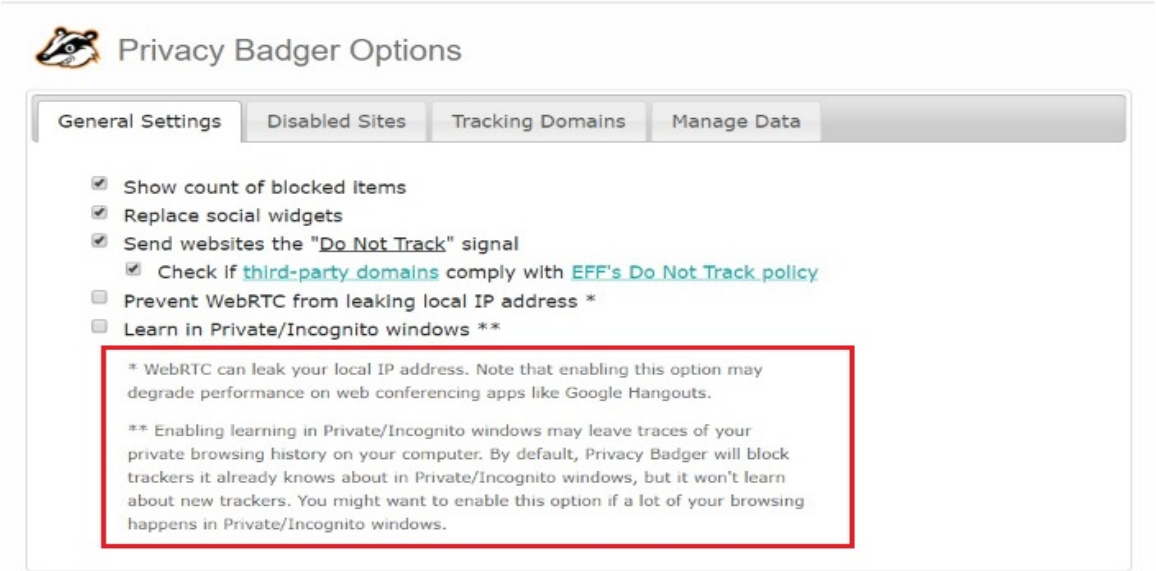
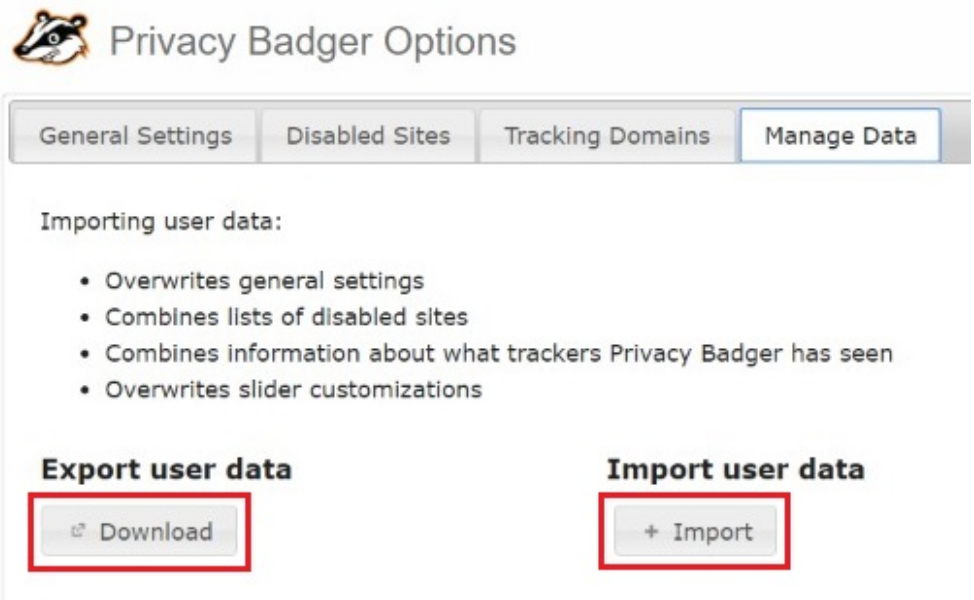


Figura 4.15: Designer comunicando sobre efeitos colaterais.

4.3.3 Signos Estáticos

No Privacy Badger, foram identificados poucos signos estáticos relacionados à IHD. Na tela inicial, o designer busca comunicar ao usuário os níveis de controle que estão sendo aplicados aos domínios de terceiros identificados pela ferramenta, tais como 'Domínio Bloqueado', '*Cookie* Bloqueado' ou 'Domínio liberado'. Além disso, são oferecidas opções de uso para o seu usuário. A Figura 4.16a mostra os exemplos de signos estáticos utilizados nessa comunicação. Na seção de configuração, designer também apresenta outras opções de controle ao usuário, conforme ilustra a Figura 4.16b.

(a)



(b)

Figura 4.16: Exemplo de signos estáticos no Privacy Badger.

4.3.4 Reconstrução da Metamensagem dos Signos Estáticos

Você, usuário, conhece o idioma inglês, com pouca experiência de navegação em interfaces de sistemas. Conhece o conceito de 'Rastreadores' ou '*trackers*', bem como o termo 'Domínios de terceiros'.

Você, usuário, quer consultar o nome de todos os domínios de terceiros identificados pelo sistema, e gostaria de realizar algumas customizações como inserir domínios em uma *whitelist*, assim como desabilitar o monitoramento do sistema em sites específicos. Além disso, quer ser capaz de reportar problemas de "página quebrada".

Você, usuário, prefere não conhecer todas os recursos do sistema. Na maioria dos casos, prefere visualizar uma lista de domínios de terceiros identificados ajustar o nível de risco para algum domínio específico, caso isso se mostre necessário. Além disso, prefere recorrer a uma seção de configurações simples, com opções essenciais.

4.3.5 Signos Dinâmicos

Assim como nos signos estáticos, os signos dinâmicos dinâmicos também são poucos utilizados pelo designer do Privacy Badger. Para comunicar o nível de controle aplicado a um domínio de terceiro, o designer utiliza *switch buttons* os quais permitem a intervenção do usuário para modificá-lo. A transição entre os níveis de controle sugeridos nesse signo é comunicada a partir da troca das cores entre vermelho, amarelo e verde, parecido com o significado de um semáforo. Desse modo, a cor vermelho indica que o domínio de terceiro certamente é um *tracker* e, portanto, terá a sua execução bloqueada. A cor amarelo indica que a realização do serviço do domínio de terceiro é permitida, porém expressa atenção ao não permitir que tal domínio utilize *cookies*. Por fim, a cor verde indica que domínio de terceiro não apresenta comportamento malicioso e, portanto, está livre executar o seu serviço. Além disso, o designer comunica continuamente ao usuário sobre a quantidade de possíveis *trackers* identificados, por meio de um ícone localizado ao lado da barra de endereço do navegador. A Figura 4.17 mostram exemplos de signos dinâmicos utilizados nesta comunicação. O designer também utiliza essa classe de signos para comunicar ações que o usuário poderá realizar em suas configurações, conforme mostra a Figura 4.18.

4.3.6 Reconstrução da Metamensagem dos Signos Dinâmicos

Você, usuário, possivelmente possui familiaridade com o idioma inglês, e parece familiarizado com termos técnicos, como *'Do Not Track'* e 'Domínios de terceiros', sendo possível recorrer a mais detalhes sobre isso, caso precise.

Você, usuário, quer visualizar e modificar informações oferecidas pelo sistema.

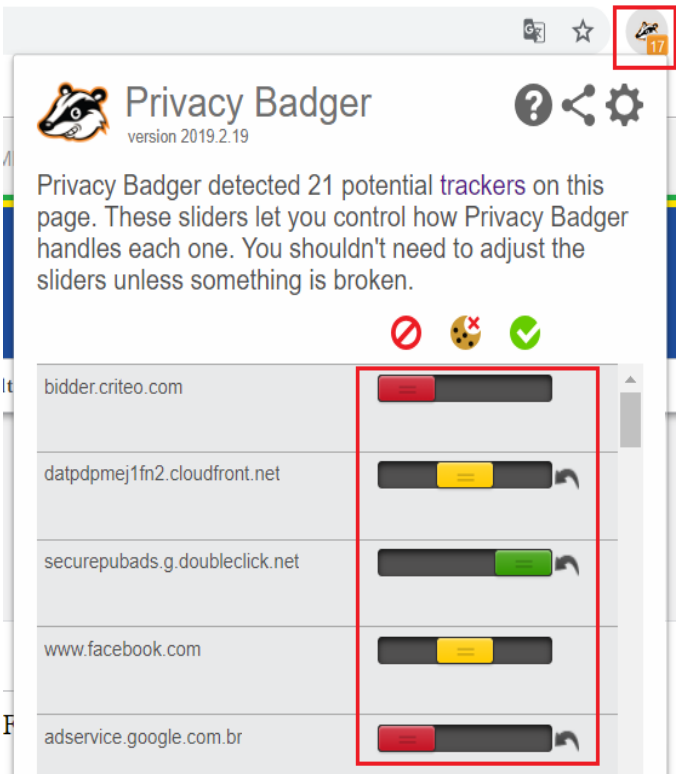


Figura 4.17: Uso de *switch buttons* e contador de possíveis trackers encontrados pelo Privacy Badger.

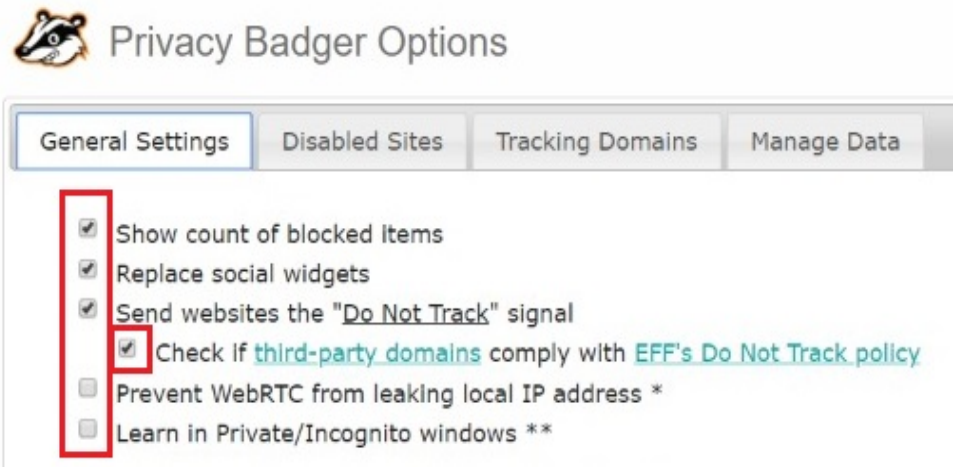


Figura 4.18: Signos dinâmicos no Privacy Badger.

Você, usuário, prefere, de modo geral, que o sistema assuma o controle, identificando e classificando automaticamente os domínios de terceiros, só intervindo quando optar por modificar o nível de controle, escolhendo entre 'verde', 'amarelo' ou 'vermelho'. Prefere que tais ações sejam feitas de forma rápida, com apenas um ou dois cliques, e que a maior parte de tudo aquilo que precisa saber ou fazer esteja em um lugar.

4.3.7 Reconstrução da Metamensagem Designer-Usuário

A reconstrução da metamensagem do Privacy Badger, com base na análise de signos, revela a seguinte intenção comunicativa designer-usuário: "Este é o meu entendimento, como designer, de quem você é: uma pessoa que compreende o idioma inglês. Possui pouca familiaridade com sistemas TET, mas parece já ter ouvido falar sobre 'Rastreadores' ou '*trackers*' , 'Domínios de terceiros' e sobre *'Do Not Track'*. Portanto, parece possuir familiaridade em identificar esses domínios pelo seu endereço, bem como seus objetivos de operação. Por outro lado, pode querer saber de mais detalhes sobre essas questões. Além disso, você se preocupa com seus dados ou com o que pode ser monitorado ao usar serviços na web, desejando ter maior privacidade ao navegar por sites da web. Já possui algum conhecimento sobre formas de monitoramento não consensual que são realizados por terceiros e parece ser um usuário que busca compreender formas de resguardar sua privacidade ao navegar pela web, mas sem ser impedido de acessar o que realmente deseja acessar, a menos que isso ponha sua privacidade em risco."

"Este é o meu entendimento, como designer, do que você quer: bloquear todo rastreamento não consensual que é feito secretamente por domínios de terceiros à medida que navega na Web e gostaria de consultar o nome de todos os domínios de terceiros identificados. Quer também impedir que anunciantes ou rastreadores o monitorem para obter seus hábitos ou realize inferências sobre seu comportamento que são geradas pelo simples uso da web. Quer também tomar decisões no controle mais efetivo sobre sua privacidade, não desejando compartilhar seus dados de navegação com entidades terceiras de forma passiva e sem seu consentimento. Também gostaria de reportar problemas de uso decorrentes do Privacy Badger, como "página quebrada". Por fim gostaria de realizar algumas customizações como inserir domínios em uma *whitelist*, assim como desabilitar o monitoramento do sistema em sites específicos."

"Este é o meu entendimento, como designer, das maneiras que prefere fazer suas atividades: Prefere fazer uso de diferentes classificações para mensurar o seu nível de risco, optando por três níveis de controle: 'Domínio liberado' (Verde) , '*Cookie* Bloqueado'

(Amarelo) e 'Domínio Bloqueado' (Vermelho). Prefere que o bloqueio de possíveis rastreadores seja de forma automática, embora opte por intervir na decisão final do algoritmo, definindo o nível de controle para domínios de terceiros específicos, caso tenha necessidade, com o mínimo de interação possível no sistema. Na maioria dos casos, prefere visualizar uma lista de domínios de terceiros identificados. Quando preferir, deseja ter acesso a detalhes sobre os mecanismos de privacidade implementados pelo Privacy Badger por meio de ilustrações e textos explicativos em uma seção apropriada. Além disso, prefere recorrer a uma seção de configurações simples, com opções essenciais. Prefere que tais ações sejam feitas de forma rápida, com apenas um ou dois cliques, e que a maior parte de tudo aquilo que precisa saber ou fazer esteja em um lugar."

4.3.8 Consistência das Metamensagens

Verifica-se que se trata de um indivíduo que conhece o idioma inglês, com pouca familiaridade com ferramentas TETs, conectado à internet e preocupa-se com sua privacidade no meio digital. Desse modo, possivelmente possui conhecimentos sobre técnicas de coleta de dados a partir monitoramento da atividade do usuário por terceiros, como o uso de *cookies*.

A comunicação entre designer-usuário se mostra bem concisa, mas em alguns casos, em que o designer informa sobre os mecanismos de controle e sobre as ações que oferece ao seu usuário, a comunicação se mostra presente nas três classes de signos. Além disso, a maior parte dessa comunicação ocorre na tela inicial e na seção de configurações do Privacy Badger, permitindo ao usuário rapidez e objetividade. Dessa forma, deduz-se outra característica do usuário: ele prefere ter uma visão ampla do que está acontecendo e do que ele pode fazer em apenas um ponto, ao invés de explorar o sistema. Uma questão que o designer comunica de forma concisa é a possibilidade do usuário reportar erros. Por outro lado, o designer comunica, de forma mais detalhada, sobre os mecanismos de privacidade utilizados pelo Privacy Badger somente por meio de signos metalinguísticos, como no caso das seções de ajuda e de informações técnicas, o que causa certo desbalanceamento.

A flexibilidade e transparência para interagir com os resultados do sistema foi uma constante nas metamensagem, sugerindo que o usuário possa intervir quando necessário ao que o sistema pensa que pode ser algo impróprio. Assim, podemos deduzir que o usuário pode permitir ser monitorado por domínio de terceiro quando achar necessário, já que assim, estará ciente e no controle de tal monitoramento.

4.3.9 Resultados

Com base no mapeamento dos signos metalinguísticos, estáticos e dinâmicos, e suas respectivas meta-mensagens, as estratégias de comunicação identificadas na ferramenta Privacy Badger são:

(EC6) Oferecer formas de intervenção quanto ao uso de dados.

(EC7) Exibir domínios de terceiros identificados.

Sobre a Estratégia (EC6): De modo geral, o conteúdo de uma página da Web pode ser proveniente de várias fontes diferentes, i.e., domínios de terceiros. Em uma página de *e-commerce*, por exemplo, a exibição de produtos será realizada por uma loja virtual, o mecanismo de busca pode ser de uma empresa contrata para disponibilizar tal serviço e os anúncios serão de uma empresa de publicidade. Dessa forma, o Privacy Badger, por meio de algoritmos de classificação, analisa o comportamento de todos os servidores de terceiros identificados a medida que o usuário navega por diferentes domínios, aplicando um dos seguintes *status*: 'Bloqueado', 'Bloqueado Parcialmente' e 'Permitido'. Caso algum domínio esteja tentando monitorar, sem permissão, o registro de navegação do usuário, por meio de *cookies*, então o Privacy Badger irá automaticamente bloquear o conteúdo proveniente de tal servidor. Caso este domínio esteja fornecendo um tipo de conteúdo importante para o funcionamento da página, então o Privacy Badger permitirá conexões com este servidor, mas bloqueará a sua injeção de *cookies* no navegador. Por fim, o Privacy Badger permitirá a injeção de conteúdo de terceiros caso não seja detectada atividade de monitoramento.

A ferramenta permite, ainda, que o usuário modifique o status aplicado, oferecendo, assim, poder de intervenção no resultado do algoritmo de classificação. Dessa forma, esse domínio passará a ser classificado de acordo com a decisão do usuário final. Além disso, o Privacy Badger oferece uma *whitelist* local, em que o usuário poderá acrescentar domínios de sua confiança, de modo que esses estarão fora da análise do Privacy Badger. Dessa forma, podemos observar uma correlação com o conceito de Agência em apoiar o usuário para exercer controle sobre o acesso aos seus dados de navegação. Contudo, a ferramenta não permite ao usuário definir quais tipos de dados deseja disponibilizar, por exemplo.

Sobre a Estratégia (EC7): O Privacy Badger oferece uma lista com o endereço e o respectivo status para cada domínio de terceiro identificado, permitindo que o usuário fique ciente sobre quais são os domínios de terceiros atuantes, bem como aqueles que tentaram realizar, ou não, algum tipo de monitoramento oculto. Entretanto, a ferramenta

falha ao comunicar informações sobre os domínios identificados, como o tipo de conteúdo ou que funcionalidade um determinado servidor estava tentando inserir, o que poderia auxiliar o entendimento do usuário sobre como os domínios de terceiros atuam. Assim, podemos apontar, nesta estratégia, para uma referência ao conceito de Legibilidade com base na identificação de quais domínios tentaram coletar os dados do usuário. Entretanto, o usuário não será informado sobre alguns aspectos importantes sobre o processo de coleta, armazenamento e processamento, como a finalidade da coleta de dados ou que tipos de dados, de fato, podem ser coletados a seu respeito

4.4 Classes de Signos

Nesta seção, serão apresentados as classes de signos que foram identificadas durante a execução do MIS nos Estudos 1 e 2. Estas opções representam sugestões visuais usadas para interagir com sistemas e que foram adotadas pelos designers dessas aplicações. A ferramenta MyActivity usa todos os tipos identificados. Porém, a ferramenta Privacy Badger não oferece as classes *Cards* e *Modal*, conforme apresentado a seguir:

- **Cards**: são as atividades registradas do usuário. Cada atividade é representada por um título (mostrando o serviço usado), um *link* para a atividade realizada antecedido por uma palavra-chave que caracteriza o tipo de atividade registrada, tal como *'Assistido'* (Vídeos), *'Visitado'* (Páginas Web), *'Pesquisa de'* (Pesquisa no Google) ou *'Área Vista'* (Uso de Mapas), por exemplo. Além disso, opções de *'Detalhes'* ou *'Excluir'* são exibidas em cada registro de atividade. Geralmente, uma figura pode estar associada a uma atividade e agrupamentos de atividades podem ser feitos automaticamente para resumir a exibição de registros. Assim, uma opção é exibida no rodapé do *card* caso o usuário deseje visualizar itens que foram suprimidos. É interessante notar que todas as atividades compõem um histórico de registros, de forma que esses registros estão distribuídos em seus respectivos dias. Cada *card*, que pode ser uma atividade ou um agrupamento de registros, são ligados por uma linha do tempo com um *timestamp* associado. A Figura 4.19 mostra um exemplo de *cards*.

- **Modal**: são alertas geralmente exibidos para confirmar ações do usuário, com textos que descrevem brevemente suas consequências. A Figura 4.20 mostra um exemplo de *Modal* no MyActivity.

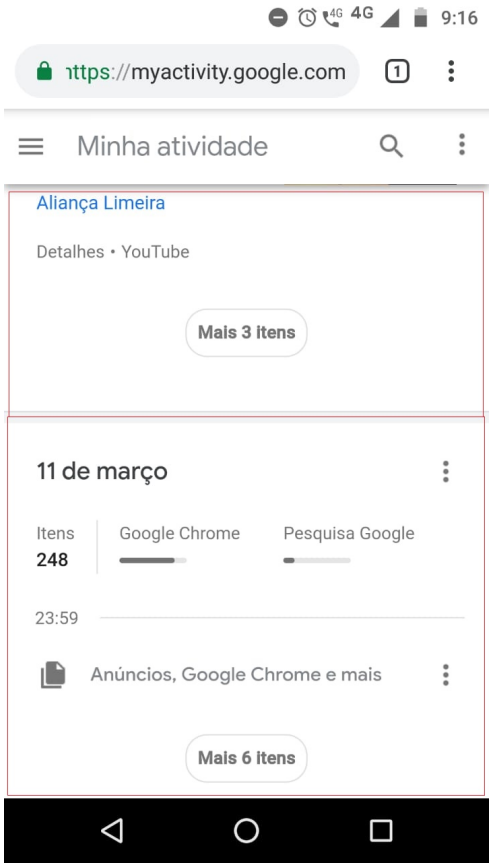


Figura 4.19: Exemplo de *Cards* MyActivity.

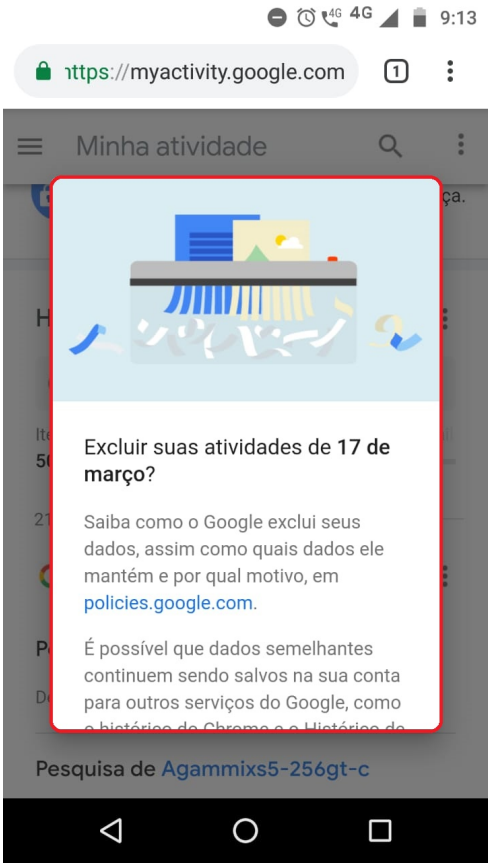


Figura 4.20: Exemplo de *Modal* MyActivity.

- **Filtro de Busca**: permitem ao usuário refinar a exibição de registros por contexto. Por exemplo, no MyActivity, é possível selecionar os tipos de serviços, intervalo de datas, dentre outras opções. No Privacy Badger, é possível optar pelo *status* associado ao domínio, por exemplo. A Figura 4.21 mostra o exemplo de filtro utilizado pelo Privacy Badger.

- **Switch Button**: representam as preferências do usuário em relação a sua privacidade, i.e., sobre o que pode ser visto sobre ele pelas entidades interessadas em seus dados pessoais. A Figura 4.22 mostra exemplos de *Switch Buttons* no Privacy Badger.

4.5 Análise Comparativa Entre os Resultados de Estudo 1 e Estudo 2

Um dos principais desafios observados durante as inspeções foi a aplicação parcial dos aspectos advogados pelos conceitos de IHD, apontando para possíveis barreiras ou limita-

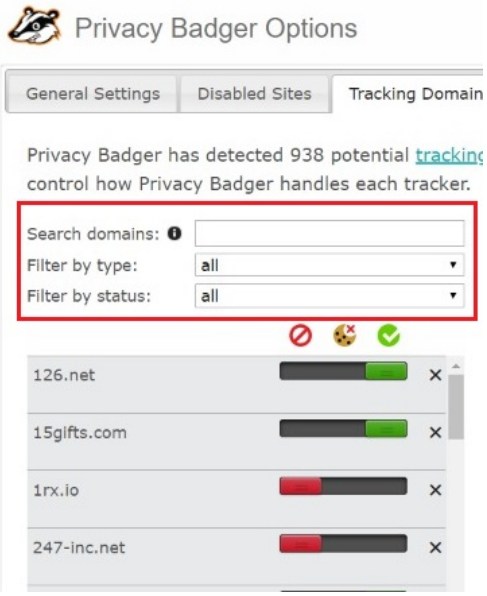


Figura 4.21: Exemplo de Filtros de Busca no Privacy Badger.

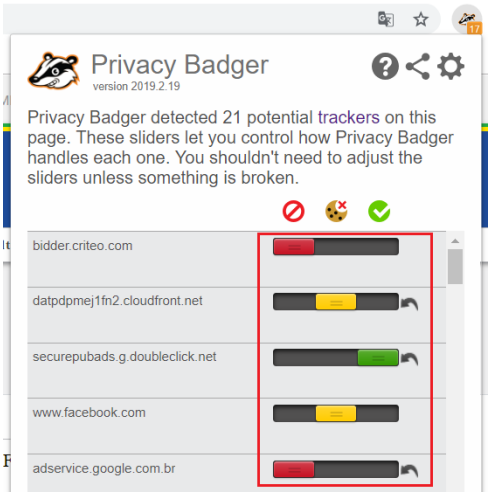


Figura 4.22: Exemplo de *Switch Buttons* no Privacy Badger.

ções na adoção de fatores humanos face aos uso e armazenamento de dados pessoais por terceiros. Por outro lado, identificamos a possibilidade de viabilizar a Interação Humano-Dados sem que todos traços de seus conceitos estejam presentes.

Sobre o conceito de Legibilidade em IHD, identificamos alguns de seus aspectos presentes nas Estratégias de Comunicação EC1, EC2, EC4, EC6. Entendemos que esse conceito representa a primeira etapa para viabilizar Interação Humano-Dados, conferindo diretrizes que apoiam o entendimento das pessoas sobre as ações de terceiros que atuam como interessados em seus dados pessoais. Os problemas de comunicação encontrados podem apontar para a resistência em tornar mais transparentes os algoritmos empregados na geração de inferências sobre as pessoas. Isso corrobora com a observação de Mortier em [39], ao mencionar o conflito em tornar público tais algoritmos que são propriedade intelectual de empresas. Contudo, foi possível identificar mecanismos importantes relacionados a aspectos de Legibilidade, como a classificação de dados monitorados, identificação daqueles que pretendem acessar os dados pessoais, formas de coleta usadas e os objetivos pretendidos das partes interessadas. Entretanto, percebemos o emprego mais tímido desse conceito pela ferramenta Privacy Badger, por meio dos possíveis problemas de comunicação relatados no Estudo 2 (veja seção 4.3).

Em relação ao conceito de Agência em IHD, foram percebidos, também, traços desse conceito em ambas as ferramentas. Podemos observar que o emprego abrangente de Legibilidade oferece um contexto mais propício à adoção dos aspectos de Agência. Em outras

palavras, caso as pessoas não estejam cientes sobre quem são os interessados em coletar seus dados, quais são os dados pretendidos, os seus métodos de coleta e objetivos almejados, então a capacidade das pessoas em atuar sobre seus dados fica limitada, de modo que não haverá informações importantes disponíveis aos usuários afim de os apoiarem em suas decisões ou, ainda, auxiliar na criação de critérios e controles mais adequados sobre o acesso e uso de seus dados por terceiros. Portanto, observamos que a ferramenta MyActivity comunica esses aspectos de forma mais clara, refletindo o conceito de Agência de modo mais abrangente.

Por fim, não foram encontrados traços de aplicação dos aspectos relacionados ao conceito de Negociabilidade nas estratégias identificadas. Isso pode apontar a dificuldade em definir mecanismos os quais permitam identificar as características que são expressos em dados e são passíveis de mudança ao longo do tempo, tais como as atitudes e interesses individuais, por exemplo. Entretanto, essas questões se mostram relevantes no contexto de processamento e geração de inferência a partir de dados pessoais. A tabela 4.1 reúne as respostas obtidas para as questões de pesquisa QP1 e QP2.

Tabela 4.1: Sumário das respostas obtidas nos estudos 1 e 2 para as questões de pesquisa definidas.

(QP1)	(QP2)
EC1: Prover diferentes categorizações de dados coletados.	Legibilidade
EC2: Exibir atividades monitoradas e o nível de uso de produtos ou serviços.	Legibilidade
EC3: Oferecer formas de intervenção sobre a coleta de dados.	Agência
EC4: Prover alertas de ações executadas pelo usuário.	Legibilidade
EC5: Disponibilizar ao usuários meios de reportar problemas ou colaborar com ideias.	Agência
EC6: Oferecer formas de intervenção quanto ao uso de dados.	Agência
EC7: Exibir domínios de terceiros identificados.	Legibilidade

4.6 Estudo 3: Triangulação

Para validar cientificamente os resultados obtidos na aplicação do MIS nos Estudos 1 e 2, a fim de gerar novos conhecimentos científicos, foi realizado uma etapa de triangulação a qual denominamos de Estudo 3. Neste caso, trata-se de uma triangulação endógena,

i.e. mantemos o mesmo domínio investigado, mudando o método de avaliação. Dessa forma, este estudo consiste de testes de observação com a participação de 5 pessoas (ver detalhes na seção 4.1) e a partir dos discursos registrados de cada participante, foi possível evidenciar convergências e divergências, tanto em relação a percepção das estratégias de comunicação identificadas no MIS (i.e. relativas à QP1), quanto pelo reconhecimento dos aspectos relativos aos conceitos de IHD presentes na comunicação entre Designer e Usuário em cada EC (i.e. relativas à QP2).

A tabela 4.2 apresenta o sumário desses resultados obtidos na etapa de triangulação. É possível observar, para cada EC encontrada no MIS, os participantes (denotados por Px, onde $1 \leq x \leq 5$) que identificaram a referida EC (convergência em relação à QP1) e associá-la ao mesmo conceito de IHD a qual foi atribuída no MIS (convergência em relação à QP2). Em outras palavras, as intenções de design identificadas pelos avaliadores durante a aplicação do MIS se mostraram, de fato, percebidas pelos participantes. É possível notar, também, as divergências em relação à QP1 para cada EC (i.e. os participantes que não a identificaram), bem como as divergências em relação à QP2 (i.e. os participantes que conseguiram identificar tal EC, mas associaram-na a um conceito de IHD diferente daquele atribuído no MIS). As convergências e divergências serão apresentadas nas subsecções 4.5.1 e 4.5.2, respectivamente.

Tabela 4.2: Sumário dos resultados convergentes e divergentes identificados na triangulação.

	Convergências		Divergências	
ECs	QP(i)	QP(ii)	QP(i)	QP(ii)
1	P1, P2, P3, P4, P5	P1, P2, P3, P4	-	P5
2	P1, P2, P3, P4, P5	P1, P2, P3, P4, P5	-	-
3	P1, P2, P3, P4, P5	P1, P2, P3, P4, P5	-	-
4	P2, P3, P4	P2, P3, P4	P1, P5	P1, P5
5	P2, P3, P4, P5	P3, P4, P5	P1	P1, P2
6	P2, P3, P4	P2, P3, P4	P1, P5	P1, P5
7	P2, P3, P4	P3, P4	P5	P1, P2, P5

4.6.1 Convergências

Nesta seção, serão apresentado, para cada estratégia de comunicação, os trechos dos discursos que evidenciam as convergências identificadas, relacionados às respostas das questões QP1 e QP2.

Como evidência de EC1, prover diferentes categorizações de dados coletados, os participantes demonstraram certa facilidade em identificar quais tipos de dados podem ser

gerados ou monitorados e, com isso, alguns expuseram preocupações sobre a falta de considerações mais detalhadas quanto à manipulação de seus dados, como P2 e P4:

P1: "Pelo que vejo, a Google está de olho nos meus interesses, em especial, os que movem o meu quotidiano. Assim, ela busca monitorar os meus clicks, os textos, vídeos, comentários e aonde eu fui. Isso está relacionado ao conceito de Legibilidade."

P2: "...Percebo que a Google quer saber sua localização, os locais que você visitou, o que você pesquisa (no buscador, no Youtube e no Play Música) porque isso irá ajudá-los em suas recomendações. Isso está relacionado ao conceito de legibilidade, porque a ferramenta mostra o que a Google tem interesse em fazer com esses dados, mas não de forma aprofundada. Ou seja, ela diz o que irá fazer e com o que, mas não diz como irá fazer."

P3: "... é possível perceber facilmente os dados que a Google tem sobre você. Neste caso, é o conceito de legibilidade envolvido."

P4: "... tem praticamente tudo sobre mim, como localização, locais que visito e a hora, o que assisti ou fiz no Youtube, minha assinatura vocal... A legibilidade não é completamente aplicada porque percebo que ainda há uma certa falta de transparência sobre formas de utilização do meus dados e seus propósitos."

P5: "Sim, por exemplo a localização, tipos de músicas, o que vejo no Youtube."

Como evidência de EC2, exibir atividades monitoradas e o nível de uso de produtos/serviços, os participantes foram unânimes em associar esta estratégia com o conceito de legibilidade:

P1: "... eu consigo ver o que o Google registrou sobre mim. Isso está associado à legibilidade, já que há o uso de textos ou palavras como "Saiba Mais"que ajudam a entender sobre o que foi registrado."

P2: "... é possível visualizar, inclusive o circuito que o usuário realizou em uma localidade, uma espécie de história de como você visitou um lugar. Assim, é possível associar ao conceito de legibilidade, porque você está ciente sobre o que ele está monitorando."

P3: "... é possível consultar os registros por meio de históricos, tais como o de localização, que permite identificar até mesmo o trajeto realizado, de forma fácil e organizada para o usuário. Então, esta visão se enquadra no conceito de legibilidade, porque esta bem claro o que foi gravado, registrado, i.e., uma consulta."

P4: "... o MyActivity mostra o histórico de todas esses tipos de atividades ... então é

Legibilidade."

P5: "... o MyActivity registra (no caso do Chrome), não somente qual site eu visitei, mas quais seções do site eu passei. Aqui eu acho que é Legibilidade, porque ele mostra exatamente o que eu fiz."

Como evidência de EC3, oferecer formas de intervenção sobre a coleta de dados, os participantes ficaram inseguros sobre as opções oferecidas (P1, por exemplo). Outros, como P2, acharam que não estavam muito visíveis:

P1: "Não senti 'firmeza' em controlar meus dados porque não temos uma política ou algo que torne esse controle mais presente em nosso dia-a-dia. Entretanto, com a opção de download dos meus dados me deixou mais tranquilizada. Isso esta atrelado ao conceito de Agência."

P2: "... percebi que em alguns casos, as opções ficam escondidas, talvez. Mas é possível, sim, controlar o que eles podem ter acesso ou não aos seus dados. Tem a ver como o conceito de agência, por permitir agir sobre os dados."

P3: "... é possível, por exemplo, tanto excluir, quanto impedir que eles continuem a te monitorar. Então, existem opções de agência que te conferem um controle sobre seus dados."

P4: "... eu posso apagar histórico, intervir em algumas coisas ... o mínimo existe, que são os casos de poder deletar, modificar, permitir ou negar ... i.e. Agência. Mas, nesse caso, eu não consigo gerenciar para terceiros, somente para mim."

P5: "... ele disponibiliza a opção do que eu posso liberar ou não. Acho que é o [conceito] de Agência, porque é um meio de realizar gerência sobre meus dados. É você mostrando o que você quer que aconteça."

Como evidência de EC4, prover alertas de ações executadas pelo usuário, alguns usuários notaram maiores esclarecimentos relativos aos seus dados através desta estratégia comunicativa:

P2: "... fica claro os prós e os contras de permitir que o Google monitore ou não as suas atividades. Esses alertas reforçam o que a sua ação irá ocasionar, não permitindo que o usuário simplesmente realize a ação, forçando o usuário a se atentar para isso. Assim, o conceito de legibilidade aparece outra vez."

P3: "Eles fornecem informações mais aprofundadas sobre os seus dados. Logo, torna-se legibilidade."

P4: "Ele me dá informações mais aprofundadas quando eu clico em ativar ou quando quero pausar. Legibilidade."

Como evidência de EC5, disponibilizar ao usuários meios de reportar problemas ou colaborar com ideias, alguns participantes consideraram interessante recorrer a esse mecanismo de controle:

P3: "... o MyActivity permite até que capturas de telas sejam enviadas, para ajudar na identificação do problema. Permite até modificações por motivos legais, e como é uma empresa global, então é importante ter essa opção mesmo. Percebi que a opção de excluir aparece em alguns casos em outros não, mas presumo que todas deveriam possuir. Está relacionado a Agência."

P4: "... o MyActivity oferece uma forma reportar problemas legais, não problemas com terceiros. Mas a tela passa informações genéricas então, acho que poderia ser para qualquer tipo de problema também. Por outro lado, ele disponibiliza um 'saiba mais', então talvez seja o caso de ir e ler mais a respeito. Seria a Agência, pois a oferece possibilidades parecidas como as outras ações das outras telas."

P5: "... no caso é a opção de feedback. Essa opção permite que eu participe, seja para reclamar ou sugerir ou dar algum tipo de contribuição. Por isso, eu acho que está mais relacionado ao [conceito] de Agência do que com os outros dois conceitos."

Como evidência de EC6, oferecer formas de intervenção quanto ao uso de dados, alguns usuários gostariam de informações mais precisas:

P2: "Eu consegui distinguir as intenções dos domínios de terceiros por cores e por alguns nomes de domínio, ou seja, aqueles que estão interessados no meu comportamento ou não. Essa identificação pode estar relacionada ao conceito de Legibilidade."

P3: "Quando você clica no total de trackers identificados, ele te disponibiliza os nomes, então é bem fácil e tranquilo de identificar essas coisas nele. Isso se relaciona com a Legibilidade e pouco, porque a ferramenta oferece apenas que esse domínio está tentando te monitorar, mas você não sabe o que ele ta registrado, i.e., é realmente o mínimo da Legibilidade."

P4: "Achei muito bom conseguir identificar, pois a ferramenta mostra muitos domínios que podem estar me monitorando, mas, por outro lado, faltou mais transparência pois ele não descreve muito bem o objetivo desses possíveis trackers estarem agindo. Acho que se eu soubesse disso, eu poderia permitir o monitoramento caso fosse para beneficiar as pessoas. Assim, percebo que isso está relacionado com o princípio de Legibilidade."

Como evidência para o EC7, mostrar os domínios de terceiros identificados, alguns participantes perceberam certas limitações na aplicação do conceito de Agência:

P2: "... eu posso habilitar e desabilitar, por exemplo, domínios de terceiros. Isso está relacionado ao conceito de Agência. Mas os conceitos aplicados aqui são de maneira fraca, porque ele poderia fornecer mais informações sobre o que cada domínio de terceiro deseja fazer, ou qual comportamento o domínio de terceiro apresentou para o Privacy Badger efetuar o bloqueio."

P3: "Consegui bloquear alguns domínios, mas como a ferramenta não traz informações sobre as consequências dessa ação, talvez possa impactar no funcionamento da página. Está relacionado ao conceito de Agência, mas somente até a parte de gerir o acesso. O uso de seus dados por terceiros já não é possível porque não compete a essa ferramenta, já que ela não tem acesso ao o que o terceiro registrou sobre você."

P4: "... O Privacy Badger me permite realizar o bloqueio ou a liberação, então é o mínimo de gerência. Logo, está associado ao conceito de Agência."

4.6.2 Divergências

As divergências identificadas na etapa de triangulação podem ser classificadas em dois casos: o primeiro caso envolve os participantes que não conseguiram identificar alguma estratégica comunicativa e, portando, não puderam associar a um conceito de IHD. Assim, a divergência está associada à QP1. O segundo caso compreende os participantes que conseguiram identificar tais estratégias comunicativas, mas para alguma delas, relacionaram com um conceito de IHD diferente daquele estipulado no estudo 1 e 2. Portanto, a divergência está associada à QP2.

Com relação ao primeiro caso, algumas estratégias comunicativas não foram percebidas por alguns participantes. Os exemplos identificados foram: P1 e P5 tiveram contato com EC4. No entanto, eles não o consideraram como um alerta, mas sim como outra informação textual apresentada na interface. P1 também não conseguiu localizar EC5 nem entender EC7, como segue: *"Os nomes identificados de domínios de terceiros não faziam sentido para mim."* Além desses exemplos, P5 não pôde avaliar o Privacy Badger, pois essa ferramenta não oferecia a linguagem desejada pelo usuário, como evidenciado em sua fala: *"A interface não faz sentido para mim, pois não sei inglês, então eu não iria manipular este programa."*

Em relação ao segundo caso, por exemplo, a partir da descrição textual apresentada

para cada categoria de atividade no MyActivity, através de E1, P5 entendeu que o monitoramento de atividades permite que os usuários se entendam melhor ao longo do tempo através de um possível processamento de seus registros históricos. Esse novo entendimento pode ser relevante nas trocas de dados subsequentes, permitindo o compartilhamento de novas reavaliações em relação ao seu comportamento ou interesses expressos em dados, com outros interessados em seus dados. Então, P5 vinculou o EC1 ao conceito de Negociabilidade, como relatado: *"Eu acho que é Negociabilidade, porque poderíamos permitir que fossemos monitorados para certos tipos de atividades em algum momento, talvez para obter algum benefício. Ao saber que tipos de atividades eu sou monitorado, permite-me configurar o seu perfil e perceber, ao longo do tempo, mudanças de comportamento ou interesses sobre mim. Dessa forma, pode ser interessante que outras pessoas saibam sobre essas mudanças."*

Em um segundo exemplo, P2 considera que o EC5 está relacionada ao conceito de Negociabilidade, pois entendeu que esta estratégia permite não apenas reportar falhas do sistema, mas também para expressar suas considerações sobre o uso de seus dados por terceiros, conforme relatado : *"Pode ter a ver com Negociabilidade, porque permite que você negocie sobre seus dados, dizendo o que desaprova o uso de dados."*

Houveram duas outras divergências sobre o EC7: P1 considera que está relacionado ao conceito de Legibilidade, porque o Privacy Badger realiza automaticamente um possível bloqueio em um domínio de terceiros. Assim, a ferramenta sugere que não é necessário que o usuário modifique tais controles, mas apenas observe o tipo de restrição aplicada a um domínio particular de terceiros, conforme relatado: *"A opção de bloquear terceiros interessados em meus dados pode se referir ao conceito de Legibilidade, porque fica ao meu critério bloqueá-lo ou não."* Por fim, P2 considera que o EC7 está ligada ao conceito Negociabilidade porque *"a ferramenta permite não apenas bloquear ou ativar, mas fazer meio termo, bloqueando apenas o cookies e permitindo que o domínio de terceiro execute sua funcionalidade na página."*

Capítulo 5

Conclusões e Contribuições

Este trabalho descreve, em detalhes, processo de caracterização das oportunidades de IHD por meio da investigação de estratégias para comunicar os conceitos propostos por Mortier et. al., i.e, Legibilidade, Agência e Negociabilidade, em ferramentas de apoio à transparência.

Para isso, foi aplicado o Método de Inspeção Semiótica (MIS) para fins científicos, com enfoque na avaliação da Comunicabilidade dos conceitos apresentados em IHD, em duas aplicações, sendo estas a Google MyActivity e Privacy Badger. O Google MyActivity é uma ferramenta de transparência que permite a revisão do histórico de atividades do usuário em alguns produtos e serviços da Google, oferencendo mecanismos para o gerenciamento de dados pessoais na plataforma. O Privacy Badger é um *Add-on* para navegadores e tem por objetivo bloquear a ação de *trackers* que buscam coletar dados, de forma indevida, sobre o comportamento do usuário a partir de sua navegação na internet através de um navegador.

As avaliações das respectivas ferramentas se desdobraram em dois estudos, tendo em vista responder à duas questões de pesquisa definidas neste trabalho. Para validar cientificamente os resultados obtidos nesses estudos e, assim, gerar novos conhecimentos científicos, realizamos uma etapa de triangulação endógena, dado o mesmo contexto de uso das ferramentas estudadas: gerenciamento de dados pessoais. Neste trabalho, a triangulação consiste de uma etapa de avaliação considerando a participação de pessoas, conforme sugere o MIS. Assim, foi possível identificar e evidenciar convergências e divergências em relação aos resultados obtidos nos Estudos 1 e 2.

Este capítulo apresenta as publicações realizadas (Seção 5.1), as principais conclusões (Seção 5.2) e contribuições desta pesquisa (Seção 5.3), bem como as oportunidades de

trabalhos futuros (Seção 5.4).

5.1 Principais Conclusões da Pesquisa

A partir da inspeção e avaliação dos signos, bem como da reconstrução da meta-mensagem sobre as possíveis intenções do designer, foi possível identificar as seguintes Estratégias Comunicativas sobre os conceitos de IHD. Para o conceito de Legibilidade, as estratégias encontradas são: (EC1) Prover diferentes categorizações de dados coletados; (EC2) Exibir atividades monitoradas e o nível de uso de produtos ou serviços; (EC4) Prover alertas de ações executadas pelo usuário; (EC7) Exibir domínios de terceiros identificados. Já as ECs relacionadas ao conceito de Agência foram: (EC3) Oferecer formas de intervenção sobre a coleta de dados; (EC5) Disponibilizar aos usuários meios de reportar problemas ou colaborar com ideias; (EC6) Oferecer formas de intervenção quanto ao uso de dados. Não observamos traços da aplicação do conceito de Negociabilidade.

Identificamos, também, alguns problemas em comunicar aspectos importantes sobre tais conceitos, como a explicação de métodos empregados na geração de inferências (EC1), o acesso a diferentes categorias relativas ao histórico de atividades registradas (EC2), especificação de tipos de dados que podem coletados (EC6) e até mesmo, sobre os formas ou objetivos da coleta de dados (EC7), por exemplo. Entretanto, a ocorrência desses problemas de comunicação evidenciam a possibilidade de viabilizar, mesmo que de modo parcial, os conceitos de IHD. De modo geral, observamos que ferramenta Privacy Badger poderia se apropriar com mais profundidade dos aspectos envolvidos em IHD, já que identificamos limitações comunicativas significantes em comparação ao MyActivity.

Nas Classes de Signos, foram identificadas como viabilizadoras dos conceitos de IHD, dentre as quais, destacamos o uso de *cards*, Modais e *switch buttons*. O uso de *cards* permite organizar um conjunto de informações e de ações associadas a estas informações. Neste caso, o uso de *cards* ajuda na percepção dos aspectos de Legibilidade e Agência relativos às informações pessoais exibidas. O uso de *Modais* permite por em evidência, geralmente uma informação importante a respeito do usuário ou relacionada aos efeitos de uma ação em curso, de modo a trazer a atenção do usuário especificamente para o conteúdo desse elemento visual. Por fim, o uso de *switch buttons* podem ajudar na representação de alguma decisão do usuário, como 'permitir' ou 'bloquear' o acesso a seus dados, apoiando em aspectos relativos à Agência.

Os resultados obtidos na Triangulação corroboram com as características comunica-

tivas apontadas durante o MIS. A partir das falas dos usuários, foi possível obter convergências tanto em relação a percepção das ECs identificadas no MIS, quanto pelo reconhecimento dos aspectos relativos aos conceitos de IHD presentes na comunicação entre Designer e Usuário. Divergências também foram identificadas e agrupadas em dois casos: o primeiro relacionado a não identificação de ECs, e o segundo sendo associação de uma EC a um conceito de IHD diferente ao que fora associado durante o MIS.

No primeiro caso, o uso de avisos textuais se mostrou, para alguns participantes, pouco eficaz. Isso se dá porque, geralmente, os avisos ocorrem durante a realização de uma ação, de modo que o participante se sinta desconfortável em ler, obrigatoriamente, um conteúdo textual extenso dado o contexto de tomada de decisão rápida. Assim, após uma ou duas rolagens, o participante passa a desejar apenas a finalização do processo, não absorvendo apropriadamente o conteúdo mostrado. Há casos em que o participante entrou em contato com uma EC, porém esta pareceu não fazer sentido devido a falta de clareza em expressar um conceito de IHD, confirmando alguns dos problemas comunicativos pontuados durante o MIS. Um exemplo é o de P1 que não conseguiu compreender a mensagem de EC7, o que remete à tímida apropriação do conceito de Legibilidade pelo Privacy Badger.

No segundo caso, houve alguns casos de interpretação difusa sobre qual conceito de IHD estava sendo comunicado por uma EC. No Exemplo de P5 em relação a EC1, é evidente que a descrição textual sobre os tipos de atividades que podem ser monitoradas abrange apenas aspectos relacionados ao uso de dados pessoais, o que, segundo IHD, relaciona-se com Legibilidade. Assim, tais descrições não fazem menção a mecanismos que permitam Negociabilidade. Do mesmo modo, em P2 relacionada à EC5, de fato, o canal de *feedback* permite ao usuário sugerir criação de mecanismos com o intuito de permitir a Negociabilidade de seus dado. Entretanto, esse canal não permite uma Negociação em sí, já que seu objetivo principal é reportar erros relacionados à manipulação dos dados do usuário. Conforme IHD, esse objetivo se enquadra no conceito de Agência.

Outro ponto observado pelas convergências e divergência é a confirmação de certa dependência entre os conceitos de IHD para melhor apropriação dos mesmos pelas pessoas. Assim, quanto melhor for a apropriação de Legibilidade, melhor preparado estará para realizar intervenções no controle de seus dados.

5.2 Contribuições

Este trabalho possui três contribuições principais. A primeira é a aplicação do MIS em um contexto ainda não explorado, permitindo relacionar os conceitos de IHD com questões de *design* pertinentes ao uso de ferramentas de apoio a transparência, mostrando que a aplicação do MIS foi pertinente no referido contexto. A segunda contribuição é a identificação de um conjunto de estratégias comunicativas e das classes de signos usadas por designers para viabilizar a IHD. Tais estratégias podem apoiar designers de outras TETs em suas decisões sobre qual(is) estratégias utilizar, bem como ajudar estudos como uma abordagem para melhoria do processo de IHC no contexto de gerenciamento de dados pessoais. O resultado da investigação do modelo proposto por Mortier e colegas [39] em associação à aplicação do MIS, i.e. a inspeção e avaliação por modelo, mostrou-se promissora na avaliação de IHC em aplicações que buscam dar meios para a Interação Humano-Dados.

Conforme mencionado na seção 2.1, IHD destaca o papel central em considerar a interação com dados pessoais pela sociedade e seu gerenciamento em sistemas computacionais como uma dimensão ainda não explorada em IHC. Tendo isso em vista, bem como as demais contribuições mencionadas, e a metodologia empregada a fim de gerar resultados com validade científica, essa dissertação contribui uma abordagem semiótica preliminar para avaliar IHD. Trabalhos futuros devem avaliar a Negociabilidade, bem como explorar outros domínios.

5.3 Trabalhos Futuros

As conclusões desta pesquisa apontam oportunidades interessantes para trabalhos futuros. Em nosso estudo, o tipo de usuário selecionado foi do tipo inexperiente com aplicações do contexto de controle de privacidade, mas que possua interesse em proteger seus dados pessoais. Vimos também que IHD poder ser viabilizada mesmo com a parcial aplicação de seus conceitos. Assim, uma interessante oportunidade de pesquisa é mensurar e propor possíveis níveis de aplicabilidade de cada um dos conceitos de IHD, i.e, Legibilidade, Agência e Negociabilidade, de modo que possam ser implementados em sistemas de quaisquer domínio. Dessa forma, tal proposta poderia alcançar tanto os projetistas, servindo com diretrizes para implementação de aspectos associados a valores humanos e privacidade, quanto para o usuário, orientando-o em suas expectativas ou engajamento em realizar controle sobre seus dados de forma consciente.

Pela aplicação do MIS, foi possível compreender a interação dos signos metalinguísticos, estáticos e dinâmicos dos sistemas estudados. Um foco interessante para estudos futuros seria pesquisar os efeitos desses signos na Interação Humano-Computador em sistemas computacionais de outro domínio, por exemplo, na área médica, financeira ou profissional. Isto é, dado um contexto de tratamento médico, o qual inclui dados sobre resultados de exames e de uso de medicamentos, qual seria o impacto na utilização das três classes de signos em relação à comunicabilidade de oportunidades para interagir com dados pessoais.

Outra oportunidade surge a partir dos resultados dessa pesquisa: após identificar as principais estratégias para comunicar os conceitos de IHD, seria possível a realização de um estudo com designers para propor melhorias no (re)*design* de aplicações de apoio a transparência. Assim, através desse estudo, verificar pontos de melhorias na comunicabilidade , apresentar as principais preocupações encontradas e realizar testes com usuários após a nova interface ser (re)projetada.

5.4 Publicações Realizadas

A pesquisa apresentada nessa dissertação resultou em duas publicações durante o seu desenvolvimento, sendo ambos artigos completos (*full-paper*). Primeiro, o artigo intitulado *"Transparency Communication Strategies in Human-Data Interaction"* foi apresentado no SBSI 2018 (Simpósio Brasileiro de Sistemas de Informação) em sua trilha principal, abordando as questões de pesquisa definidas nesta pesquisa e os resultados obtidos nos Estudos 1 e 2. Em segundo, o artigo intitulado *"Assessing the Communicability of Human-Data Interaction Mechanisms in Transparency Enhancing Tools"* foi apresentado no MIDI'18 (*6th Conference on Multimedia, Interaction, Design and Innovation*), durante o FedCSIS 2018 (*Federated Conference on Computer Science and Information Systems*). Nesse artigo, foram abordados os mesmos estudos do primeiro artigo, com adição do Estudo 3 sobre a Triangulação e validação dos resultados obtidos.

Referências

[1] Ackerman, M. S.; Mainwaring, S. D. Privacy issues and human-computer interaction. *Computer 27*, 5 (2005), 19–26.

[2] Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and human behavior in the age of information. *Science 347*, 6221 (2015), 509–514.

[3] Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and human behavior in the age of information. *Science 347*, 6221 (2015), 509–514.

[4] Assal, H.; Hurtado, S.; Imran, A.; Chiasson, S. What's the deal with privacy apps?: a comprehensive exploration of user perception and usability. In *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia* (2015), ACM, pp. 25–36.

[5] B. Friedman, P. K.; Borning, A. Value sensitive design and information systems. *Human-Computer Interaction and Management Information Systems: Foundations, Armonk* (2006), 348–372.

[6] Bannon, L. Reimagining hci: toward a more human-centered perspective. *interactions 18*, 4 (2011), 50–57.

[7] Bao, J.; Zheng, Y.; Wilkie, D.; Mokbel, M. Recommendations in location-based social networks: a survey. *GeoInformatica 19*, 3 (2015), 525–565.

[8] Baranauskas, M. C. C.; de Souza, C. S.; Pereira, R. I grandihc-br–grand research challenges for human-computer interaction in brazil. *Human-Computer Interaction Special Committee (CEIHC) of the Brazilian Computer Society (SBC)* (2015).

[9] Bim, S. A.; de Souza, C. Obstáculos ao ensino dos métodos de avaliação da engenharia semiótica. *PUC-Rio. Tese* (2009).

[10] Burnap, P.; Colombo, W.; Scourfield, J. Machine classification and analysis of suicide-related communication on twitter. In *Proceedings of the 26th ACM conference on hypertext & social media* (2015), ACM, pp. 75–84.

[11] Cafaro, F. Using embodied allegories to design gesture suites for human-data interaction. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012), ACM, pp. 560–563.

[12] Cavoukian, A.; Weiss, J. Privacy by design and user interfaces: Emerging design criteria–keep it user-centric. *Information and Privacy Commissioner of Ontario* (2012).

[13] Crabtree, A.; Mortier, R. Human data interaction: historical lessons from social studies and cscw. In *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway* (2015), Springer, pp. 3–21.

[14] Creswell, J. W. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* SAGE Publications, 2012.

[15] de Souza, C. S. The semiotic engineering of user interface languages. *International journal of man-Machine Studies 39*, 5 (1993), 753–773.

[16] De Souza, C. S. *The semiotic engineering of human-computer interaction.* MIT press, 2005.

[17] de Souza, C. S. *Sobre a Engenharia Semiótica da interação com Sistemas de Monitoração.* Tese de Doutorado, PUC-Rio, 2010.

[18] De Souza, C. S.; Leitão, C. F. Semiotic engineering methods for scientific research in hci. *Synthesis Lectures on Human-Centered Informatics 2*, 1 (2009), 1–122.

[19] de Souza, C. S.; Leitão, C. F.; Prates, R. O.; Bim, S. A.; da Silva, E. J. Can inspection methods generate valid new knowledge in hci? the case of semiotic inspection. *International Journal of Human-Computer Studies 68*, 1-2 (2010), 22–40.

[20] de Souza, C. S.; Leitão, C. F.; Prates, R. O.; da Silva, E. J. The semiotic inspection method. In *Proceedings of VII Brazilian symposium on Human factors in computing systems* (2006), ACM, pp. 148–157.

[21] Debes, C.; Merentitis, A.; Sukhanov, S.; Niessen, M.; Frangiadakis, N.; Bauer, A. Monitoring activities of daily living in smart homes: Understanding human behavior. *IEEE Signal Processing Magazine 33*, 2 (2016), 81–94.

[22] Denzin, N. K. *Collecting and interpreting qualitative materials*, vol. 3. Sage, 2008.

[23] Elmqvist, N. Embodied human-data interaction. In *ACM CHI 2011 Workshop "Embodied Interaction: Theory and Practice in HCI"* (2011), ACM, pp. 104–107.

[24] Estrada-Jiménez, J.; Parra-Arnau, J.; Rodríguez-Hoyos, A.; Forné, J. Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications 100* (2017), 32–51.

[25] Fischer-Hübner, S.; Angulo, J.; Pulls, T. How can cloud users be supported in deciding on, tracking and controlling how their data are used? In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (2013), Springer, pp. 77–92.

[26] Haddadi, H. Human-data interaction. *Encyclopedia of Human Computer Interaction* (2016).

[27] Holzinger, A.; Plass, M.; Holzinger, K.; Crişan, G. C.; Pintea, C.-M.; Palade, V. Towards interactive machine learning (iml): applying ant colony algorithms to solve the traveling salesman problem with the human-in-the-loop approach. In *International Conference on Availability, Reliability, and Security* (2016), Springer, pp. 81–95.

[28] Hornung, H.; Pereira, R.; Baranauskas, M. C. C.; Liu, K. Challenges for human-data interaction–a semiotic perspective. In *International Conference on Human-Computer Interaction* (2015), Springer, pp. 37–48.

[29] Hornung, H.; Piccolo, L. S.; Arpetti, A. Human values: the gap between academia and industry. In *Proceedings of the 13th Brazilian Symposium on Human Factors in Computing Systems* (2014), Sociedade Brasileira de Computação, pp. 449–452.

[30] Jaatun, M. G.; Cruzes, D. S.; Angulo, J.; Fischer-Hübner, S. Accountability through transparency for cloud customers. In *International Conference on Cloud Computing and Services Science* (2015), Springer, pp. 38–57.

[31] Janic, M.; Wijbenga, J. P.; Veugen, T. Transparency enhancing tools (tets): an overview. In *2013 Third Workshop on Socio-Technical Aspects in Security and Trust* (2013), IEEE, pp. 18–25.

[32] Karegar, F.; Pulls, T.; Fischer-Hübner, S. Visualizing exports of personal data by exercising the right of data portability in the data track-are people ready for this? In *IFIP International Summer School on Privacy and Identity Management* (2016), Springer, pp. 164–181.

[33] Koreshoff, T. L.; Leong, T. W.; Robertson, T. Approaching a human-centred internet of things. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (2013), ACM, pp. 363–366.

[34] Kwon, Y.; Kang, K.; Bae, C. Unsupervised learning for human activity recognition using smartphone sensors. *Expert Systems with Applications 41*, 14 (2014), 6067–6074.

[35] Lathia, N.; Pejovic, V.; Rachuri, K. K.; Mascolo, C.; Musolesi, M.; Rentfrow, P. J. Smartphones for large-scale behavior change interventions. *IEEE Pervasive Computing*, 3 (2013), 66–73.

[36] Leitão, C.; Maciel, C.; Piccolo, L. S. G.; Salgado, L.; de Souza, P. C.; Prates, R.; Pereira, R.; Pereira, V. C. Human values in hci: a challenge for the grandihc-br. In *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems* (2017), ACM, p. 70.

[37] Leitão, C.; Maciel, C.; Piccolo, L. S. G.; Salgado, L.; de Souza, P. C.; Prates, R.; Pereira, R.; Pereira, V. C. Human values in hci: a challenge for the grandihc-br. In *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems* (2017), ACM, p. 70.

[38] Mortier, R.; Haddadi, H.; Henderson, T.; McAuley, D.; Crowcroft, J. Challenges & opportunities in human-data interaction. *University of Cambridge, Computer Laboratory* (2013).

[39] Mortier, R.; Haddadi, H.; Henderson, T.; McAuley, D.; Crowcroft, J. Human-data interaction: The human face of the data-driven society. *arXiv preprint arXiv:1412.6159* (2014).

[40] Mowery, D. L.; Park, A.; Bryan, C.; Conway, M. Towards automatically classifying depressive symptoms from twitter data for population health. In *Proceedings of the Workshop on Computational Modeling of People's Opinions, Personality, and Emotions in Social Media (PEOPLES)* (2016), pp. 182–191.

[41] Nagaraj, S. K.; Bryant, A. Factors in building transparent, usable and comprehensive user privacy policy system. In *11th International Conference on Cyber Warfare and Security: ICCWS2016* (2016), Academic Conferences and publishing limited, p. 253.

[42] Nicolescu, R.; Huth, M.; Radanliev, P.; De Roure, D. Mapping the values of iot. *Journal of Information Technology* (2018), 1–16.

[43] Nunes, L.; Alvão, C. M. Perspectives in sustainable interaction design: A preliminary discussion involving human values and hci. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (2017), vol. 61, SAGE Publications Sage CA: Los Angeles, CA, pp. 823–827.

[44] Pereira, R.; Baranauskas, M. C. C.; Liu, K. An essay on human values in hci. *SBC Journal on Interactive Systems 9*, 1 (2018), 4–16.

[45] Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context aware computing for the internet of things: A survey. *IEEE communications surveys & tutorials 16*, 1 (2014), 414–454.

[46] Prates, R. O.; Barbosa, S. D. J. Introdução à teoria e prática da interação humano computador fundamentada na engenharia semiótica. *Atualizações em informática* (2007), 263–326.

[47] Prates, R. O.; de Souza, C. S.; Barbosa, S. D. Methods and tools: a method for evaluating the communicability of user interfaces. *interactions 7*, 1 (2000), 31–38.

[48] Ruths, D.; Pfeffer, J. Social media for large studies of behavior. *Science 346*, 6213 (2014), 1063–1064.

[49] Seidelin, C.; Dittrich, Y.; Grönvall, E. Data work in a knowledge-broker organisation: how cross-organisational data maintenance shapes human data interactions. In *Proceedings of the 32nd International BCS Human Computer Interaction Conference* (2018), BCS Learning & Development Ltd., p. 14.

[50] Widjojo, E. A.; Chinthammit, W.; Engelke, U. Virtual reality-based human-data interaction. In *2017 International Symposium on Big Data Visual Analytics (BDVA)* (2017), IEEE, pp. 1–6.

APÊNDICE A - TERMO DE CONSENTIMENTO

Você foi convidado(a) para participar de um teste de avaliação da Interação Humano-Computador de um projeto de pesquisa que está avaliando o uso de Estratégias de Comunicação para viabilizar a Interação Humano-Dados (IHD). Essa avaliação utilizará os sistemas MyActivity e Privacy Badger, usados para tornar o uso e controle de dados pessoais mais transparente ao usuário. Neste teste, buscamos verificar indícios dos conceitos de IHD nos elementos de interface desses sistemas, durante a realização de tarefas específicas. Por essa razão, solicitamos seu consentimento para realização deste teste e, em seguida, uma breve entrevista. Para tanto, é importante que você tenha algumas informações :

- Os dados coletados durante o teste destinam-se estritamente a atividades de pesquisa e desenvolvimento;
- A equipe dessa pesquisa tem o compromisso de divulgar os resultados obtidos para fins acadêmicos. A divulgação desses resultados pauta-se no respeito a sua privacidade e o anonimato é preservado em quaisquer documentos elaborados.;
- O consentimento para o teste é uma escolha livre, feita mediante a prestação de todos os esclarecimentos necessários sobre a pesquisa;
- A realização do teste pode ser interrompida a qualquer momento, segundo a disponibilidade do participante. Nesse caso, a equipe se compromete a descartar o teste para fins da avaliação a que se destina;
- Nossa equipe se encontra disponível para contato através do telefone (21) 97038-3887, ou pelo e-mail patrickbarreto@id.uff.br. Caso queira tirar alguma dúvida, procure por Patrick Barreto.

De posse das informações acima, gostaríamos do seu pronunciamento acerca do teste, escolhendo uma das opções abaixo.

( ) Dou meu consentimento para realização do teste.
( ) Não autorizo sua realização.

Data do Teste: _____/_____/_____

_____ _____
Nome do Participante Nome do Avaliador

Caso você tenha optado por participar, por favor, responda ao breve questionário na próxima folha. Obrigado!

APÊNDICE B – QUESTIONÁRIO PRÉ-TESTE

QUESTIONÁRIO PRÉ-TESTE

1. Idade:

a. Até 18 anos

b. 19 – 29 anos

c. 30 – 39 anos

d. 40 – 49 anos

e. 50 – 59 anos

f. 60 anos ou mais.

2. Você atua em qual área?

a. Computação/Sistemas de Informação

b. Psicologia

c. Direito

d. Administração

e. Biologia

f. Matemática

g. Outra. Qual: _____

3. Você preocupa-se com questões relacionadas à Privacidade ou Transparência ao utilizar serviços ou produtos on-line?

a. Sim

b. Não

4. Tempo de experiência com navegação em sites usando:

a. Desktop/Notebook: ___ meses ou _____ anos

b. Tablets: _____ meses ou _____ anos

c. Smartphones: _____ meses ou _____ anos

5. Qual nível de conhecimento no idioma Inglês (leitura)?

a. Nenhum

b. Básico

c. Intermediário

d. Avançado

6. Já ouviu falar sobre as Ferramentas de Apoio à Transparência (Do inglês, *Transparency Enhancing Tools*)?

a. Sim

b. Não

7. Você já usou alguma ferramenta de apoio à transparência?

a. Sim

b. Não

8. Qual grau de habilidade você considera que possui para navegar em sites na Internet?

a. Em Desktops/Notebooks:

( ) Pouca

( ) Moderada

( ) Muita

b. Em Tablets:

( ) Pouca

( ) Moderada

( ) Muita

c. Em Smartphones:

( ) Pouca

( ) Moderada

( ) Muita

9. Você se sente familiarizado com algum(ns) termo(s) abaixo? Se sim, assinale-o(s) com um '[x]'.

a. [ ] 'Monitoramento não-consensual'

b. [ ]'Transparência e Privacidade Digital'

c. [ ] 'Domínio de Terceiros'

d. [ ] 'Trackers'

e. [ ] 'Monitoramento de Atividades'

10. Você prefere utilizar a sua conta de rede social, por exemplo, para se cadastrar de forma simplificada em aplicativos ou serviços online?

a. Sim

b. Não

11. Ao efetuar um cadastro online, você busca realizar configurações de privacidade?

a. Sim

b. Não

APÊNDICE C – CENÁRIOS E TAREFAS

- **Cenário 1:**

Luana realiza várias tarefas pelo smartphone. Todos os dias, ela acessa o noticiário, redes sociais, realiza pesquisas de interesse profissional e pessoal, busca opções de lazer e o melhor caminho no trânsito. Luana sempre optou em utilizar os serviços de grandes empresas, como a Google, devido à grande aceitação desses serviços por outros usuários e por conseguir acessar várias ferramentas e serviços com apenas uma conta.
Com isso, Luana busca experimentar uma navegação baseada nos seus gostos, interesses e em tipos de conteúdo consumido, evitando assim, receber notificações ou conteúdo desnecessários.
Recentemente, Luana foi notificada pelo Google a conhecer sua recente ferramenta de gerenciamento de Dados, o MyActivity. Segundo a proposta do MyActivity, Luana descobriu que pode gerenciar os serviços da empresa de modo que estes sejam mais úteis. Luana ficou surpresa em saber que pode exercer controle sobre seus dados ou atividades realizadas por meio do seu smartphone.

Agora, coloque-se no lugar da Luana e realize as seguintes tarefas:

(1) Navegue pelo MActivity nas opções do menu **"Controle de Atividade"**, **"Outra Atividade do Google"** e "**Enviar Feedback**" e descreva o que encontrou em cada.

(2) Com base na tarefa anterior, é possível identificar...

a. ...quais tipos de dados(atividades) o Google tem interesse em coletar sobre você? Se sim, descreva-os.

b. ...atividades que foram registradas?

c. ... opções que permitam realizar controle sobre os dados pessoais?

d. ... o que ocorre após clicar nas opções visualizadas?

e. ... reportar problemas de uso?

- **Cenário 2:**

João usa seu computador pessoal frequentemente para ler notícias, emails, pesquisar produtos, realizar compras online e acessar o internet banking. João faz uso de suas informações pessoais para realizar boa parte dessas ações. Assim, preocupado com o risco de invasão de privacidade por robôs de monitoramento, denominados '*trackers*', recorreu à algumas ferramentas de apoio à transparência, dentre elas, o Privacy Badger.

Agora, coloque-se no lugar do João e realize as seguintes tarefas no PrivacyBadger:

(1) Identifique, ao menos 3, possíveis domínios de terceiros classificados como "*trackers*" pelo software. Visualize a quantidade total de *trackers* identificados.

(2) Agora, realize o bloqueio de 2 domínios de terceiros que <u>não</u> tenham sido classificados como *trackers*.

APÊNDICE D – QUESTIONÁRIO PÓS-TESTE

Questionário OFICIAL (MyActivity e PB)

1. É possível relacionar esta tarefa com algum(ns) conceito(s) sobre IHD? Justifique?

   Quais elementos ou opções do sistema você considera como sendo uma forma de exercer o(s) conceito(s) identificado(s) na questão anterior? Justifique.