

UNIVERSIDADE FEDERAL DO PARANÁ

LUIZ ADOLPHO BARONI

DECEPTIVE PATTERNS SOB UMA VISÃO SOCIOTÉCNICA

CURITIBA PR

2023

LUIZ ADOLPHO BARONI

DECEPTIVE PATTERNS SOB UMA VISÃO SOCIOTÉCNICA

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Informática no Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Roberto Pereira.

CURITIBA PR

2023

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA DE CIÊNCIA E TECNOLOGIA

Baroni, Luiz Adolpho
Deceptive patterns sob uma visão sociotécnica / Luiz Adolpho Baroni. –
Curitiba, 2023.
1 recurso on-line : PDF.

Dissertação (Mestrado) - Universidade Federal do Paraná, Setor de
Ciências Exatas, Programa de Pós-Graduação em Informática.

Orientador: Roberto Pereira

1. Interfaces de usuário (Sistemas de computação). 2. Framework
(Arquivo de computador). 3. Semiótica. I. Universidade Federal do Paraná. II.
Programa de Pós-Graduação em Informática. III. Pereira, Roberto. IV .
Título.

Bibliotecário: Leticia Priscila Azevedo de Sousa CRB-9/2029



MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIÊNCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO INFORMÁTICA -
40001016034P5

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **LUIZ ADOLPHO BARONI** intitulada: **DECEPTIVE PATTERNS SOB UMA VISÃO SOCIOTÉCNICA**, sob orientação do Prof. Dr. ROBERTO PEREIRA, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 12 de Dezembro de 2023.

Assinatura Eletrônica

01/01/2024 21:34:07.0

ROBERTO PEREIRA

Presidente da Banca Examinadora

Assinatura Eletrônica

03/01/2024 16:01:42.0

GEORGE AUGUSTO VALENCA SANTOS

Avaliador Externo (UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO)

Assinatura Eletrônica

01/01/2024 15:08:32.0

LAURA SANCHEZ GARCIA

Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

*Dedico este trabalho aos meus pais,
pois sem eles este e muitos dos meus
sonhos não se realizariam.*

AGRADECIMENTOS

Escrevo esta carta de agradecimento com profunda gratidão e apreço pelo apoio e orientação valiosos que recebi ao longo do desenvolvimento da minha dissertação de mestrado, intitulada "DECEPTIVE PATTERNS SOB UMA VISÃO SOCIOTÉCNICA". É com grande satisfação que expresso minha gratidão a todas as pessoas e instituições que contribuíram para o sucesso deste projeto.

Primeiramente, gostaria de expressar minha sincera gratidão ao meu orientador, Professor Dr. Roberto Pereira, por sua orientação excepcional, paciência e dedicação ao longo de todo o processo. Sua experiência e visão foram fundamentais para moldar e aprimorar minha pesquisa, e estou verdadeiramente grato por ter tido a oportunidade de trabalhar sob sua supervisão.

Além disso, desejo estender meus agradecimentos aos membros da banca examinadora, Professora Dra. Laura Sánchez Garcia e Professor Dr. George Augusto Valença Santos, por dedicarem seu tempo e expertise para avaliar e enriquecer meu trabalho acadêmico.

Gostaria também de expressar minha gratidão aos colegas do grupo de pesquisa e amigos que proporcionaram um ambiente estimulante e encorajador durante esta jornada acadêmica. Suas discussões e insights foram inestimáveis para o desenvolvimento das ideias apresentadas na dissertação.

Agradeço também à CAPES pelo suporte financeiro que possibilitou a realização desta pesquisa.

Por fim, não posso deixar de agradecer à minha família, meus amigos, e especialmente minha mulher e meu psicólogo, por seu constante apoio emocional e encorajamento. Suas palavras de estímulo foram um farol durante os momentos desafiadores.

Em conjunto, todas essas contribuições foram essenciais para o sucesso deste projeto, e estou extremamente grato por ter tido a sorte de contar com uma rede tão solidária.

RESUMO

Deceptive patterns são padrões de interface que visam enganar o usuário ou favorecer interesses específicos, como os do proprietário ou projetista do software. Amplamente utilizados em diversas interfaces, como software, web e aplicativos, um exemplo notório é a colocação intencional de termos de compromisso em caixas de texto pequenas e difíceis de ler, escondendo cláusulas de compartilhamento de dados. Apesar de não serem novos, esses padrões continuam impactando negativamente a experiência do usuário e, por vezes, comprometendo a privacidade e bem-estar dos usuários. Esses comportamentos enganosos violam questões éticas e de privacidade, prejudicando a interação fluida do usuário com a interface. Considerados um fenômeno sociotécnico, envolvem interações humanas com a tecnologia, exigindo uma análise que leve em conta tanto as dimensões humanas (crenças, valores, emoções) quanto as técnicas (construção, tecnologia usada). No entanto, o mapeamento sistemático realizado nesta pesquisa revelou poucos estudos abordando de maneira abrangente os deceptive patterns, com a maioria focando em aspectos específicos, como listar tipos ou efeitos, sem adotar uma perspectiva sociotécnica. Isso representa um desafio, pois uma análise puramente social pode negligenciar aspectos técnicos, enquanto uma abordagem puramente técnica pode subestimar os impactos nos usuários. Assim, o objetivo deste estudo de mestrado é caracterizar deceptive patterns como um fenômeno sociotécnico, proporcionando uma compreensão mais abrangente e abrindo novas perspectivas de pesquisa e conscientização para usuários e desenvolvedores. Para isso, como contribuição empírica, foi analisado e caracterizado um deceptive pattern sob a luz da Semiótica Organizacional, utilizando o Framework Semiótico para representar e entender os aspectos sociotécnicos do padrão. Também, foi conduzido um mapeamento sistemático da literatura sobre deceptive patterns em Ciência da Computação para mapear os padrões que já foram identificados pela literatura científica. A partir do mapeamento, foram analisados quais aspectos sociotécnicos têm sido considerados ou negligenciados na literatura. Como contribuição técnica, foi construído um catálogo, totalmente em português, contendo todos os deceptive patterns encontrados na literatura, disponibilizado de forma aberta online para todos que queiram aprender mais sobre, conhecer diferentes tipos, entender os riscos e perigos, e como se proteger dos deceptive patterns.

Palavras-chave: Deceptive patterns 1. sociotécnico 2. interfaces de usuários 3.

ABSTRACT

Deceptive patterns are interface patterns that aim to deceive the user or favor specific interests, such as those of the software owner or designer. Widely used in various interfaces, such as software, web and applications, a notorious example is the intentional placement of terms of commitment in small and difficult to read text boxes, hiding data sharing clauses. Although not new, these standards continue to negatively impact the user experience and, at times, compromise users' privacy and well-being. These deceptive behaviors violate ethical and privacy issues, hindering the user's fluid interaction with the interface. Considered a socio-technical phenomenon, they involve human interactions with technology, requiring an analysis that takes into account both human dimensions (beliefs, values, emotions) and technical dimensions (construction, technology used). However, the systematic mapping carried out in this research revealed few studies comprehensively addressing deceptive patterns, with the majority focusing on specific aspects, such as listing types or effects, without adopting a sociotechnical perspective. This presents a challenge, as a purely social analysis may neglect technical aspects, while a purely technical approach may underestimate the impacts on users. Thus, the objective of this master's study is to characterize deceptive patterns as a socio-technical phenomenon, providing a more comprehensive understanding and opening new research and awareness perspectives for users and developers. To this end, as an empirical contribution, a deceptive pattern was analyzed and characterized under the light of Organizational Semiotics, using the Semiotic Framework to represent and understand the sociotechnical aspects of the pattern. Also, a systematic mapping of the literature on deceptive patterns in Computer Science was conducted to map the patterns that have already been identified in the scientific literature. From the mapping, we analyzed which sociotechnical aspects have been considered or neglected in the literature. As a technical contribution, a catalog was created, entirely in Portuguese, containing all the deceptive patterns found in the literature, made openly available online for everyone who wants to learn more about them, get to know different types, understand the risks and dangers, and how to protect themselves from them. deceptive patterns.

Keywords: Deceptive patterns 1. sociotechnical 2. user interfaces 3.

LISTA DE FIGURAS

1.1	Deceptive pattern conhecido como <i>Confirmshaming</i>	13
	13figure.caption.15	
1.3	deceptive pattern do tipo <i>Does not count</i> (Soe e et al., 2020).	14
1.4	Exemplo de Obstrução.	15
1.5	Exemplo de <i>Sneaking</i>	16
1.6	Exemplo de Interferência na Interface.	16
1.7	Banco de praça com barra metálica instalada, exemplo de deceptive pattern físico.	17
2.1	Resumo da metodologia.	19
4.1	Framework Semiótico de Ronal Stamper (Stamper, 1993)	23
4.2	Exemplo do deceptive pattern Hotel de Baratas	24
4.3	Continuação do exemplo do deceptive pattern Hotel de Baratas.. . . .	25
5.1	Distribuição de artigos através dos anos.	36
5.2	Tipos de publicação.	37
5.3	Veículos de publicação.. . . .	38
5.4	Tipos de domínio de aplicação que mais apareceram.	38
5.5	Contagem dos tipos de definições encontradas.	39
5.6	Os diferentes tipos de referenciais usados nos artigos.	40
5.7	Diagrama de Venn representando as categorias de problemas.. . . .	42
5.8	Quantidade de trabalhos que apresentaram algum estudo/avaliação/experimento.. . . .	43
5.9	Quantidade de artigos que se enquadram em cada camada.	43
6.1	Tela inicial do website.. . . .	48
6.2	Catálogo e categoria Desorientação.	49
6.3	Tela da categoria Desorientação.	49
6.4	Exemplos práticos de deceptive patterns implementados no website do catálogo.. . . .	50
6.5	Questionário de caracterização e respostas dos participantes.	52
6.6	Facilidade de Uso.. . . .	53
6.7	Questionário sobre a facilidade de uso.. . . .	54
6.8	Questionário sobre Utilidade Percebida.	54
6.9	Utilidade Percebida.. . . .	55

LISTA DE TABELAS

5.1	Objetivo do mapeamento sistemático.	30
5.2	Subquestões de pesquisa.	31
5.3	Crítérios de Inclusão e Exclusão	33
5.4	Tabela auxiliar do primeiro e segundo filtros.	33
5.5	Tabela de extração de dados.	35
5.6	Categorias identificadas de deceptive patterns e quantidade de tipos em cada uma.	37
5.7	Artigos separados por camadas do framework.. . . .	47
6.1	Resumo do estudo realizado com o catálogo.. . . .	51
6.2	Breve resumo do grupo focal.. . . .	55

LISTA DE ACRÔNIMOS

GDPR	General Data Protection Regulation
CCPA	California Consumer Privacy Act
LGPD	Lei Geral de Proteção de Dados Pessoais

SUMÁRIO

1	INTRODUÇÃO	12
1.1	PROBLEMA DE PESQUISA	15
1.2	OBJETIVO	17
1.3	MÉTODOS E RESULTADOS	17
2	METODOLOGIA	19
3	TRABALHOS RELACIONADOS	21
4	UMA PERSPECTIVA SOCIOTÉCNICA PARA DECEPTIVE PATTERNS.	23
4.1	ANALISE DO HOTEL DE BARATAS	24
4.2	DECEPTIVE PATTERNS SOB O FRAMEWORK SEMIÓTICO.	26
4.3	CARACTERIZANDO UM DECEPTIVE PATTERN COMO UM FENÔMENO SOCIOTÉCNICO.	27
4.4	RESULTADO PRÁTICO DA ANÁLISE.	29
5	PROTOCOLO E RESULTADOS DO MAPEAMENTO SISTEMÁTICO	30
5.1	OBJETIVO E QUESTÕES DE PESQUISA	30
5.2	ESCOPO E LÍNGUA	30
5.3	ESTRATÉGIA PARA SELEÇÃO DE ARTIGOS	32
5.4	ESTRATÉGIA PARA EXTRAÇÃO DE DADOS	32
5.5	ESTRATÉGIA PARA ANÁLISE DOS DADOS -CODIFICAÇÃO ABERTA/-DESCRITIVA.	35
5.6	RESULTADOS DO MAPEAMENTO SISTEMÁTICO	36
5.7	ASPECTOS SOCIOTÉCNICOS DA LITERATURA EM DECEPTIVE PATTERNS	43
5.8	GAPS DE PESQUISA E OPORTUNIDADES.	46
6	O CATÁLOGO DE DECEPTIVE PATTERNS	48
6.1	PÁGINA INICIAL DO CATÁLOGO.	49
6.2	PÁGINA DO CATÁLOGO	50
6.3	ESTUDO PARA ENTENDIMENTO DA ACEITAÇÃO DO CATÁLOGO	50
6.3.1	Resultados do Estudo	51
6.3.2	Facilidade de Uso e Utilidade Percebida	51
6.3.3	Grupo Focal.	53
7	CONCLUSÃO	56
7.1	ESTRATÉGIA DO CAPITALISMO	57
7.2	LIMITAÇÕES E AMEAÇAS A VALIDADE	58
7.3	CONTRIBUIÇÕES E TRABALHOS FUTUROS	58

REFERÊNCIAS	60
APÊNDICE A – ARTIGOS SELECIONADOS NO MAPEAMENTO SISTEMÁTICO	69
APÊNDICE B – VEÍCULOS DE PUBLICAÇÃO E QUANTIDADES DE VEZES QUE APARECERAM	75
APÊNDICE C – LISTA DE DECEPTIVE PATTERNS SEPARADOS POR CATEGORIA	77
APÊNDICE D – TEORIAS E CONCEITOS QUE APARECERAM NOS ARTIGOS	85
APÊNDICE E – EXPERIMENTOS E ESTUDOS ENCONTRADOS NOS ARTIGOS	89

1 INTRODUÇÃO

O conceito de padrões de design foi proposto originalmente por Christopher Alexander como um conceito da arquitetura e popularizado em seu livro de 1979 *“The Timeless Way of Building”* Alexander (1979). Em 1987, Kent e Cunningham adaptaram o conceito de padrão de design trazendo-o para a programação de computadores (Beck e Cunningham, 1987). Esses padrões de design foram criados para auxiliar os praticantes do design de software a resolverem problemas já conhecidos na comunidade de software: padrões que compreendem práticas ou soluções bem definidas e documentadas para problemas conhecidos dentro do design de software.

Um exemplo conhecido de padrão de design para interfaces de usuário é o *“Good Defaults”*¹ em tradução livre: Boas Predefinições. Quando um usuário precisa preencher um formulário em um site ou aplicativo, muitas vezes os valores que ele vai usar são os mesmos de outros usuários, então a interface já vem com valores pré definidos que facilitam o preenchimento do formulário para o usuário.

Além dos padrões de software há também os anti-padrões (*anti-patterns*), que são práticas ou soluções conhecidamente ruins, que buscam resolver algum problema mas acabam sendo ineficientes ou contraproducentes. O termo anti-padrão foi criado por Andrew Koenig em 1995 no seu livro intitulado *“Patterns and anti-patterns”* (Koenig, 1998). Aos anti-patterns se aplica a Navalha de Hanlon²: “nunca atribua à maldade aquilo que é adequadamente explicado pela estupidez”.

Um exemplo de anti-padrão muito usado é o *“Ambiguous link labeling”*³ em tradução livre: Rotulagem de link ambígua. Quando um site pretende redirecionar o usuário usando um link chamado apenas “Clique aqui!”. Muitos usuários acabam não entendendo como a ação deve ser realizada nem mesmo para onde o link irá redirecionar. Os anti-padrões são ruins por ignorância ou inexperiência do projetista/desenvolvedor.

Em 2010, Harry Brignull cunhou o termo *“dark patterns”*, em português: padrões obscuros, que são “truques usados em sites e aplicativos que levam você a fazer coisas que não pretendia, como comprar ou se inscrever em algo”⁴ (Brignull et al., 2023). Porém o autor abandonou o uso do termo “dark”afim de evitar uma linguagem que possa inadvertidamente conter associações negativas ou reforçar estereótipos prejudiciais, a própria ACM(*Association for Computing Machinery*) reconhece como inadequado o uso desse termo. Brignull também criou um site, o www.deceptive.design/, onde lista 12 tipos de deceptive patterns encontrados por ele ao longo de sua carreira como designer de experiência de usuário, dentre eles: Trick Questions (Perguntas Difíceis), Roach Motel (Hotel de Baratas), Privacy Zuckering (Invasão de Privacidade Zuckerberg), e outros. Ao longo do trabalho será utilizado o termo “deceptive patterns”, e interfaces maliciosas ou padrões enganosos e manipulativos como sinônimos.

Uma diferença essencial entre anti-patterns e deceptive patterns é a intencionalidade: enquanto um anti-pattern é ruim por culpa da falta de experiência ou de conhecimento do designer de software em projetar algo melhor, o deceptive pattern tem a intenção de enganar e explorar o usuário ou favorecer interesses de partes específicas (proprietário ou projetista do software, por exemplo) em detrimento do usuário. Outra diferença entre anti e deceptive patterns seria o grau de

¹Disponível em: <<http://ui-patterns.com/patterns/GoodDefaults>> Acesso em: 15 dez, 2021.

²Disponível em: <https://en.wikipedia.org/wiki/Hanlon's_razor> Acesso em: 12 out, 2021.

³Disponível em: <<http://ui-patterns.com/blog/User-Interface-AntiPatterns>> Acesso em: 15 dez, 2021.

⁴Tradução livre do autor. tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something.

complexidade: enquanto muitos deceptive patterns apresentam um grau maior de complexidade na sua construção e forma de manipulação, se utilizando de diferentes técnicas e interfaces elaboradas para a manipulação, os anti padrões, por serem fruto da falta de conhecimento ou técnica de seus autores, não costumam ser tão complexos em sua construção e funcionamento. A Figura 1.1 é um exemplo de um deceptive pattern conhecido como *Confirmshaming*, que tenta dissuadir o usuário a clicar na propaganda usando um apelo emocional. A Figura 1.2 traz um exemplo de anti-pattern que é mais recente, os desenvolvedores criam layouts de sites para celular, e quando esse mesmo site é aberto em uma tela maior, como um computador de mesa, o layout é apenas estendido para preencher a tela, sem considerar todo o espaço vazio que fica sobrando.



Figura 1.1: Deceptive pattern conhecido como *Confirmshaming*.

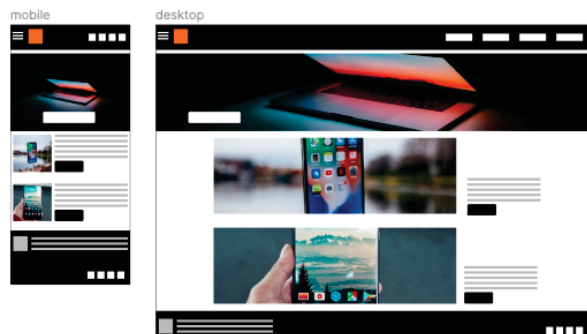


Figura 1.2: Anti-pattern onde o desenvolvedor/projetista usou um *layout* para celulares no website sem se preocupar com telas grandes⁵.

Deceptive patterns são construídos para influenciar o comportamento dos usuários (Acquisti e et al., 2017) a fim de beneficiar outras partes interessadas que não os próprios usuários, também podendo influenciar o comportamento de usuários (Utz e et al., 2019). Além disso, um estudo recente aponta que usuários são manipulados mesmo quando estão cientes de que isso vai acontecer (Bongard-Blanchy e et al., 2021).

As questões éticas levantadas pelos impactos de deceptive patterns também têm sido estudadas pela academia (Gray e et al., 2018; Lacey e Caudwell, 2019; Chivukula e et al., 2019; Di Geronimo e et al., 2020). deceptive patterns podem causar incômodo, frustração, raiva, e outras emoções em usuários (Maier e Harr, 2020; Gray e et al., 2021b). São conhecidos por manipular o comportamento dos usuários explorando vieses cognitivos (Mathur e et al., 2019) como, por exemplo, o “Framing effect” (Tversky e Kahneman, 1981): a tendência que humanos têm de chegar à diferentes conclusões a partir da mesma informação dependendo de como essa

⁵Fonte: <https://diti.site/blog/top-10-erros-de-design-em-websites-de-2021-por-jakob-nielsen>.

informação é apresentada. Nos deceptive patterns, a informação pode ser apresentada de maneira que reduza a autonomia de escolha dos usuários (Utz e et al., 2019). A Figura 1.3 traz um exemplo de deceptive pattern, um aviso de cookies do site que diz “Ao prosseguir você está concordando com nossa Política de Privacidade, incluindo o uso de cookies e outras tecnologias de rastreamento.”⁶. Esse tipo específico de deceptive pattern é chamado de “*Does not count*”, ou em português “Não vale”, pois se trata de uma forma inválida de conseguir o consentimento dos usuários.



Figura 1.3: deceptive pattern do tipo *Does not count*(Soe e et al., 2020).

Outros exemplos de deceptive patterns incluem: Na Figura 1.4 há um exemplo do tipo Obstrução: a interface de controle das notificações do aplicativo foi feita de forma a dificultar que o usuário desligue todos os tipos de notificações. Há 32 botões que precisam ser pressionados individualmente para desligar tudo.

A Figura 1.5 contém um exemplo de “*Sneaking*” uma tela de instalação de um programa, que contém uma opção em letras miúdas, que instala um programa terceiro caso o usuário não desative essa opção.

Finalmente, a Figura 1.6 representa um deceptive pattern do tipo Interferência na Interface: um *pop-up* aparece aleatoriamente enquanto se usa o celular, e esse *pop-up* bloqueia a tela impedindo o usuário de continuar o que fazia até que escolha alguma das opções: Cancelar ou OK.

Esse tipo de prática antiética tem ocorrido há décadas fora e dentro da internet, e tem ganhado cada vez mais atenção de pesquisadores na Ciência da Computação e principalmente de Interação Humano-Computador (IHC) (Mathur et al., 2021). Entretanto, apesar de estarem sendo explorados principalmente nas tecnologias digitais, os deceptive patterns já existem há muito tempo. Um exemplo são as empresas que oferecem períodos de teste grátis de seus produtos em troca de um cadastro do cliente (e.g., a assinatura de uma revista), mas ao se cadastrar a pessoa é obrigada a entregar suas informações do cartão de crédito e, chegado o término do período gratuito, a empresa não avisa o cliente e cobra automaticamente do cartão a assinatura do produto mesmo sem o cliente desejar.

Deceptive patterns também existem no mundo físico. A Figura 1.7 ilustra um exemplo de um banco de praça que não permite que uma pessoa se deite ou que duas pessoas se sentem juntas porque uma barra de metal foi colocada no meio do banco. O projeto desse banco é um deceptive pattern pois favorece os interesses de terceiros que não querem pessoas deitadas nos bancos das praças, ao custo dos interesses de cidadãos que queiram se deitar ou sentar junto de outra pessoa (por exemplo, os interesses da Prefeitura acima dos interesses do cidadão). Uma pessoa cansada procurando um lugar para descansar, um casal num encontro, ou uma mãe que quer sentar junto de seus filhos, serão forçados a se comportar de forma diferente do que esperavam ou desejavam quando forem interagir com o banco. A Figura 1.7 também é um exemplo de design opressivo (Gonzatto e Van Amstel, 2017), também conhecido como design

⁶Tradução livre do autor.

Categorias	E-mail	SMS	Push	WhatsApp
Oportunidades de investimentos Receba sugestões de investimentos selecionadas pelo nosso time de especialistas.	☒	☒	☒	☒
Conteúdos Conteúdos como newsletter, lives e vídeos pra que você se sinta cada vez mais seguro, confiante e com autonomia em relação ao seu dinheiro.	☒	☒	☒	☒
Eventos Receba convites para eventos online e presenciais.	☒	☒	☒	☒
Novidades da Marca Receba novidades sobre a Rico e o grupo XP Inc.	☒	☒	☒	☒
Análise independente Desejo receber conteúdos exclusivos e relatórios especiais da Spiti.	☒	☒	☒	☒
Relatórios Receba relatórios do Rico Matinal, demais relatórios da Rico e de Casas de análise independentes, como a Spiti, Eleven e Infomoney.	☒	☒	☒	☒
Pesquisas Receba convites para participar de pesquisas digitais e presenciais e ajude a Rico a tornar a sua experiência cada vez melhor.	☒	☒	☒	☒
Cursos Cursos gratuitos e pagos para ajudar você no mundo dos investimentos.	☒	☒	☒	☒

Salvar

Figura 1.4: Exemplo de Obstrução.

desagradável ou hostil (Savic e Savicic, 2014; Rosenberger, 2020), pois pré-determina quem poderá usar o banco e como. O design hostil tem sido relacionado com a Aporofobia, ou o ódio aos pobres.

Outro exemplo de deceptive pattern no mundo físico são as escadas rolantes dos shoppings, construídas de forma desconstruída, que exigem que o usuário percorra toda uma ala do shopping, passando na frente de várias lojas, para poder descer ou subir um nível do shopping. Portanto, é possível entender os deceptive patterns como um fenômeno sociotécnico: são decisões de design propositalmente aplicadas em artefatos técnicos, digitais ou físicos, para beneficiar uma terceira parte em detrimento de quem utiliza os artefatos. Para se manifestarem, deceptive patterns dependem tanto de aspectos técnicos que os operacionalizam e dão forma em um produto ou serviço, quanto de aspectos sociais que permeiam o contexto situado em que seu uso ocorre e tem sentido.

Baseado na literatura (Conti e Sobiesk, 2010; Gray et al., 2018; Mathur et al., 2021), é possível definir um deceptive pattern como: uma decisão de design propositalmente aplicada a artefatos técnicos, digitais ou físicos para beneficiar um terceiro em detrimento daqueles que usam estes artefatos.

1.1 PROBLEMA DE PESQUISA

Deceptive patterns podem estar presentes em qualquer tipo de interface e afetam de forma negativa o comportamento dos usuários, favorecendo o interesse de terceiros e podendo levar a



Figura 1.5: Exemplo de *Sneaking*.

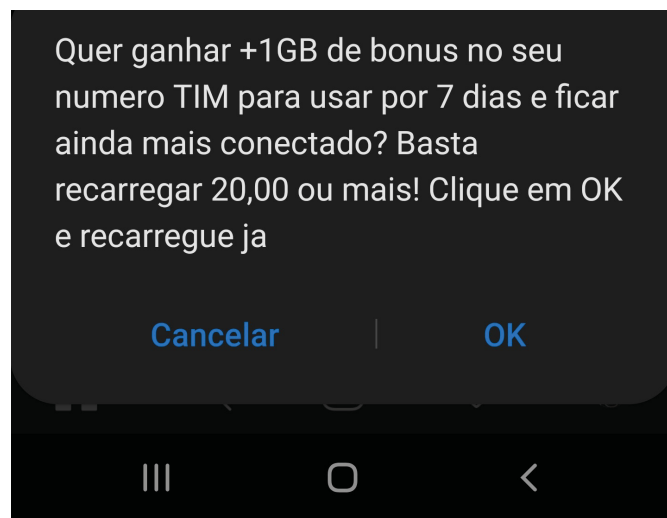


Figura 1.6: Exemplo de Interferência na Interface.

situações indesejadas, sentimentos ruins ou até mesmo perdas financeiras. Embora a literatura reconheça desafios em lidar com deceptive patterns, as pesquisas existentes normalmente têm focado em pontos específicos de deceptive patterns, e tratado esses pontos de forma isolada ou fragmentada. Sem uma caracterização dos deceptive patterns a partir de uma perspectiva que considere questões sociais e técnicas de forma associada, torna-se difícil desenvolver um entendimento de deceptive patterns como algo aplicado por meio de hardware e software (artefato técnico), e que influencia (molda, restringe) o comportamento das pessoas, impactando em seu mundo social.

Nos resultados do mapeamento sistemático conduzido no escopo desta pesquisa, o que se viu foram trabalhos que trazem discussões e análises focadas e limitadas a partes específicas do tema interfaces maliciosas como, por exemplo: apenas listar e categorizar tipos de deceptive patterns, apresentar opiniões de usuários dessas interfaces, discutir temas ligados à sociedade como ética e valores desses deceptive patterns, deixando de lado outros aspectos dos deceptive patterns que são fundamentais. Por exemplo: quem criou/financiou a criação desses padrões, como as empresas se aproveitam das capacidades do meio de transmissão para atrair e manipular, e como esses padrões são capazes de se aproveitar até mesmo do meio físico do usuário.

Portanto, até onde identificamos, há poucos artigos que apresentam esse tema sob uma visão sociotécnica, sistêmica. Nesses artigos ((Gray e et al., 2021a,b; Westin e Chiasson, 2021; Mathur et al., 2021)) os autores fazem uma análise sistêmica porém abrangente, entrando em diferentes áreas do conhecimento como Direito e Psicologia, mas sem se aprofundar nos detalhes



Figura 1.7: Banco de praça com barra metálica instalada, exemplo de deceptive pattern físico.

de funcionamento e como isso é implementado. Também, suas análises não são apoiadas por uma ferramenta como o Framework Semiótico, por exemplo. O que pode resultar em análises que deixam de lado pontos importantes das questões sociais envolvidas (manipulações e impactos no usuário e na sociedade) ou nas questões técnicas relacionadas (planejamento e construção das interfaces, características do meio de transmissão, impactos no mundo físico, etc.).

1.2 OBJETIVO

O objetivo geral desta pesquisa de mestrado é: **Caracterizar deceptive patterns como um fenômeno sociotécnico na Computação.**

Para alcançar esse objetivo, os seguintes objetivos específicos foram trabalhados:

1. Analisar e caracterizar um deceptive pattern a partir de uma visão sociotécnica;
2. Mapear a literatura sobre deceptive patterns na computação;
3. Elaborar um catálogo dos deceptive patterns mapeados.

1.3 MÉTODOS E RESULTADOS

Seguindo os objetivos específicos, os resultados obtidos foram:

1. A partir de uma análise qualitativa, informada pelo Framework Semiótico de StamperStamper (1993), feita considerando tanto as questões técnicas quanto às questões humanas envolvidas no fenômeno deceptive pattern, foi obtida uma ampliação do entendimento sobre o funcionamento dos deceptive patterns. Essa análise resultou em um artigo publicado e premiado no XX Simpósio Brasileiro de IHC, *Dark Patterns: Towards a Socio-technical Approach* (Baroni e et al., 2021).
2. A partir de um mapeamento sistemático da literatura foi obtido um panorama atual e rigoroso da literatura sobre deceptive patterns em Ciência da Computação.
3. Os aspectos sociotécnicos dos artigos encontrados no mapeamento também foram analisados utilizando o Framework Semiótico, e foram identificados pontos já estudados

e possíveis espaços para pesquisa, abrindo espaço para novas formas de se investigar deceptive patterns, contribuindo para o entendimento desse fenômeno de forma sistêmica e sociotécnica.

4. A partir do mapeamento um catálogo foi construído com os padrões encontrados na literatura, como contribuição técnica do trabalho. Este catálogo passou por uma avaliação com um grupo focal. E concluiu-se que o catálogo apoia a disseminação do conhecimento sobre os deceptive patterns já identificados na literatura para pesquisadores e profissionais que estejam buscando aprender sobre esse tema.

No Capítulo 2 é discutido o método do trabalho; no Capítulo 3 estão listados os trabalhos relacionados com o tema; e no Capítulo 4 é explicada a visão sociotécnica utilizada nas análises juntamente do resultado da análise do deceptive pattern Roach Motel; e no Capítulo 5 está o protocolo utilizado e os resultados obtidos no mapeamento sistemático da literatura. No Capítulo 6 está descrito o catálogo construído e o estudo realizado com participantes. Finalmente, no Capítulo 7 estão as conclusões do trabalho, os espaços para pesquisa e as possibilidades de estudos futuros.

2 METODOLOGIA

A metodologia empregada neste trabalho é apoiada em uma investigação analítico-construtiva, baseada no trabalho de Oulasvirta e Hornbæk (2016). Analítica: análise crítica e detalhada de um fenômeno, os deceptive patterns, para compreender melhor sua natureza, componentes, características e implicações; e construtiva: construção de um artefato técnico, o catálogo organizado, contendo os deceptive patterns citados na literatura; a Figura 2.1 traz um esquema resumindo a metodologia. A investigação analítica se deu em três etapas:

1. análise do deceptive pattern chamado *Roach Motel*;
2. mapeamento sistemático de literatura;
3. análise dos aspectos sociotécnicos considerados e negligenciados na literatura.

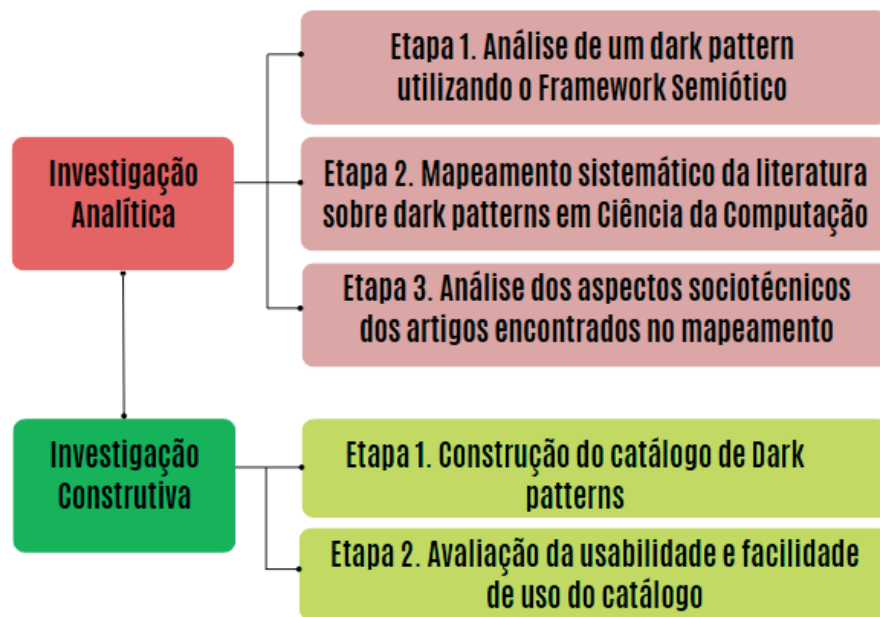


Figura 2.1: Resumo da metodologia.

Para garantir o rigor da pesquisa, todo o planejamento, execução e análise foi conduzida pelo autor deste trabalho, e validado por pelo menos outros dois pesquisadores¹.

Etapa 1. Análise de um deceptive pattern: um deceptive pattern conhecido como “Hotel de Baratas” foi analisado a partir de uma visão sociotécnica, considerando-se os aspectos sociais e técnicos que formam os deceptive patterns, e a partir dessa análise foi possível caracterizar os deceptive patterns como sendo um fenômeno sociotécnico. A análise foi fundamentada no Framework Semiótico, um artefato da Semiótica Organizacional que possibilita a análise de questões técnicas e humanas de forma integrada (Stamper, 1993). Ao utilizar o Framework Semiótico, torna-se possível olhar para o deceptive pattern como camadas interligadas entre si, partindo do Social e chegando no Físico (e vice-versa), e isso abre a possibilidade de analisar os deceptive patterns de diferentes ângulos, considerando que deceptive patterns são aplicados em

¹Dr. Roberto Pereira e Dr. Alisson Puska

artefatos técnicos com propriedades físicas e que eles causam impactos no mundo social e na vida das pessoas. O Framework Semiótico já tem sido aplicado na literatura para apoiar a análise de sistemas sociotécnicos (Maïke et al., 2015; Ferrari et al., 2019; Puska et al., 2020).

Etapla 2. Mapeamento sistemático de literatura: o mapeamento sistemático foi planejado e conduzido com base nas diretrizes de Kitchenham et al. (Kitchenham e Charters, 2007), com um protocolo previamente definido e analisado por outros dois pesquisadores. O mapeamento possui oito questões de pesquisa (QP):

- QP1: Quais deceptive patterns foram estudados/apresentados?
- QP2: A quais domínios de aplicação esses deceptive patterns estão relacionados?
- QP3: Como esses deceptive patterns são definidos?
- QP4: Como esses deceptive patterns estão sendo catalogados?
- QP5: Quais são as fundamentações teóricas das publicações?
- QP6: Quais são os problemas de pesquisa estudados?
- QP7: Qual é a principal contribuição dos artigos?
- QP8: Há alguma forma de avaliação ou experimento?

Ao todo, 97 artigos foram selecionados e passaram pelo processo de extração e análise. O protocolo e os resultados do mapeamento também foram validados pelos mesmos pesquisadores.

Etapla 3. Análise dos aspectos sociotécnicos: os resultados do mapeamento sistemático foram explorados para identificar aspectos sociotécnicos relevantes – do mundo físico ao mundo social – sendo considerados e negligenciados na literatura. O Framework Semiótico foi utilizado como artefato de base para a análise.

CITAR OUSLARVITA na construção Construtiva

Na *investigação construtiva*, como contribuição técnica, um catálogo contendo os deceptive patterns mapeados da literatura científica foi organizado, construído e apresentado. Este catálogo foi disponibilizado em forma de *website*², dividido em 3 páginas principais: a primeira página traz informações gerais sobre deceptive patterns, possíveis dúvidas dos usuários, e as informações de contato do autor; a segunda página traz um texto explicando mais a fundo sobre deceptive patterns; e a terceira página traz o catálogo propriamente dito, dividido em onze categorias diferentes, com todos os deceptive patterns encontrados na literatura. O catálogo foi então avaliado quanto a sua Facilidade de Uso e Utilidade Percebida por especialistas em IHC, sendo utilizado para a avaliação o Modelo de Aceitação de Tecnologia (TAM) (Davis, 1985) seguido de um grupo focal com os participantes. Até onde foi identificado, este é o único catálogo construído a partir de um mapeamento sistemático da literatura.

²<https://darkpattern.nicepage.io/>

3 TRABALHOS RELACIONADOS

Durante o mapeamento foi encontrado um trabalho intitulado "*What makes a dark pattern. . . dark?*" (Mathur et al., 2021) (em tradução livre: O que faz um padrão obscuro ser. . . obscuro?). Neste trabalho, Mathur et al. trazem uma revisão da literatura sobre deceptive patterns, porém não sistemática, e apresentam uma análise multidisciplinar, trazendo uma visão sistêmica do problema, e apontam inconsistências nas definições do fenômeno por parte dos pesquisadores, e mostram que há uma falta de uma base conceitual clara e consistente na literatura. Neste trabalho os autores apresentam uma visão a partir de diferentes disciplinas como a Economia Comportamental, a Filosofia, a Ética, e o Direito. Os autores propoem uma maneira de observar os deceptive patterns a partir de 4 lentes distintas: como os deceptive patterns diminuem o bem-estar individual, como diminuem o bem-estar coletivo, como interferem com regulações, e como deceptive patterns enfraquecem a autonomia individual.

Gray et al. (Gray e et al., 2018) revisitaram o trabalho original de Brignull e construíram, a partir dos 12 tipos de deceptive patterns originais, uma nova categorização. Por meio de uma coleta e análise de exemplos de deceptive patterns e dos 12 tipos originais, os autores criaram cinco categorias principais: Atrasando (*Nagging*), Obstruindo (*Obstruction*), Escondendo (*Sneaking*), Interferência na Interface (*Interface Interference*) e Ação Forçada (*Forced Action*). Os autores analisaram os deceptive patterns e concluíram que eles afetam a experiência e a interação do usuário por meio de duas dimensões específicas: a interpretação do usuário sobre o sistema e seu potencial, e as expectativas dos usuários sobre o resultado de suas ações no sistema. Há uma discussão interessante sobre diferentes dimensões impactadas (expectativas e interpretações) na experiência do usuário (UX) pelos deceptive patterns, porém os autores focam apenas nas que afetam diretamente o usuário e sua experiência de uso.

Mathur et al. (Mathur e et al., 2019) desenvolveram um *web crawler* que analisou aproximadamente 11 mil sites de compras. Os autores coletaram imagens e textos de cada site e encontraram ao menos um deceptive pattern em 11.1% dos sites analisados. A partir da análise desses resultados, os autores descobriram 15 tipos de deceptive patterns e, baseado nos trabalhos de Gray et al. (Gray e et al., 2018) e Brignull (Brignull et al., 2023), agruparam os deceptive patterns encontrados em 7 categorias principais: Escondendo (*Sneaking*), Urgência (*Urgency*), Direção Errada (*Misdirection*), Comprovação Social (*Social Proof*), Escassez (*Scarcity*), Obstrução (*Obstruction*), e Ação Forçada (*Forced Action*).

Gray et al. (Gray et al., 2023) afirmam que a falta de definições universalmente aceites no espaço acadêmico, legislativo e regulamentar provavelmente limitou o impacto que os estudos sobre deceptive patterns podem ter no apoio a sanções e na evolução das práticas de design. Com isso eles estudaram e agregaram taxonomias regulatórias e acadêmicas de padrões enganosos, propondo uma ontologia preliminar de três níveis para criar uma linguagem compartilhada que apoie a pesquisa interdisciplinar e a ação regulatória.

Outros autores também apresentam mais tipos de deceptive patterns: a “fofura” como um deceptive pattern em robôs (Lacey e Caudwell, 2019), deceptive patterns nas relações próximas (relações de proximidade e distância entre pessoas e objetos durante suas interações) (Greenberg e et al., 2014), e também deceptive patterns em jogos (Zagal et al., 2013). Há também trabalhos discutindo a visão dos usuários e a experiência deles com deceptive patterns (Bhoot et al., 2020; Di Geronimo e et al., 2020). Apesar de ser um tópico relativamente novo na Ciência da Computação, há um corpo relevante de literatura científica sobre o tema. Porém, esses artigos têm focado principalmente na identificação de tipos de deceptive patterns ou na análise

de aspectos específicos dos deceptive patterns em situações diversas, desconsiderando a natureza sociotécnica desses padrões. Ou seja, os artigos deixam de lado a natureza interconectada da relação entre um artefato técnico e pessoas no meio social, o que impede um entendimento completo e sistematizado dessas relações, podendo levar a análises incompletas ou mesmo conclusões precipitadas. O foco deste trabalho foi analisar justamente essa natureza sociotécnica, a relação entre diferentes “camadas” que existem desde o mundo social até o mundo físico que fazem parte da interação de um usuário com um deceptive pattern.

4 UMA PERSPECTIVA SOCIOTÉCNICA PARA DECEPTIVE PATTERNS

De acordo com danah boyd¹ (Boyd, 2008), “O estudo de fenômenos sociotécnicos é sobre entender as interseções entre tecnologias e práticas sociais.”². Deceptive patterns são aplicados em artefatos técnicos e causam impactos na vida social, como por exemplo a coleta de dados pessoais dos usuários muitas vezes sem consentimento claro (Bösch e et al., 2016), a invasão de privacidade (Lacey e Caudwell, 2019; Greenberg e et al., 2014), frustração emocional (Conti e Sobiesk, 2010; Bösch e et al., 2016), sendo assim importante analisá-los sob uma perspectiva sociotécnica a fim de não deixar de lado questões sociais importantes que estão interligadas a questões técnicas.

Uma ferramenta promissora para apoiar análises e estudos a partir de uma perspectiva sociotécnica é o Framework Semiótico (Stamper, 1993) proposto por Ronald Stamper. O framework considera, de forma integrada, a Plataforma Técnica e as Funções Humanas envolvidas no processo informacional – ver Figura 4.1. O framework é composto de seis camadas: Mundo Social, Pragmático, Semântico, Sintático, Empírico, e o Mundo Físico. A seguir cada camada é explicada mais em detalhes.

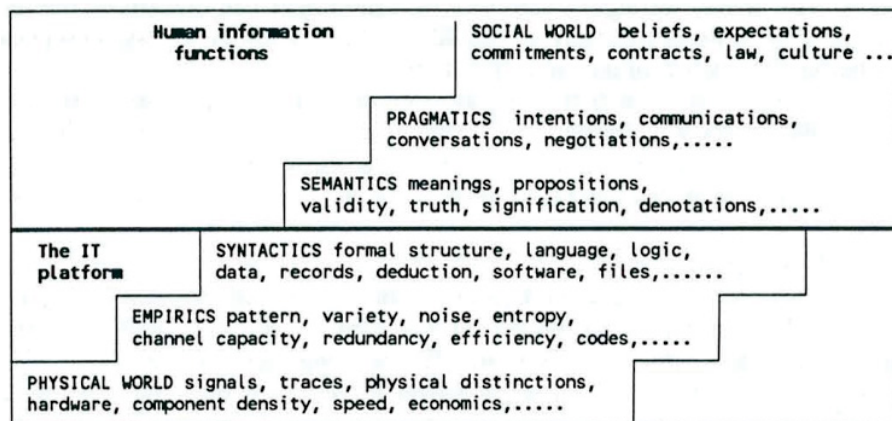


Figura 4.1: Framework Semiótico de Ronal Stamper (Stamper, 1993)

Mundo Social: Esta camada trata dos impactos do processo informacional no mundo social real e nas crenças e ações das pessoas (e vice-versa); envolve os valores, expectativas e compromissos das pessoas, a cultura dos indivíduos, as experiências pessoais que moldam as suas percepções e ações.

Pragmática: A camada pragmática trata das intenções incluídas nos signos, da relação entre essas intenções e a intenção do intérprete e do contexto em que o criador e o intérprete estão inseridos. Dado um contexto social, um sinal significativo de uma forma sintática compreensível é utilizado numa codificação adequada através de um determinado significado físico.

Semântica: Esta camada abrange a subjetividade individual dos sinais de cada parte que significam a interpretação no processo de informação. Trata-se da relação entre os signos utilizados e seus significados, e os significados das estruturas sintáticas.

Sintática: A camada sintática representa as estruturas formais complexas e os padrões construídos com sinais. Esta camada inclui a construção textual/visual, a linguagem formal

¹Grafia em letra minúscula pela própria autora.

²Tradução livre do autor: “The study of socio-technical phenomena is about understanding the intersections between technologies and social practices.”

utilizada, a lógica que os torna compreensíveis. A sintática trata das estruturas que fazem parte do processo informacional.

Empírico: Esta camada trata da codificação de signos, visto que existe uma camada física própria para ser codificada; também se preocupa com as propriedades estatísticas dos sinais, a probabilidade de cada sinal aparecer, os sinais de frequência que podem aparecer e a capacidade do canal de transmissão.

Mundo Físico: A camada física, a camada inferior no processo informacional, trata das formas físicas pelas quais os sinais podem ser representados. Inclui os meios físicos de representação (escritos, falados), como o tipo de hardware utilizado, um livro escrito ou a tela de um smartphone. Também inclui as propriedades físicas dos sinais, como material, necessidade de energia, tamanho, etc.

4.1 ANÁLISE DO HOTEL DE BARATAS

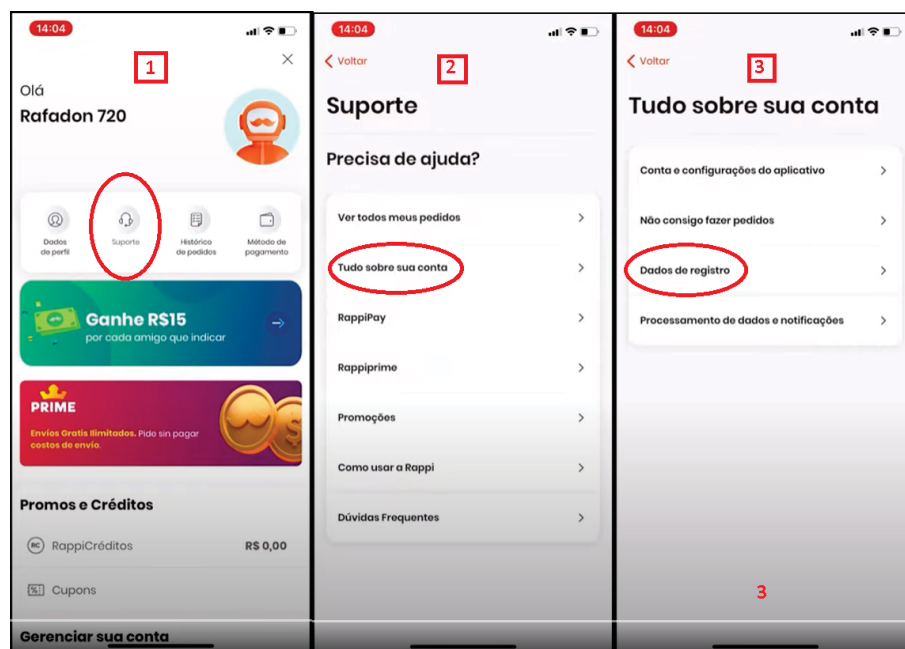


Figura 4.2: Exemplo do deceptive pattern Hotel de Baratas

Aqui apresentamos a análise de um deceptive pattern específico conhecido como Hotel de Baratas (4.1,4.3). O Hotel de Baratas é uma situação fácil de entrar porém difícil de sair, e geralmente é encontrado quando o usuário deseja deletar uma conta ou cancelar algum serviço. Esse deceptive pattern foi escolhido por ser um padrão que aparece constantemente em diversos serviços online, e por ser um exemplo onde fica perceptível como um artefato técnico é capaz de impactar negativamente de forma direta o mundo social.

As Figuras 4.2 e 4.3 trazem um exemplo do Hotel de Baratas durante o processo de exclusão de conta em um aplicativo, tornado difícil de forma proposital. Analisando o exemplo das Figuras 4.2 e 4.3 é possível perceber que o deceptive pattern afeta os usuários de formas diferentes, mas interligadas, nas seis camadas do Framework Semiótico:

Para deletar sua conta, o usuário deve primeiro passar por diversas telas, primeiro clicando em “Suporte” (Tela 1), depois em “Tudo sobre sua conta” (Tela 2), então em “Dados de registro” (Tela 3), para finalmente achar a opção “Cancelar a minha conta” (Tela 4). Ao utilizar a palavra “Cancelar”, há um impacto afetando a **camada semântica**, o usuário quer encerrar sua

conta, possivelmente deletar seus dados, e o aplicativo oferece apenas a opção de “Cancelar” a conta, cancelar não tem o mesmo sentido de deletar/excluir. Uma prática comum nesses casos é a de a empresa manter os dados do usuário mesmo após o pedido de encerramento de conta por parte do usuário, num conflito de interesses afetando a **camada pragmática**.

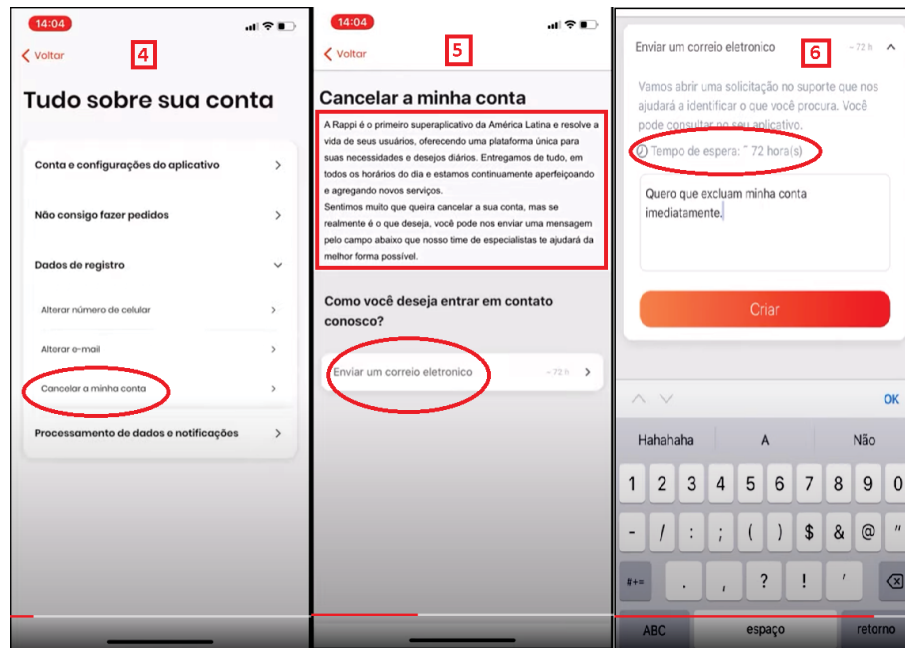


Figura 4.3: Continuação do exemplo do deceptive pattern Hotel de Baratas.

Dando continuidade, o usuário que acredita ter finalmente achado a opção para excluir sua conta se depara com uma longa mensagem (Tela 5). A primeira metade dessa mensagem contém apenas informações irrelevantes para o usuário, causando uma sobrecarga de informações na mente do usuário, afetando a **camada empírica**. E a segunda metade da mensagem, que se utiliza de palavras emocionalmente carregadas –“Sentimos muito que queira cancelar, mas se realmente é o que deseja . . .”– que afetam a **camada do mundo social**, também informa ao usuário que para deletar a conta será necessário o envio de um “correio eletrônico” para a equipe de suporte do aplicativo.

O usuário fica impossibilitado de realizar a exclusão sozinho já que fica dependendo da ação de terceiros, o que afeta a **camada sintática**. Então, ao clicar na opção de envio de mensagem, finalmente o usuário tem a possibilidade de fazer algo (Tela 6), neste caso para deletar sua conta, será necessário enviar um email para o suporte, que poderá realizar a ação em até 72 horas. Isso afeta a **camada do mundo físico**, forçando o usuário a realizar uma atividade secundária (enviar a mensagem) e o forçando a esperar um tempo variável que pode atrapalhar até mesmo outros planos do usuário.

O elevado uso de telas diferentes, a quantidade de palavras utilizadas, os passos extras adicionados no caminho do usuário (ter que enviar mensagem e esperar uma equipe de suporte), tudo isso está sendo explorado na **camada empírica**.

Nessa análise, é possível considerar que os deceptive patterns influenciam o comportamento de usuários, explorando desde as intenções das pessoas, seu grau de conhecimento, suas expectativas, como também exploram elementos da estrutura da interface, dos textos e imagens utilizados e o próprio mundo físico. Decisões de design aplicadas a artefatos técnicos que tiram dos usuários a possibilidade de tomarem escolhas informadas sobre suas ações, levando-os a situações indesejadas em suas vidas. Também pode-se constatar que o framework semiótico é

capaz de apoiar a análise sobre deceptive patterns ao olhar para o objeto analisado considerando-se desde as questões humanas do mundo social, até as questões técnicas do mundo físico. Isso permite caracterizar os deceptive patterns como um fenômeno sociotécnico, considerando de forma integrada elementos técnicos e sociais.

4.2 DECEPTIVE PATTERNS SOB O FRAMEWORK SEMIÓTICO

A intenção de influenciar o comportamento dos usuários para favorecer outras partes interessadas é um aspecto chave nos deceptive patterns. Essa intenção explora diferentes aspectos da plataforma técnica e das funções humanas. Os sistemas computacionais podem promover certos comportamentos sociais enquanto inibem outros (Fogg, 1999). Portanto, o que faz um deceptive pattern ser "*deceptive*" é se ele explora elementos em qualquer camada do framework contra os usuários. Um deceptive pattern, no entanto, tende a explorar diferentes elementos em diferentes camadas de forma interligada.

No **Mundo Social**, os deceptive patterns têm impactos profundos na vida dos usuários e podem influenciar comportamentos e escolhas. Nesta camada, a preocupação é com os efeitos negativos na vida dos usuários e na sociedade, considerando também os impactos das características socioculturais, emoções, expectativas, e valores pessoais dos usuários em como eles interagem e percebem os deceptive patterns. É também na camada social que os construtores de deceptive patterns extraem informações relevantes contra usuários, explorando características individuais como idade, crenças pessoais, e contexto social.

Explorando a camada **Pragmática**, os deceptive patterns tiram vantagem das diferentes intenções e expectativas das partes envolvidas (e.g., usuários, designers, organizações). Idealmente, um sistema computacional deveria suportar a negociação dessas intenções e interesses para o bem comum de todos os envolvidos ou afetados pelo sistema e pelas ações/tarefas que ele oferece. Deceptive patterns exploram as intenções dos usuários a fim de persuadi-los ou forçá-los a se comportarem de acordo com as intenções de outras partes.

Os deceptive patterns também exploram a **Semântica** por trás dos elementos utilizados, como botões, textos, imagens, cores, palavras, e estruturas construídas para enganar. Esta camada trata sobre o que os elementos dos deceptive patterns podem significar para os usuários e como os significados escondidos podem impactar os usuários.

Explorando a camada **Sintática**, por sua vez, deceptive patterns podem tirar vantagem da construção e das estruturas das tarefas, e na forma como elementos são organizados e combinados para formar estruturas complexas que enganam e manipulam. A linguagem usada, a construção das frases, a posição de elementos na tela (e.g., botões, imagens, textos) podem ser manipuladas para enganar usuários.

Na camada **Empírica** são exploradas as propriedades estatísticas dos elementos dos deceptive patterns, como quantidade e tamanho do texto, tamanho, relação entre o tamanho dos botões e o espaço de visualização, combinação de cores, frequência de atualização, taxa de atualização da tela, alteração (real ou aparente) do tempo de resposta da aplicação, e como essas propriedades podem afetar os usuários. Esses elementos são usados de diferentes formas para impactar negativamente as ações e escolhas dos usuários.

No **Mundo Físico**, os deceptive patterns exploram propriedades físicas dos dispositivos e infraestruturas contra os usuários. Se os usuários usam um aplicativo em um smartphone com tela de toque, o tamanho da interface pode ser explorado para tornar a interação difícil e cansativa. Ao restringir a interação a apenas dispositivos de apontamento (e.g., um mouse), várias ações difíceis de clicar podem ser necessárias para desmotivar e cansar os usuários. Quando usando teclado, os deceptive patterns podem forçar os usuários a escreverem longos textos e a lembrarem

informações específicas. deceptive patterns podem explorar o mundo físico para forçar as pessoas a tomarem decisões ou se comportarem de formas que não queriam.

4.3 CARACTERIZANDO UM DECEPTIVE PATTERN COMO UM FENÔMENO SOCIO-TÉCNICO

Os deceptive patterns causam sofrimento emocional/econômico, favorecendo os interesses de terceiros que não os usuários (*mundo social*); frustrar as intenções e expectativas dos usuários (*pragmática*); aumentando o esforço mental e afetando a capacidade de compreensão (*semântica*); alterar a estrutura das tarefas, a posição/tamanho/cor dos elementos (*sintática*); aumentar a frequência/quantidade de elementos com os quais o usuário tem que lidar (*empíricos*); aproveitar estruturas físicas ou aumentar o esforço físico dos usuários (*mundo físico*);

Se considerada isoladamente, cada camada oferece uma visão prática mas fragmentada do fenômeno. Por exemplo, olhando para os deceptive patterns apenas de um ponto de vista técnico, podemos não perceber muito do mundo social – as crenças e o conhecimento pessoal dos utilizadores afetam e são afetados pelos aspectos técnicos da estrutura. Porém, quando considerada de forma interligada, cada camada revela aspectos ou elementos que influenciam os aspectos e elementos de outras camadas: questões técnicas influenciam a forma como as pessoas entendem e usam os sistemas e, conseqüentemente, o seu impacto na sociedade. Esta análise abre possibilidades para uma melhor compreensão dos deceptive patterns e para informar a investigação e o desenvolvimento no que diz respeito à identificação e ao tratamento dos mesmos, sensibilizando os utilizadores e designers.

Do **Mundo Social**, os deceptive patterns podem explorar o contexto do sistema/objeto que está sendo usado e os valores, preferências ou padrões de comportamento das pessoas que podem ser explorados contra os usuários. O foco principal dos deceptive patterns é enganar ou desfavorecer os usuários no sentido de beneficiar outras partes interessadas. Nesta camada, os impactos e conseqüências dos deceptive patterns podem ser vistos e sentidos. Principalmente emocionais Maier e Harr (2020); Gray et al. (2020) mas também impactos monetários, por exemplo. No mundo social, os deceptive patterns podem explorar as características das pessoas, tais como preferências ou inclinações políticas. Eles podem tirar vantagem dos usuários envergonhando-os, afetando-os emocionalmente por não clicarem em um botão (ConfirmShaming Brignull et al. (2023)). Eles podem aproveitar que as pessoas tendem a escolher o caminho mais fácil e aumentar deliberadamente a carga de trabalho para concluir uma ação, de modo que os usuários se sintam menos inclinados a prosseguir (Roach Motel Brignull et al. (2023), Hard to Cancel Mathur e et al. (2019)). Os deceptive patterns podem aproveitar a distração ou o cansaço dos usuários, disfarçando os anúncios como conteúdo genuíno na interface/sistema (Disguised Ad Brignull et al. (2023)).

Os deceptive patterns exploram as expectativas e intenções das pessoas, na camada **Pragmática**. Quando os usuários interagem com um sistema, por exemplo, clicando em um botão, eles esperam uma reação do sistema. Os deceptive patterns aproveitam essas expectativas para induzir os usuários a algo que eles não estariam dispostos a fazer - por exemplo, quando os usuários desejam baixar algo e há dezenas de botões de download na tela (Disguised Ad Brignull et al. (2023)) . Aquele por trás do padrão escuro torna os processos mais difíceis de serem executados. Os deceptive patterns exploram as intenções dos usuários de fazer algo, criando uma falsa demanda ou sugerindo uma falsa urgência (Scarcity Mathur e et al. (2019)). Os deceptive patterns podem explorar as intenções dos usuários de progredir em uma atividade (por exemplo, um jogo online), forçando os usuários a enviar convites aos seus amigos (Esquemas de Pirâmide Social Zagal et al. (2013)).

Quando se trata das habilidades de interpretação das pessoas, os deceptive patterns podem afetar o conhecimento prévio e a educação dos usuários, na camada **Semântica**. Podem dificultar a compreensão dos textos, sobrecarregando os usuários; ou tornam o uso da interface confuso, favorecendo ações específicas a outras. Por exemplo, quando os sites pedem aos usuários que permitam cookies que rastreiam dados pessoais, eles se aproveitam do fato de que a maioria dos usuários não tem conhecimento técnico e não entende o que são cookies, então pedem permissão usando frases genéricas e oferecem apenas um botão Aceitar Utz e et al. (2019). Outro exemplo: quando os usuários estão preenchendo um formulário on-line e respondem a uma pergunta criada para induzi-los a dar uma resposta indesejada, como permitir que o formulário colete e use seus dados (Perguntas capciosas Mathur e et al. (2019); Brignull et al. (2023), Confusion Conti e Sobiesk (2010)), o deceptive pattern está explorando o conhecimento e a interpretação dos usuários.

Os deceptive patterns exploram as propriedades da interface e seus elementos ou exploram a tarefa que os usuários desejam realizar para persuadi-los ou enganá-los a fazer algo que não pretendiam fazer, na camada **Sintática**. Eles podem explorar a interface alterando a posição dos elementos de onde os usuários estão acostumados (por exemplo, invertendo inadvertidamente os botões confirmar ou cancelar). Eles podem bloquear a tela, interrompendo os usuários e forçando-os a fazer outra coisa para continuar o que estavam fazendo antes. Por exemplo, alguns aplicativos forçam os usuários a assistir a um vídeo publicitário após alguma ação para continuar usando o aplicativo (Interferência de interface Gray e et al. (2018), Ação forçada Gray e et al. (2018)). Na Figura 1.7, o banco do parque não permite deitar, pois o padrão escuro modificou a estrutura do banco, acrescentando um novo elemento: então, se o usuário quiser tirar uma soneca, não poderá mais fazê-lo naquele banco. Os deceptive patterns podem modificar o tamanho de elementos essenciais na interface para favorecer outras opções que não tenham em mente os melhores interesses dos usuários. O esquema de cores pode variar para algo mais atraente, então os usuários compram a opção mais cara. Em sites de compras, os deceptive patterns podem facilmente impedir que os usuários comparem preços de produtos semelhantes, induzindo o processo de compra (Price Comparison Prevention Brignull et al. (2023)).

Os deceptive patterns exploram as propriedades do meio, como capacidade e tempo de resposta, sobrecarregando as capacidades cognitivas das pessoas, na camada **Empírica**. Eles exploram a capacidade do meio, por exemplo, aumentando a quantidade de texto ou opções mostradas na tela aos usuários (Misdirection Brignull et al. (2023), Distraction Conti e Sobiesk (2010)); ou explorar o tempo de carregamento de recursos que os usuários podem precisar com anúncios em vídeo (Obstrução Gray e et al. (2018), Interrupção Conti e Sobiesk (2010)). Um padrão escuro pode explorar a capacidade cognitiva dos usuários, mostrando tantas opções na tela que os usuários não sabem onde clicar, ou exigindo que os usuários se lembrem de ações ou informações anteriores para prosseguir. Por exemplo, se os usuários desejarem desativar as notificações, um padrão escuro pode: i) fazer com que os usuários percorram uma lista de notificações que podem ser desativadas individualmente sem oferecer a opção “Desativar todas as notificações”; ii) exigir confirmação desnecessária para cada opção; e iii) atrasar o tempo de resposta do sistema após cada confirmação. Por ser uma tarefa árdua, os usuários podem se sentir sobrecarregados e dissuadidos de concluí-la.

Os deceptive patterns exploram propriedades físicas como o tamanho de uma tela, afetando a quantidade de esforço físico que os usuários precisam fazer, no **Mundo Físico**. Os deceptive patterns podem explorar o mundo físico dos usuários, fazendo com que eles realizem outras ações em vez de interagir com a interface/sistema/objeto (por exemplo, para fazer uma chamada telefônica). Eles também podem explorar características do meio físico, aproveitando que os usuários podem não conseguir alterar as propriedades físicas da interface para evitar o

padrão escuro. Eles podem aumentar a quantidade de esforço físico que os usuários precisam fazer para atingir uma meta, como escrever longas respostas em um smartphone ou enviar uma carta para cancelar a assinatura de um serviço. Padrões físicos escuros, como o banco da Figura 1.7, usam características físicas para afastar as pessoas, como uma barra de metal que impede uma pessoa de se deitar; ou os espetos colocados em frente aos estabelecimentos comerciais para desencorajar as pessoas de se sentarem ali. Além disso, os deceptive patterns podem explorar o mundo físico através de incompatibilidades de hardware projetadas, forçando os usuários a comprar adaptadores ou trocar seus antigos dispositivos incompatíveis por novos, mesmo entre produtos da mesma marca.

Olhar os deceptive patterns de forma estratificada fornece diferentes perspectivas para analisá-los e estudá-los, considerando elementos sociotécnicos. A perspectiva em camadas pode mostrar detalhes de elementos de cada camada que podem não ser vistos em uma análise não estruturada. Cada camada está ligada à anterior e à posterior, formando uma interconexão dentro de padrões sombrios sociais, técnicos e físicos. Argumentamos que uma análise de deceptive patterns sem uma visão multifocal, que considere as características sociotécnicas, acabará por deixar de lado elementos ou partes essenciais para a compreensão de todo o padrão escuro e seus efeitos.

4.4 RESULTADO PRÁTICO DA ANÁLISE

Cumprindo o primeiro objetivo específico, a fim de investigar o potencial do Framework Semiótico (Stamper, 1993) como ferramenta de análise de deceptive patterns, foi realizada uma análise de um deceptive pattern específico conhecido como Hotel de Baratas (4.1,4.3). O Hotel de Baratas é uma situação fácil de entrar porém difícil de sair, e geralmente é encontrado quando o usuário deseja deletar uma conta ou cancelar algum serviço. Essa análise foi revisada e discutida com outros três pesquisadores com conhecimento prévio em semiótica, sendo dois deles já experientes em análises com o framework semiótico, a fim de garantir o rigor da análise na pesquisa.

Essa análise (4.1,4.3) resultou em um artigo, que foi publicado no XX Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais, premiado como o melhor artigo da trilha de Ideias Inovadoras e Resultados Emergentes, e denominado: “Dark Patterns: Towards a Socio-Technical Approach” (Baroni e et al., 2021). No estudo, foi identificado que o framework semiótico é capaz de aprofundar a análise do funcionamento de um deceptive pattern, explorando detalhes que poderiam passar despercebidos em uma análise puramente técnica, como, por exemplo, os impactos sociais e emocionais de se enganar ou incomodar os usuários.

5 PROTOCOLO E RESULTADOS DO MAPEAMENTO SISTEMÁTICO

O mapeamento sistemático da literatura foi planejado e conduzido baseado nas diretrizes de Kitchenham et al. (Kitchenham e Charters, 2007). Uma chave de busca foi construída e usada em bibliotecas digitais para obter uma lista de publicações científicas relevantes aos objetivos do mapeamento. Essas publicações passaram por diferentes etapas para que as publicações não relacionadas pudessem ser retiradas. No final, os dados dessas publicações foram extraídos e serão analisados, favorecendo o rigor científico e a reprodutibilidade.

5.1 OBJETIVO E QUESTÕES DE PESQUISA

O **objetivo principal** do mapeamento, baseado no paradigma GQM (Goal-Question-Metric) (Basili e Rombach, 1988), (Tabela 5.1) é identificar e analisar as pesquisas científicas sobre deceptive patterns na literatura em Ciência da Computação. Os objetivos específicos são:

- 1. encontrar e identificar quaisquer deceptive patterns já estudados/apresentados pela literatura em Ciência da Computação; e
- 2. analisar como os pesquisadores têm estudado e catalogado deceptive patterns.

A principal **questão de pesquisa** é "*Qual é o estado da arte em deceptive patterns na literatura de computação?*" A definição de deceptive pattern usada é dada por Bösch: "... uma solução estabelecida para explorar e enganar os usuários de uma forma genérica"¹ (Bösch e et al., 2016). A definição é intencionalmente ampla para que a pesquisa possa incorporar tantos deceptive patterns diferentes quanto possível. A Tabela 5.2 traz as sub-questões que foram definidas para ajudar a responder à questão principal.

5.2 ESCOPO E LÍNGUA

A construção de uma boa chave de busca é importante para garantir um resultado representativo nos motores de busca das bibliotecas digitais. Uma chave de busca foi construída baseada no modelo **PICOC**, População (*Population*), Intervenção (*Intervention*), Comparação (*Comparison*), Resultado (*Outcome*) e Contexto (*Context*) (Kitchenham e Charters, 2007), mas usando apenas a parte da População, a fim de não limitar os resultados da busca. A chave de busca foi construída a partir de uma busca no Google Acadêmico usando a expressão "dark patterns" (com as aspas). À época o termo "dark patterns" ainda era amplamente utilizado.

¹Tradução livre do autor: (an established solution for exploiting and deceiving users in a generic form)

analisar	publicações científicas
com o propósito de	identificar e catalogar deceptive patterns
em relação a	tipos de deceptive patterns e possíveis categorias, suas características e métodos para identificação
do ponto de vista de	pesquisadores da Ciência da Computação
no seguinte contexto	interfaces de usuário

Tabela 5.1: Objetivo do mapeamento sistemático.

Subquestões	Explicação
QP1 - Quais deceptive patterns foram estudados/apresentados?	Para encontrar os deceptive patterns já reportados na literatura científica e compreender melhor o estado da arte em deceptive patterns na literatura da computação.
QP2 - Quais os domínios de aplicação os artigos focam que são relacionados a deceptive patterns?	Para entender se existe alguma relação entre os domínios e a presença de deceptive patterns (websites, compras online, propagandas, etc) e comparar o quanto deceptive patterns são usados em diferentes domínios.
QP3 - Como esses deceptive patterns são definidos?	Para entender como os cientistas estão definindo deceptive patterns, e comparar essas definições, com o objetivo de encontrar uma definição geral. Essa definição geral pode ajudar no processo de identificação de um deceptive pattern.
QP4 - Como esses deceptive patterns estão sendo catalogados?	Para ver se há algum esquema de categorização/classificação sendo usado para catalogar os deceptive patterns. Como funciona esse esquema e se pode ser utilizado de forma generalizada.
QP5 - Quais são as fundamentações ou ferramentas teóricas das publicações?	Para identificar bases metodológicas e teóricas que possam fundamentar a pesquisa em deceptive patterns.
QP6 - Qual é o problema de pesquisa estudado?	Para entender o contexto do deceptive pattern apresentado/estudado e ver os problemas mais e menos estudados, procurando por problemas não resolvidos e gaps de pesquisa.
QP7 - Qual é a principal contribuição do artigo?	Para identificar quais pontos são atacados pelos pesquisadores, e possíveis gaps de pesquisa.
QP8 - Há alguma forma de avaliação ou experimento?	Para identificar quais os aspectos avaliados pelos pesquisadores na pesquisa em deceptive patterns.

Tabela 5.2: Subquestões de pesquisa.

O filtro de ordenação dos resultados do Google Acadêmico foi mantido no padrão, ou seja, os resultados foram listados de acordo com a relevância de cada artigo naquele momento. Então, as dez primeiras publicações que apareceram naquele momento foram escolhidas (Zagal et al., 2013; Bösch e et al., 2016; Gray e et al., 2018; Mathur e et al., 2019; Nouwens e et al., 2020; Greenberg e et al., 2014; Trice e Potts, 2018; Chromik e et al., 2019; Lacey e Caudwell, 2019; Conti e Sobiesk, 2010). As palavras-chave dessas dez publicações foram usadas na busca por termos relevantes, que foram usados na construção da seguinte chave de busca:

"dark pattern"OR "dark patterns"OR "malicious interface"OR "evil interface"OR "dark design pattern"OR "dark design patterns"OR "dark side"OR "dark strategies"OR "dark strategy"OR "dark interface"

Posteriormente o termo "deceptive pattern" foi incluído na chave de busca e os resultados foram comparados aos obtidos sem a inclusão do termo, e concluiu-se que nenhum artigo relevante para o trabalho foi deixado de fora pela falta do termo à época da pesquisa.

As seguintes bibliotecas digitais foram escolhidas para o mapeamento por serem as principais e mais conhecidas bibliotecas na área de Ciência da Computação:

- ACM Digital Library;
- IEEEExplore;
- Scopus (a busca foi limitada a Ciência da Computação).

A língua escolhida para o mapeamento sistemático foi o inglês, por ser a principal língua usada em publicações internacionais em Ciência da Computação.

5.3 ESTRATÉGIA PARA SELEÇÃO DE ARTIGOS

As publicações científicas encontradas nas bibliotecas digitais foram selecionadas por meio de um processo de dois filtros em que foram aplicados os critérios de inclusão e exclusão apresentados na Tabela 5.3. O primeiro filtro consiste na análise do título e do resumo das publicações. E o segundo filtro é uma leitura das seções de introdução e conclusão das publicações que passaram no primeiro filtro. Se após o segundo filtro ainda há dúvidas quanto a publicação, ela é lida na íntegra a fim de ter certeza sobre incluir/excluir a publicação. Finalmente, todas as publicações que atenderem aos critérios de inclusão, após os dois filtros, irão passar para a fase de extração. O primeiro e segundo filtros foram conduzidos por dois pesquisadores, ambos com experiência prévia em mapeamentos sistemáticos, a fim de reduzir o viés de seleção. O coeficiente Cohen-Kappa (Landis e Koch, 1977) foi usado para calcular a concordância entre os pesquisadores, com um coeficiente resultante de 0,8183 (concordância Quase Perfeita). Na Tabela 5.3 estão os critérios de inclusão e exclusão usados nos dois filtros de seleção:

5.4 ESTRATÉGIA PARA EXTRAÇÃO DE DADOS

Os artigos selecionados passaram pela fase de extração de dados. Durante o primeiro e segundo filtros, a Tabela 5.4 foi utilizada para ajudar a organizar e extrair os metadados. O ID é atribuído individualmente para cada publicação para controle. A seguir a lista de metadados extraídos:

- MD1 (Metadados 1): Título da publicação;

Critério de Inclusão: Publicações científicas relacionadas a deceptive patterns em Ciência da Computação;	Artigos que abordam deceptive patterns em Ciência da Computação.
Critério de Exclusão 1 (CE1): conteúdo não aborda diretamente deceptive patterns em Ciência da Computação;	Artigos cujo foco não esteja relacionado a deceptive Patterns na Ciência da Computação.
CE2: artigo não está em inglês;	Qualquer outra língua que não o inglês.
CE3: duplicatas: artigo retornado em mais de uma biblioteca digital;	Duplicatas indexadas por diferentes bibliotecas digitais.
CE4: artigos com extensões;	No caso dos artigos publicados como extensão de outro trabalho, o mais completo é o escolhido.
CE5: não acessível;	Artigos cujo texto completo não está disponível para acesso ou que requerem pagamento.

Tabela 5.3: Critérios de Inclusão e Exclusão

ID	Título	Ano	Resumo	Autores	Instituição	Tipo	Veículo	Critérios I/E	Comentários

Tabela 5.4: Tabela auxiliar do primeiro e segundo filtros.

- MD2: Ano da publicação;
- MD3: Autores;
- MD4: Instituição dos autores;
- MD5: Tipo de publicação; (Journal, Evento);
- MD6: Veículo de publicação;

Todos os artigos que passaram pelo primeiro e segundo filtros foram lidos na íntegra para garantir que estejam de fato dentro do escopo do mapeamento. Então, os dados foram extraídos baseado nas sub-questões de pesquisa definidas anteriormente e, depois de extraídos, os dados serão revisados e analisados. A extração acompanha a Tabela de Extração de Dados (Tabela 5.5), onde constam os valores exatos que devem ser extraídos do texto do artigo. Cada uma das sub-questões de pesquisa tem um ou mais dados relacionados a ela, e cada dado descrito na Tabela 3 será extraído do texto do artigo. Alguns dados deverão ser inferidos pelos pesquisadores, a partir do texto, caso os seus autores não os apresentem explicitamente, como por exemplo os dados nº10 (Domínio da aplicação) e nº18 (Tipo de Contribuição) da Tabela 5.5.

#	Dado	Valor	Objetivo	QP
1	ID	ID único por publicação, a partir da ordem em que os artigos foram recuperados das bibliotecas.	Controle e identificação.	
2	Título	O título da publicação. Copiado do texto.	Identificação individual.	MD1
3	Ano	O ano da publicação.	Ver a distribuição dos artigos selecionados ao longo dos anos.	MD2
4	Autores	Os autores da publicação.	Conhecer os nomes que mais publicam sobre deceptive patterns	MD3
5	Instituição	A instituição dos autores.	Saber quais instituições estão mais interessadas nesse assunto	MD4
6	Tipo de publicação	Evento ou revista?	Ver qual meio é o mais utilizado para publicar sobre deceptive patterns.	MD5
7	Veículo	Onde o artigo foi publicado, o nome do evento\revista.	Conhecer os veículos que estejam mais relacionados a esse tema.	MD6
8	Nome do deceptive pattern	Os nomes do(s) deceptive pattern(s) no artigo. Copiados do texto.	Para identificar os deceptive patterns da literatura.	QP1
9	Descrição do deceptive pattern	A descrição de cada deceptive pattern (se) dada pelos autores. Copiado do texto.	Para melhor entender os deceptive patterns identificados.	QP1
10	Domínio da aplicação	O domínio da aplicação da interface que usa o deceptive pattern. ex. web, entretenimento, propaganda, etc.	Para entender quais domínios são mais explorados por deceptive patterns.	QP2
11	Definição do deceptive pattern	A definição de deceptive pattern (se) dada pelos autores. Copiado do texto.	Para entender como pesquisadores veem os deceptive patterns, e comparar as diferenças e similaridades entre essas definições.	QP3
12	Método de catalogar	A descrição de como os autores catalogaram os deceptive patterns. Copiado do texto.	Para ver se já há uma forma de catalogar deceptive patterns.	QP4

#	Dado	Valor	Objetivo	QP
13	Fundamentos	Os nomes ou descrições gerais das teorias identificadas como bases do artigo. Copiado do texto.	Para ver se os autores estão fundamentando seu trabalho em alguma teoria.	QP5
14	Problema	A descrição do problema principal. Copiado do texto.	Para entender qual o problema relacionado a deceptive patterns no qual os autores estão trabalhando.	QP6
15	Contribuição	As principais contribuições do artigo, dadas pelos autores. Copiada do texto.	Para ver qual a principal contribuição dos autores nesse tema.	QP7
16	Tipo de contribuição	O tipo de contribuição. Ex. artefato, método, prática, ferramenta, etc.	Para identificar possíveis gaps de pesquisa.	QP7
17	Método de avaliação	O método usado para avaliar o trabalho. Copiado do texto.	Para identificar se e como os trabalhos estão sendo avaliados pelos pesquisadores.	QP8
18	Métricas de avaliação	As métricas usadas no processo de avaliação. Copiado do texto.	Para ver quais métricas são consideradas na avaliação.	QP8

Tabela 5.5: Tabela de extração de dados.

5.5 ESTRATÉGIA PARA ANÁLISE DOS DADOS -CODIFICAÇÃO ABERTA/DESCRITIVA

Após a etapa de extração, os dados dos artigos foram organizados de forma a responder cada uma das perguntas de pesquisa do mapeamento. Para responder a **QP1** (Quais deceptive patterns foram estudados/apresentados?), todos os deceptive patterns encontrados nos artigos selecionados foram listados com suas respectivas explicações. Os deceptive patterns foram então categorizados e agrupados conforme a semelhança entre si, e onde aplicável foram utilizadas as categorias de Gray et al. [6]. e Mathur et al.[7].

A fim de responder a **QP2** (Quais os domínios de aplicação os artigos focam que são relacionados a deceptive patterns?), os domínios de aplicação ligados aos deceptive patterns que apareceram em cada artigo foram identificados. Em seguida, os resultados foram categorizados e agrupados: temas próximos e sinônimos foram substituídos para ficarem equivalentes, por exemplo, “buying online” foi agrupado com “shopping websites”, e foi contabilizada a quantidade de vezes que cada domínio apareceu.

Para responder a **QP3** (Como esses deceptive patterns são definidos?), busquei nas definições extraídas os adjetivos e os verbos usados pelos autores para descrever os deceptive patterns, como por exemplo “enganador” (deceptive) ou “truque” (trick). Também categorizei as definições como sendo Únicas, de Gray et al. ou de Brignull.

A fim de responder às questões **QP4** (Como esses deceptive patterns estão sendo catalogados?), **QP5** (Quais são as fundamentações teóricas das publicações?), e **QP6** (Qual é o

problema de pesquisa estudado?), o conteúdo extraído dos artigos foi sumarizado e categorizado em seis diferentes tipos de problemas. Essa categorização foi criada a partir de uma codificação aberta realizada com os temas dos problemas discutidos nos artigos.

Para responder a **QP7** (Qual é a principal contribuição do artigo?) o processo foi similar a QP2, e para responder a **QP8** (Há alguma forma de avaliação ou experimento?), os artigos que apresentaram alguma forma de avaliação ou experimento foram categorizados entre três tipos: Experimentos com usuários, com designers, ou com estudantes. Usando essa categorização, os resultados encontrados foram sumarizados. Um pesquisador realizou o processo de análise dos dados extraídos descrito acima, e outro pesquisador irá revisar os resultados.

Os metadados foram agrupados e contabilizados: número de publicações sobre deceptive patterns ao longo dos anos, tipo dessas publicações (Evento ou journal), onde os artigos foram publicados (nome da revista, do evento), instituições que publicaram sobre deceptive patterns, e os países dessas instituições.

5.6 RESULTADOS DO MAPEAMENTO SISTEMÁTICO

Abaixo estão os resultados encontrados e obtidos durante a segunda parte da investigação analítica: Um mapeamento sistemático foi conduzido nas principais bases de computação (ACM, IEEE, Scopus) obtendo-se um panorama atual e rigoroso da literatura; E foi realizada uma análise dos aspectos sociotécnicos dos artigos encontrados no mapeamento.

Cumprindo o segundo objetivo específico estipulado, de mapear a literatura sobre deceptive patterns na computação, a seguir estão respondidas as questões de pesquisa estipuladas no protocolo do mapeamento:

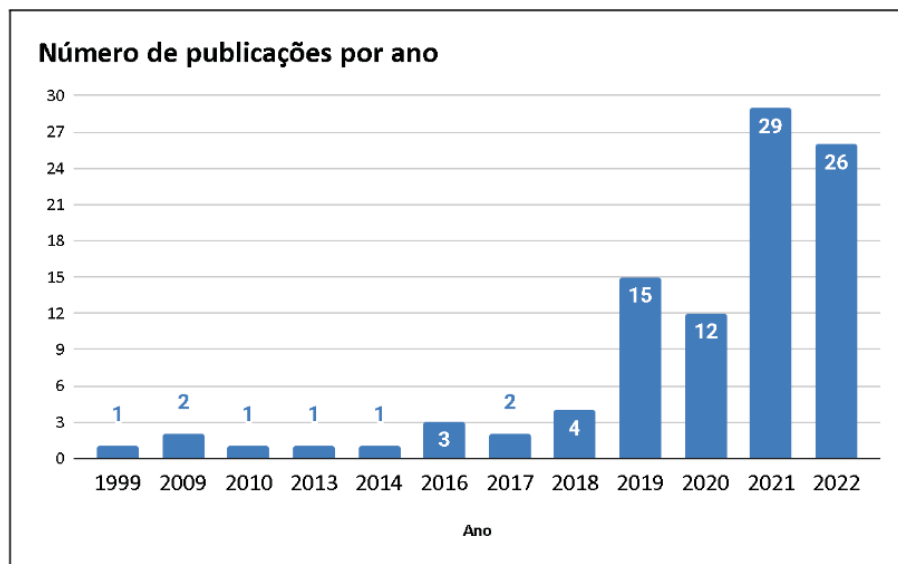


Figura 5.1: Distribuição de artigos através dos anos.

Uma lista contendo os nomes de todos os (97) artigos selecionados no mapeamento pode ser encontrada no Apêndice A. Essa lista está ordenada em ordem alfabética. A Figura 5.1 traz a distribuição de artigos por ano de publicação. Em 1999 foi publicado o trabalho de BJ Fogg sobre tecnologias persuasivas. Em 2010, o termo deceptive patterns foi criado por Harry Brignull. Em 2018, o termo deceptive pattern foi popularizado na academia após o trabalho de Gray et al. (Gray e et al., 2018) ter sido publicado, havendo um aumento na quantidade de pesquisas relacionadas ao tema. Os dados de 2022 vão até o mês de Julho.

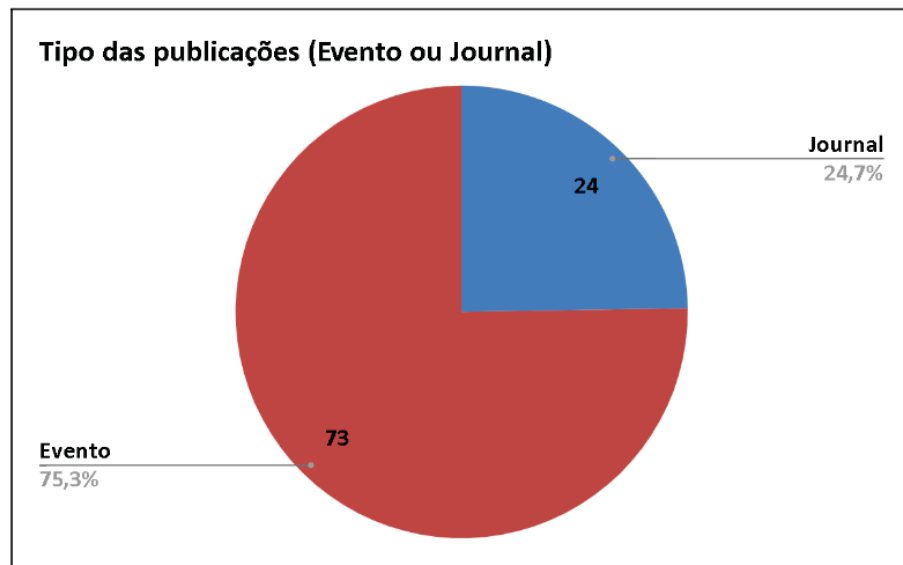


Figura 5.2: Tipos de publicação.

Categorias	Quantidade
Desorientação	25
Interferência na Interface	20
Escondendo	15
Pressão Social	15
Obstrução	14
Ação Forçada	12
Monetário	8
Sem Consentimento	7
Atraso	4
Capitalismo de Vigilância	3
Temporal	3

Tabela 5.6: Categorias identificadas de deceptive patterns e quantidade de tipos em cada uma.

A Figura 5.2 traz as quantidades dos dois principais tipos de publicação *Journals* e Eventos. Vinte e quatro artigos foram publicados em Journals, e o restante (73) foram publicados em Eventos. A Figura 5.3 traz os diferentes veículos de publicação em que artigos foram publicados. Ao todo, apareceram 46 veículos de publicação diferentes. A ACM CHI *Conference on Human Factors in Computing Systems*, conferência internacional, é o veículo que mais publica trabalhos sobre deceptive patterns e interfaces maliciosas: 34 trabalhos dos 97 selecionados, seguida do journal ACM *Human-Computer Interaction*, com 9 artigos publicados. No Apêndice B há uma tabela contendo todos os veículos de publicação que apareceram no mapeamento.

Questão de Pesquisa (QP) 1: Quais deceptive patterns foram estudados/apresentados? Ao todo foram encontrados 127 tipos (Apêndice C) de deceptive patterns divididos em 11 categorias (Tabela 5.6). As categorias foram criadas a partir de uma codificação exploratória emergente incremental, os diferentes tipos de padrões encontrados foram comparados em pares, um a um e, utilizando como base as categorias originais de Brignull, de Mathur et al. (Mathur et al., 2019) e Gray et al. (Gray et al., 2018), as categorias foram surgindo ou sendo suprimidas dentro de outras até que no fim restaram 11 categorias principais. Os tipos se dividem de forma irregular entre as categorias: a categoria Desorientação é a que mais tem diferentes tipos (25),

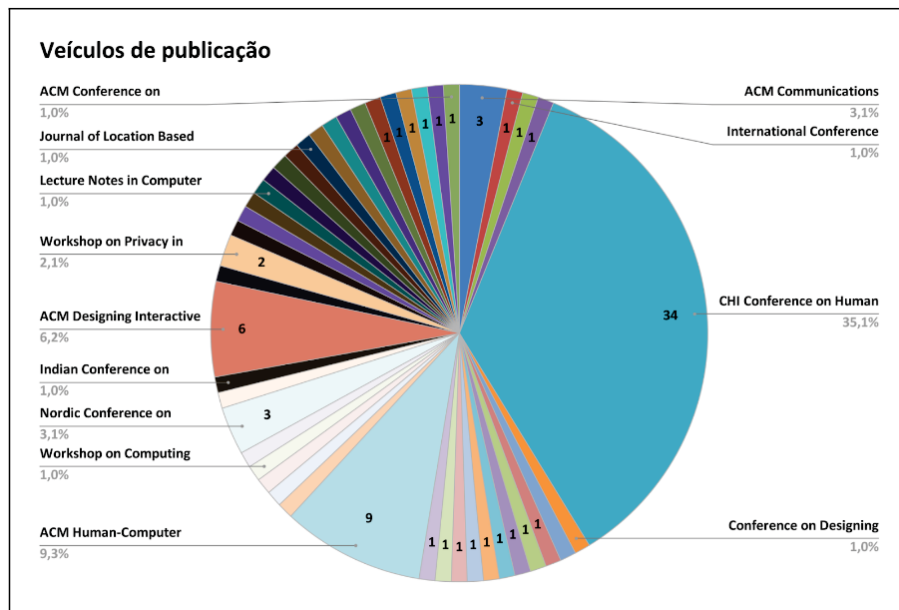


Figura 5.3: Veículos de publicação.

enquanto as categorias Temporal e Capitalismo de Vigilância tem apenas 3 tipos cada. E dos 127 tipos identificados, 26 deles apareceram em mais de um artigo ao mesmo tempo.

Dos 97 artigos analisados, em 34 deles os pesquisadores apresentaram alguma forma de “solução estabelecida para explorar e enganar usuários de forma genérica” (Bösch e et al., 2016) (a definição de deceptive pattern utilizada durante todo o mapeamento) ou categorias de tais soluções, que têm a intenção de manipular os usuários e seu comportamento. Ou seja, pouco mais de um terço dos artigos mapeados trazem novos tipos, e desses que trazem, Gray et al. foram os autores que mais trouxeram tipos inéditos (12), seguidos de Conti & Sobieski com 11 tipos inéditos, e de Mathur et al. com 10 tipos. Ao todo, 8 grupos de autores são responsáveis por mais da metade (70) dos tipos únicos identificados.

Todos os deceptive patterns mencionados nos artigos foram comparados uns com os outros e os repetidos e similares foram agrupados nos mesmos tipos. A lista de todos os deceptive patterns pode ser encontrada no catálogo online, ou no Apêndice C.

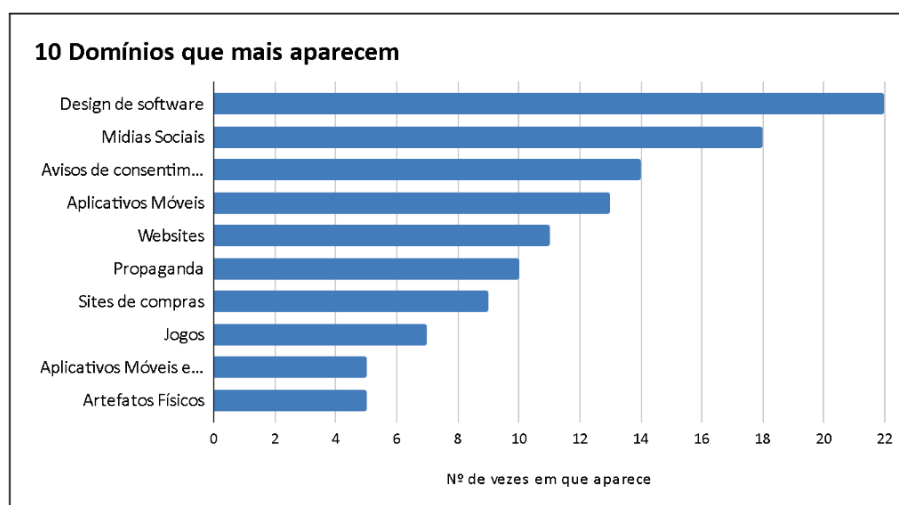


Figura 5.4: Tipos de domínio de aplicação que mais apareceram.

QP2: A quais domínios de aplicação esses deceptive patterns estão relacionados?

O domínio de aplicação que mais apareceu nos artigos foi “Design de software”, em 22 artigos, seguido de “Mídias Sociais” em 18 artigos, e em terceiro lugar “Avisos de cookies” em 14 artigos. Esses trabalhos estão focados principalmente no processo de design de software e suas interfaces e nas decisões dos designers sobre o processo de design. Ao todo, foram identificados 30 diferentes domínios e uma alta diversidade de domínios de aplicação nos quais os artigos focam, reforçando a ideia de que padrões enganosos podem aparecer em qualquer lugar onde haja uma interface de usuário. A Figura 5.4 traz os 10 domínios que mais apareceram.

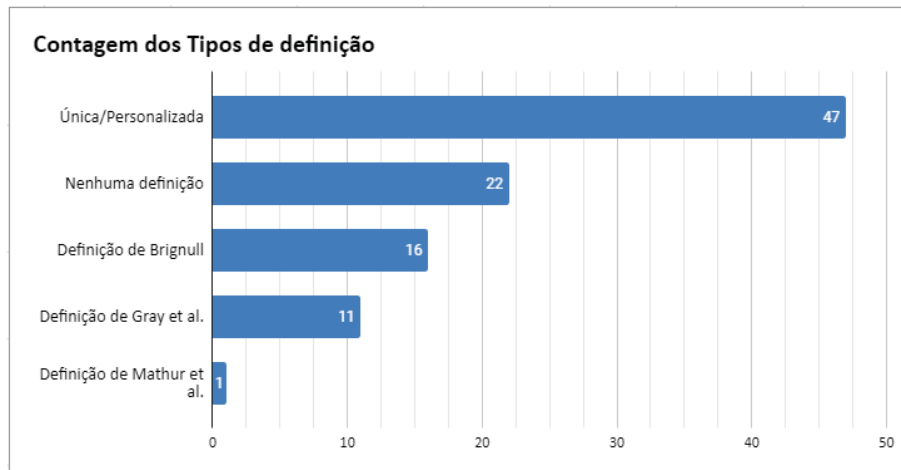


Figura 5.5: Contagem dos tipos de definições encontradas.

QP3: Como esses deceptive patterns são definidos? Quarenta e sete definições distintas/únicas foram encontradas nos artigos. A maioria dos artigos fala explicitamente da intencionalidade dos deceptive patterns já na definição (20). Além disso, muitos artigos definem os deceptive patterns como "Enganosos" (19), “Truques” (18), ou que “Atuam contra os interesses do usuário” (17). Também existem pelo menos outras vinte definições diferentes mas não exclusivas entre si. Em 22 artigos, os autores apenas mencionam ou falam sobre deceptive patterns sem trazer ou fazer menção a nenhuma definição. A Figura 5.5 traz uma contagem dos diferentes tipos de definições encontradas. De todos os 97 artigos mapeados quase metade deles (47) trazem definições únicas, e apenas 28 artigos fundamentam suas definições em autores estabelecidos no tema (Gray et al., Mathur et al., e Brignull). Os resultados indicam que falta uma base conceitual clara e consistente entre os pesquisadores, confirmando assim o trabalho de Mathur et al. (Mathur et al., 2021). Apenas 20 artigos se preocuparam em mencionar a intencionalidade dos padrões na definição, o que pode indicar uma falha na compreensão dos deceptive patterns por parte dos outros autores. A intencionalidade é parte fundamental dos deceptive patterns, e falhar em identificar ou mencionar isso em uma análise pode levar a erros de compreensão nos leitores.

QP4: Como esses deceptive patterns estão sendo catalogados? Apenas 23 artigos apresentaram algum tipo de catalogação ou explicação de como ocorreu o processo de coleta de deceptive patterns. No geral, poucos trabalhos (3) estão catalogando tipos de deceptive patterns, enquanto na maioria (18) dos trabalhos os deceptive patterns são coletados e analisados de maneira humana, para então serem categorizados pelos pesquisadores a partir de categorizações prontas, como por exemplo a de Brignull (Brignull et al., 2023) ou a de Gray et al. (Gray et al., 2018). Em dois dos trabalhos ((Mathur et al., 2019; Monge Roffarello e De Russis, 2022)), os autores utilizaram *web crawlers* para coletar os dados de forma automatizada na internet, mas ainda analisaram de forma humana posteriormente. Os três artigos (Conti e Sobiesk,

Bases teóricas	Trabalhos que utilizam	Qtd
Psicologia / Economia Comportamental / Neuromarketing [71,72,73,81,82,83,84]	A17,A32,A18,A43,A80,A62,A75,A26,A30,A34,A55,A64,A81,A27,A35,A85,A88,A15,A38,A40,A46,A47,A49,A50,A51,A52,A53,A56,A71,A92,A93,A3,A57,A61,A63,A67,A69,A72,A82,A86,A87,A94	42
Harry Brignull [4]	A32,A62,A7,A10,A76,A2,A13,A19,A25,A30,A34,A45,A55,A64,A79,A16,A21,A27,A35,A77,A85,A88,A91,A95,A96,A5,A8,A29,A49,A71,A74,A78,A90,A92,A93,A1,A44,A54,A68,A69,A82,A86	42
Tecnologia Persuasiva BJ Fogg [37]	A28,A27,A79,A64,A25,A10,A62,A37,A65,A77,A85,A91,A95,A96,A42,A48,A51,A78,A93,A61,A69	21
Questões legais [74,75,76] GDPR / CCPA [77]	A87,A83,A72,A69,A63,A54,A24,A22,A4,A93,A29,A12,A8,A5,A28,A21,A97,A81,A19,A6,A70,	21
Valores / ValueSensitiveDesign [78,79] Values at play [80]	A37,A7,A10,A76,A2,A14,A45,A55,A27,A91,A95,A31,A74,	13
Capitalismo de Vigilância [70]	A72,A73,A82,A81	4

Figura 5.6: Os diferentes tipos de referenciais usados nos artigos.

2010; Nyström e Stibe, 2020; Utz e et al., 2019) que trazem algum método de catalogação: em um artigo (Conti e Sobiesk, 2010) os pesquisadores catalogaram deceptive patterns com a ajuda de participantes em diferentes experimentos, em outro artigo (Nyström e Stibe, 2020) os pesquisadores apresentaram um novo framework chamado de Visibility-Darkness matrix, baseado no Intention-Outcome matrix. O último artigo (Utz e et al., 2019) traz uma ferramenta que extrai automaticamente informações do website, incluindo as informações dos avisos de cookies utilizados, facilitando uma análise automatizada.

QP5: Quais são as fundamentações teóricas das publicações? A Figura 5.6 traz os diferentes tipos de referenciais usados nos artigos. Analisando as fundamentações teóricas dos estudos é possível notar uma grande variedade de fontes das quais os autores se fundamentam. O trabalho original de Harry Brignull (Brignull et al., 2023) foi citado por 42 artigos, e o trabalho de B.J. Fogg (Fogg, 1999) sobre “tecnologias persuasivas” foi citado por 21 artigos. Quase metade dos artigos (42) trazem fundamentações da psicologia e áreas correlatas, como a ciência cognitiva, a economia comportamental e o neuromarketing. Por exemplo: a teoria do processo Dual de Kahneman (Kahneman, 2003), a teoria da auto-percepção (*Self-perception theory*) (Bem, 1967), ou o FoMO (*Fear of Missing Out*) (Przybylski e et al., 2013). Vinte e um trabalhos se fundamentam em artigos de bases legais ou relacionadas a GDPR (Regulamento Geral sobre a Proteção de Dados na Europa) (Union, 2022) ou a CCPA (Lei de Privacidade do Consumidor da Califórnia) (CCP, 2020). Dezesete trabalhos se fundamentam mais especificamente na economia. Por fim, 13 artigos se fundamentam em discussões sobre valores (dos usuários e dos designers) como por exemplo o Value Sensitive Design (VSD) (Friedman et al., 2008; Friedman e Hendry, 2019).

QP6: Quais são os problemas de pesquisa estudados? Foram identificados 7 categorias principais de problemas trabalhados nos artigos:

1. Ética: artigos que investigam as relações e impactos do uso de deceptive patterns com questões de natureza ética, como por exemplo como a ética é usada no dia a dia dos designers, ou como ela é discutida nas redes sociais, que há poucos trabalhos que descrevem o engajamento ético de designers, entre outros.
2. Consentimento dos usuários: pesquisas que abordam a forma com deceptive patterns são aplicados para induzir ou manipular o consentimento dos usuários a opções que beneficiam os interesses de outras partes que não os usuários.
3. Privacidade: problemas que descrevem os efeitos dos deceptive patterns na privacidade dos usuários. Por exemplo, a privacidade no contexto de rastreamento de localização, como auxiliar usuários a tomarem decisões sobre privacidade, entre outros.
4. Questões Comportamentais: foca em problemas relacionados à manipulação do comportamento dos usuários afetados por deceptive patterns. Por exemplo, como tecnologias persuasivas podem ser usadas para manipulação, como designers não possuem ferramentas para mensurar o quanto suas escolhas moldam comportamentos, e que pesquisadores ainda não forneceram as ferramentas necessárias para combater as influências dos deceptive patterns, entre outros.
5. Entendimento e mapeamento: problemas relacionados ao conceito, entendimento ou a catalogação de deceptive patterns. Por exemplo, fatores que influenciam os usuários a se tornarem vítimas dos deceptive patterns, quantos deceptive patterns aparecem em aplicativos móveis, e como o design fofo de robôs domésticos pode criar uma relação de poder ambivalente entre o usuário e o robô, entre outros.
6. Consequências: são trabalhos preocupados com as consequências de deceptive patterns específicos, e das decisões de design em geral, nos usuários e na sociedade. Por exemplo: faltam ferramentas para entender essas consequências do design, poucas pesquisas têm explorado os efeitos negativos das tecnologias persuasivas, e entre outros.
7. Capitalismo de Vigilância: trabalhos que focam nas características e problemas relacionados diretamente com o surveillance capitalism (Zuboff, 2019), um modelo de negócios que prevê e influencia o comportamento dos usuários a fim de maximizar o valor para propagandas.

A maioria dos artigos tratam de problemas em mais de uma categoria, a Figura 5.7 traz um diagrama de Venn com a quantidade de artigos em cada categoria e as interseções entre as categorias: 50 artigos tratam das Consequências do design, que são problemas relacionados aos resultados e impactos gerais das escolhas de design e dos deceptive patterns nos usuários ou na sociedade, em diferentes cenários de uso e interfaces; 39 artigos discutem problemas relacionados ao Entendimento e mapeamento de deceptive patterns, que são problemas relacionados à descrição e ao entendimento de deceptive patterns específicos e de diferentes categorias; 23 artigos tratam de Questões Comportamentais dos usuários, principalmente problemas relacionados à manipulação do comportamento dos usuários afetados por deceptive patterns; 17 artigos discutem problemas de Privacidade, que são problemas que descrevem os efeitos dos deceptive patterns na privacidade dos usuários; 14 artigos que tratam de questões relacionadas à Ética, são artigos que investigam as relações e impactos do uso de deceptive patterns com questões de natureza ética; 10 artigos trazem discussões sobre Consentimento, esses artigos abordam a forma com que deceptive patterns são aplicados para induzir ou manipular o consentimento dos usuários a opções que beneficiam os interesses de outras partes que não os usuários; e 4 artigos lidam com problemas

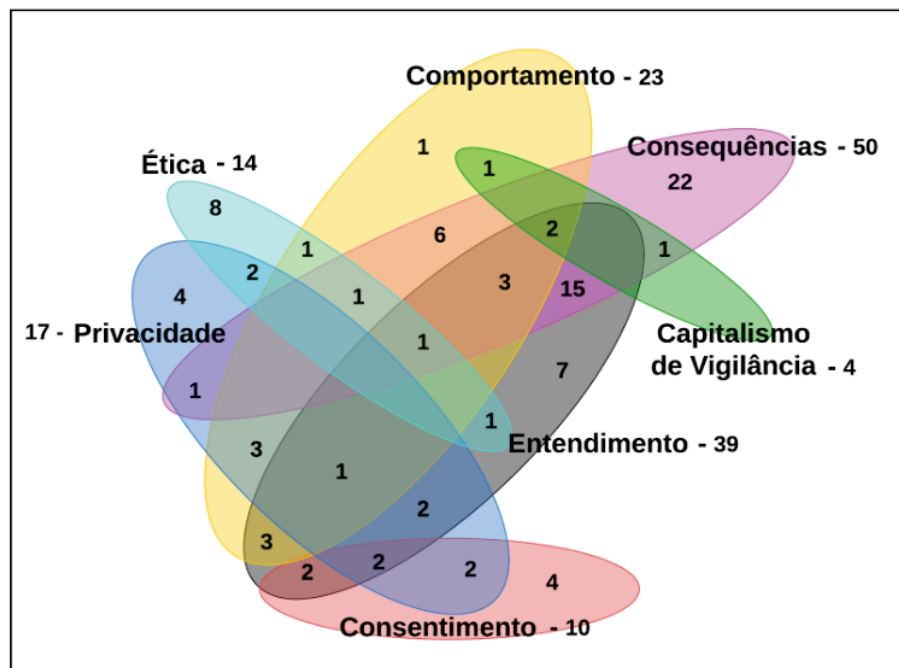


Figura 5.7: Diagrama de Venn representando as categorias de problemas.

ligados ao Capitalismo de Vigilância, que é um conceito em economia política que denota a ampla coleta e mercantilização de dados pessoais por corporações.

QP7: Qual é a principal contribuição dos artigos? Os autores dos artigos apresentaram diversos tipos de contribuições, e alguns artigos trazem mais de um tipo de contribuição: 36 artigos trazem diferentes tipos de experimentos principalmente com usuários mas também com estudantes e designers profissionais. Vinte e nove artigos também trazem diferentes tipos de interfaces maliciosas ou categorizações; há 12 artigos com discussões voltadas para a ética por exemplo: questões éticas em volta da computação persuasiva responsabilidades éticas dos profissionais, e discussões de usuários sobre questões éticas em torno de interfaces maliciosas; 16 artigos trazem discussões sobre banners de cookies, avisos de consentimento e questões legais envolvidas (GDPR, CCPA). Alguns exemplos são: como o design desses avisos impactam no comportamento e consentimento dos usuários; como e se os sites e aplicativos têm seguido as recentes leis sobre consentimento do usuário (CCPA, GDPR). Também há exemplos de como os deceptive patterns violam direitos legais dos usuários e como a manipulação pode ser usada tanto para o bem como para o mal. Também há discussões sobre o “capitalismo de vigilância” e uma análise das origens dos deceptive patterns, entre outros.

QP8: Há alguma forma de avaliação ou experimento? Trinta e sete (37) artigos trouxeram algum tipo de avaliação ou estudo (Figura 5.8) e, no geral, os experimentos têm sido bem definidos e documentados. A Tabela de Experimentos no Apêndice E traz um resumo dos experimentos e estudos encontrados nos artigos. Os artigos consistem em observações e questionários sobre o comportamento de usuários diante de situações diversas envolvendo interfaces maliciosas e deceptive patterns (como por exemplo navegando na web e interagindo com avisos de cookies, jogos no celular, ou utilizando redes sociais). Com objetivos diversos mas com propósitos parecidos: entender os efeitos de padrões de design maliciosos (reais ou criados pelos pesquisadores), em diferentes tipos de interfaces (banners de cookies, websites, redes sociais), no comportamento, sentimentos, e consentimento dos usuários. Já os estudos com estudantes e profissionais focaram mais na atuação do profissional designer: nos valores éticos e intenções do profissional durante o processo de criação e desenvolvimento de interfaces

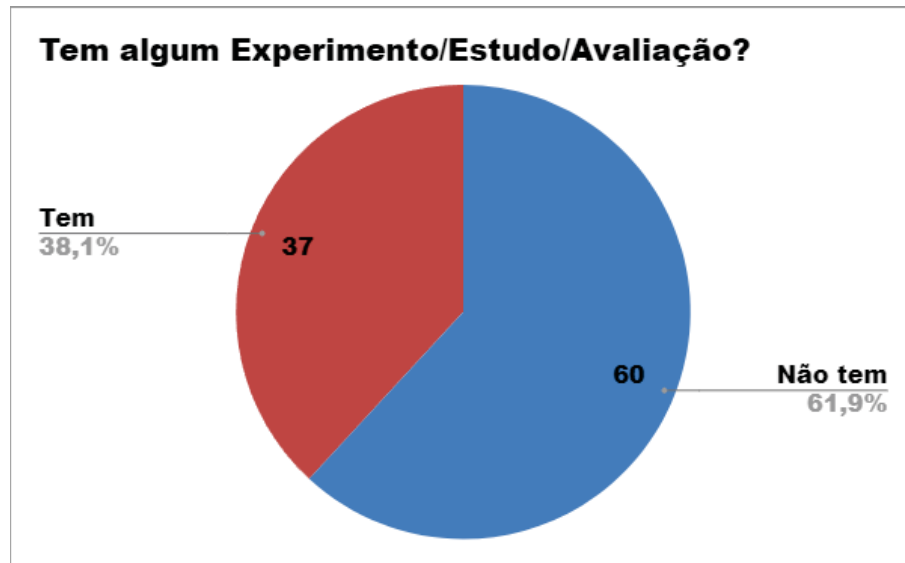


Figura 5.8: Quantidade de trabalhos que apresentaram algum estudo/avaliação/experimento.

para websites ou avisos de consentimento. Há também dois estudos (Chaudhry e Kulkarni, 2021; Tahaei e Vania, 2021) que focam em avaliações: uma avaliação de diretrizes, direcionadas a profissionais, para o design de aplicativos que favorecem bons comportamentos dos usuários; e uma avaliação de manuais (direcionados para profissionais) de uso e implementação de redes de propagandas em websites e serviços, como por exemplo o GoogleAds.

5.7 ASPECTOS SOCIOTÉCNICOS DA LITERATURA EM DECEPTIVE PATTERNS

Cumprindo o terceiro objetivo específico, de analisar os aspectos sociotécnicos considerados e negligenciados na literatura, foi utilizado o Framework Semiótico para se observar os artigos no geral a partir de uma visão sistêmica nas seis camadas distintas.

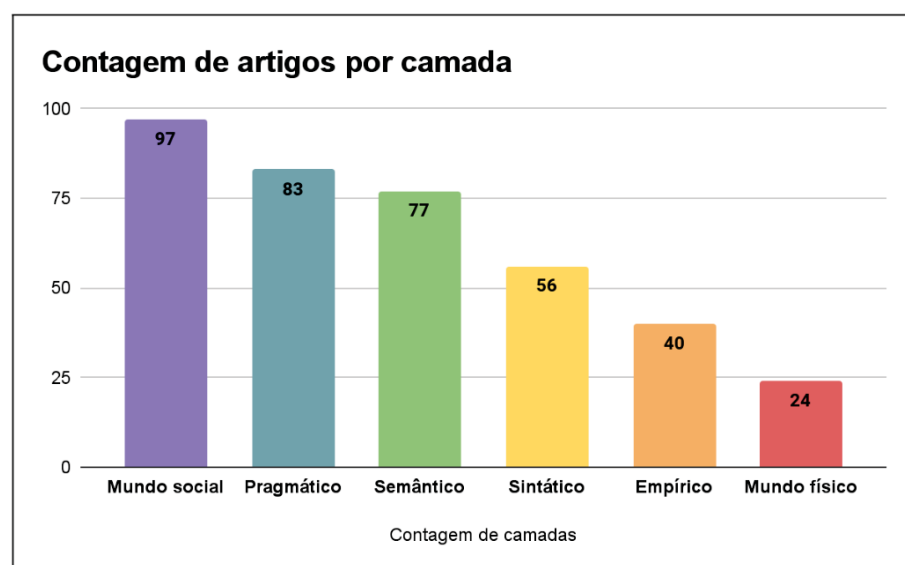


Figura 5.9: Quantidade de artigos que se enquadram em cada camada.

Os artigos foram analisados e categorizados de acordo com as camadas do framework, e a Figura 5.9 traz uma contagem de artigos que se enquadram em cada uma das camadas do

Framework Semiótico, há diversos artigos que se encaixam em mais de uma camada. A Tabela 5.7 traz todos os artigos classificados dentro das camadas do Framework Semiótico. Olhando para esses resultados pelo Framework Semiótico é possível perceber que os artigos focam mais nas camadas das funções humanas(mundo social, pragmático, e semântico): nos impactos sociais, nos usuários e suas experiências, expectativas e intenções, significados e entendimentos, e em questões relacionadas com a ética do desenvolvedor que atua com essas interfaces, valores humanos envolvidos na criação dessas interfaces, leis de diferentes países, comportamentos dos usuários e como são manipulados, entre outros.

Apesar de haver diversos trabalhos, há um foco menor dos artigos nas camadas da plataforma técnica(sintático, empírico e mundo físico): artigos que apresentam em suas discussões as características visuais, estruturais e estatísticas das técnicas utilizadas pelas interfaces maliciosas, como também discutem os impactos no mundo físico dos usuários como custos materiais e temporais por exemplo, assim como a exploração do meio físico para impactar nos usuários.

Na **camada do Mundo Social**, todos os artigos selecionados mencionam ou discutem sobre algum tipo de impacto ou consequência de interfaces maliciosas na sociedade e nos usuários, como por exemplo: prejudicando a privacidade, a segurança, o bem estar, manipulando comportamentos e emoções, afetando também diretamente o consentimento. Muitos dos artigos citam ou mencionam o Design Sensível a Valores (*Value Sensitive Design* (Friedman et al., 2008; Friedman e Hendry, 2019)) como uma das formas mais utilizadas pela literatura para lidar com essas questões negativas no design que envolvem principalmente valores humanos. Também há trabalhos que apresentam os pontos de vista dos usuários, suas experiências, interações, e sentimentos sobre deceptive patterns.

E há artigos que estudam como os padrões enganosos se relacionam com - e inevitavelmente infringem - leis como a GDPR(Union, 2022) europeia, a CCPA(CCP, 2020) do estado da Califórnia nos Estados Unidos, e a LGPD (Lei Geral de Proteção de Dados)(LGP, 2018) brasileira. Nessas leis há, entre outras coisas, uma definição clara do que deve ser considerado consentimento livre e esclarecido, como e até onde os dados dos usuários podem ser captados e manipulados, o que pode ser feito com esses dados, e quais mecanismos devem estar a disposição do usuário para controle do que é feito com esses dados incluindo sua exclusão. São principalmente artigos que lidam com avisos de cookies, que ao utilizarem deceptive patterns a fim de aumentar as taxas de consentimento, violam essas leis. Essas leis, apesar de diferentes, apresentam um teor comum: Interfaces devem prover uma maneira fácil de deletar todos os dados pessoais que a empresa ou site tenham captado do usuário, uma maneira de negar o consentimento, e informações suficientes para que o usuário possa fazer uma escolha informada. Na camada do Mundo Social há diversos estudos que já são capazes de suprir a literatura com uma vasta visão dos impactos sociais, legais, emocionais e comportamentais dos deceptive patterns.

Na **camada Pragmática** é possível perceber que em muitos dos artigos os autores apresentam de que forma as intenções dos usuários entram em choque com as intenções das interfaces maliciosas: os artigos, apoiados na psicologia, na economia comportamental, ou no neuromarketing, explicam a maneira com que os deceptive patterns exploram intencionalmente os usuários: usando vieses cognitivos [A30] que afetam o subconsciente dos usuários, usando os conhecidos testes A/B [A35,A81] que selecionam interfaces baseadas apenas em seu retorno estatístico.

No artigo [A35] os autores traçam três pontos chave para o surgimento dos deceptive patterns: práticas enganosas intencionais utilizadas no varejo há muitos anos, pesquisas dentro de IHC sobre nudges (manipulação light visando facilitar o uso de uma interface), e *growth hacking* (práticas usadas dentro de empresas para acelerar o crescimento do negócio). Há dois artigos

apenas [A69, A14] que buscam explicitar a intenção do profissional designer de interfaces, por meio de experimentos simulando o processo de criação de uma interface manipulativa.

Dentro da **camada Semântica** é possível entender que muitos dos artigos trazem análises de deceptive patterns e experimentos com usuários, mostrando os reais significados das interfaces, que são os de enganar e manipular o usuário, enquanto muitas vezes o usuário acredita estar lidando com uma interface honesta e equilibrada. A maioria dos artigos que apresentam elementos da camada Sintática, também trazem contribuições na camada Semântica. Em [A40], os autores avaliaram guias de uso e implementação, para desenvolvedores, de plataformas de anúncios online, como o *Google Ads* por exemplo. Na avaliação, os autores identificaram que quando o assunto são informações de privacidade dos usuários, essas empresas colocam os desenvolvedores como a entidade responsável, indo contra a interpretação dos próprios desenvolvedores, e de muitos pesquisadores, de que as empresas por trás dessas plataformas de anúncios é que tem a responsabilidade de zelar pela privacidade do usuário. Isso sugere uma tentativa das empresas de se livrarem da responsabilidade pela privacidade dos usuários.

Na **camada Sintática** há muitos dos artigos que trazem contribuições na camada Semântica também. Há onze artigos que mostram, com ajuda de experimentos com usuários, de que maneira as estruturas formais das interfaces maliciosas são capazes de manipular o comportamento dos usuários, e de qual forma os diferentes tipos de interfaces são capazes de manipular mais que outros tipos. Na maioria desses artigos foram avaliados diferentes tipos de avisos de consentimento, com diferentes opções de escolha, em diferentes posições da tela, usando cores e formatos diferentes, mostrando que algumas interfaces têm mais poder de aumentar as taxas de consentimento em detrimento das escolhas e intenções dos usuários. Em dois artigos, os autores avaliam especificamente a linguagem utilizada em textos de contratos *online*, o grau de formalidade utilizado e a granularidade das informações, e mostraram como esses parâmetros são utilizados para conseguir mais consentimento dos usuários. Em [A68], os autores trazem resultados que demonstram que a linguagem utilizada em questões que afetam a privacidade do usuário, como aceitar ou rejeitar cookies, pode afetar significativamente as decisões do usuário. Um artigo [A49] trata de mecanismos utilizados pelo Youtube que atrapalham o senso de controle dos usuários diante da plataforma utilizada. Há também artigos que trazem análises de interfaces e padrões maliciosos encontrados em websites, aplicativos [A51,A8,A88], ou games [A67,A25], identificando essas estruturas formais de manipulação.

Dentro da **camada Empírica** há poucos artigos que falam sobre as propriedades estatísticas e capacidades da plataforma/canal que deceptive patterns exploram, como por exemplo: termos e contratos longos e de difícil leitura, diferentes plataformas com capacidades diferentes (Facebook, Spotify, Wish), e cookies de banners com palavras demais (ou de menos). Em [A55], os autores apresentaram recursos que incentivam a compra por impulso nos usuários. Em [A57], os autores trazem uma discussão sobre como, num futuro não tão distante, os seres humanos e as máquinas estarão tão integrados entre si que os usuários correrão riscos, como a simbiose parasitária, em que uma máquina se alimenta das emoções dos usuários, podendo raptar até mesmo o funcionamento do próprio corpo do usuário.

Na **camada do Mundo Físico**, em menor número, os artigos encontrados lidam com as consequências e impactos no mundo material e econômico dos usuários. Alguns artigos apresentam e discutem especificamente sobre o Capitalismo de Vigilância, e como esse novo modelo econômico, baseado na observação e extração de dados de usuários, tem naturalizado práticas antiéticas e maliciosas de vigilância massiva e manipulação dos usuários.

5.8 GAPS DE PESQUISA E OPORTUNIDADES

A literatura mapeada tem focado bastante nos aspectos sociais dos deceptive patterns, impactos e experiências negativas(mundo social), nas intenções dos usuários (pragmático) e nos significados das estruturas e interfaces (semântico) maliciosas utilizadas para enganar os usuários. Porém, são discussões e análises focadas e limitadas a partes específicas do tema, como por exemplo: apenas listar e categorizar tipos de deceptive patterns, ou apresentar opiniões de usuários dessas interfaces, ou discutir temas ligados à sociedade como ética e valores desses deceptive patterns. Outros aspectos dos deceptive patterns que tem sido menos explorados, como por exemplo: quem criou/financiou a criação desses padrões, como as empresas se aproveitam das capacidades do meio de transmissão para atrapalhar e manipular, e como esses padrões são capazes de se aproveitar até mesmo do meio físico do usuário. Na camada Pragmática seria interessante ver mais estudos sobre a intenção dos desenvolvedores, na prática, e de onde vêm a intenção de manipular usuários, se são necessariamente “ordens superiores” o que os desenvolvedores podem fazer para combater essa cultura que cresce cada vez mais no capitalismo de vigilância.

Portanto existe uma possibilidade para que se estude mais as características técnicas dos deceptive patterns como por exemplo: como são estruturadas essas interfaces, quais dados estão sendo captados dos usuários, qual a linguagem utilizado e qual o grau de *affordance* dessas interfaces (sintático). Também é possível estudar como os deceptive patterns exploram as propriedades estatísticas do meio, a capacidade de transmissão, a velocidade de atualização da tela, a quantidade de opções, as propagandas que atrapalham as atividades que o usuário quer realizar (empírico), e também como o mundo real é utilizado em desfavor do usuário. E também é possível ir mais a fundo nas situações em que a interface maliciosa explora as capacidades físicas do hardware, processamento, capacidade de armazenamento, quando é necessário completar uma ação no mundo real para se resolver algo que poderia ser resolvido pelo próprio usuário, como ligar para terceiros, ou ter que enviar uma carta, ou ir fisicamente até uma loja/assistência.

Soluções automatizadas para detecção de deceptive patterns e outras interfaces maliciosas ainda estão apenas em fases de concepção. Apenas um trabalho [A52] trouxe uma tentativa de automatização da detecção de deceptive patterns, e outro trabalho [A95]. Portanto há espaço para ser explorado nessa área, com um possível uso de Inteligência Artificial e outras técnicas que possam ser capazes de identificar autonomamente as características e detalhes e, possa assim, identificar interfaces maliciosas sem a necessidade de um ser humano.

Camadas	Artigos
Mundo social	A11, A16, A17, A18, A22, A23, A30, A36, A38, A39, A44, A48, A49, A51, A57, A59, A60, A63, A66, A67, A77, A78, A79, A82, A87, A89, A90, A96, A97 Privacidade: A4, A12, A13, A19, A20, A26, A27, A28, A29, A32, A41, A54, A62, A64, A68, A69, A80, A91 Segurança: A61, A62, A69; Bem-estar: A3, A46, A53, A55; Emoções: A29, A35, A42, A47, A50, A52, A53, A65, A72, A73, A75, A81, A86; Consentimento: A1, A4, A6, A15, A21, A24, A28, A29, A68, A69, A70, A83; Design Sensível a Valores: A2, A7, A10, A14, A27, A31, A37, A45, A55, A74, A76, A91, A95; Ponto de vista dos usuários: A3, A9, A25, A27, A31, A40, A42, A43, A46, A47, A50, A56, A58, A71, A85, A88, A92, A94; Leis de Dados: A1, A4, A5, A6, A8, A12, A19, A20, A21, A24, A28, A29, A33, A68, A69, A70, A81, A83, A84, A93;
Pragmático	A1, A10, A12, A13, A14, A15, A16, A17, A18, A19, A24, A25, A26, A27, A28, A29, A3, A30, A31, A32, A33, A35, A36, A37, A38, A4, A40, A41, A42, A43, A44, A45, A46, A47, A48, A49, A5, A50, A51, A52, A53, A54, A56, A58, A59, A6, A61, A62, A63, A64, A65, A66, A67, A68, A69, A70, A71, A72, A74, A75, A76, A77, A78, A8, A80, A81, A82, A83, A85, A86, A87, A88, A89, A9, A90, A91, A92, A93, A94, A95, A96 Vieses Cognitivos: A30 Testes A/B: A35, A81 Intenção do Profissional/Designer: A14, A69
Semântico	A1, A10, A12, A14, A15, A16, A17, A18, A21, A24, A26, A28, A29, A3, A30, A31, A33, A34, A35, A36, A37, A38, A39, A4, A40, A41, A42, A44, A46, A47, A49, A5, A50, A51, A52, A53, A54, A55, A56, A58, A59, A6, A61, A62, A63, A64, A65, A67, A68, A69, A70, A72, A74, A75, A76, A77, A78, A8, A80, A81, A82, A83, A84, A85, A86, A88, A9, A90, A91, A92, A93, A94, A95, A96, A97
Sintático	A1, A12, A16, A17, A18, A19, A2, A20, A21, A24, A26, A29, A3, A30, A33, A34, A35, A36, A38, A39, A41, A44, A51, A52, A53, A54, A55, A56, A57, A60, A64, A67, A73, A74, A76, A77, A78, A8, A81, A82, A90, A91, A93, A95, A97 Experimentos com usuários: A80, A6, A28, A5, A15, A49, A84, A4, A63, A68, A86 Linguagem em contratos online: A63, A68
Empírico	A1, A12, A17, A18, A19, A20, A21, A26, A28, A29, A3, A30, A32, A33, A36, A38, A41, A5, A52, A53, A54, A55, A56, A57, A6, A60, A73, A76, A79, A81, A86, A90, A93, A95, Termos de Serviço de difícil leitura: A97, A63 Capacidades de Plataformas: A8 Quantidade de palavras em banners de Cookies: A4, A84, A15
Mundo físico	A1, A16, A17, A18, A22, A23, A26, A29, A30, A32, A35, A36, A53, A56, A57, A76, A89, A90, A93, A95 Capitalismo de Vigilância: A72, A73, A81, A82

Tabela 5.7: Artigos separados por camadas do framework.

6 O CATÁLOGO DE DECEPTIVE PATTERNS

Cumprindo o quarto objetivo específico (4 - Elaborar um catálogo dos deceptive patterns mapeados;), um catálogo foi construído contendo todos os deceptive patterns encontrados no mapeamento sistemático. A lista completa de deceptive patterns pode ser vista no Apêndice. Este catálogo está disponível online, todo em português, na url¹.

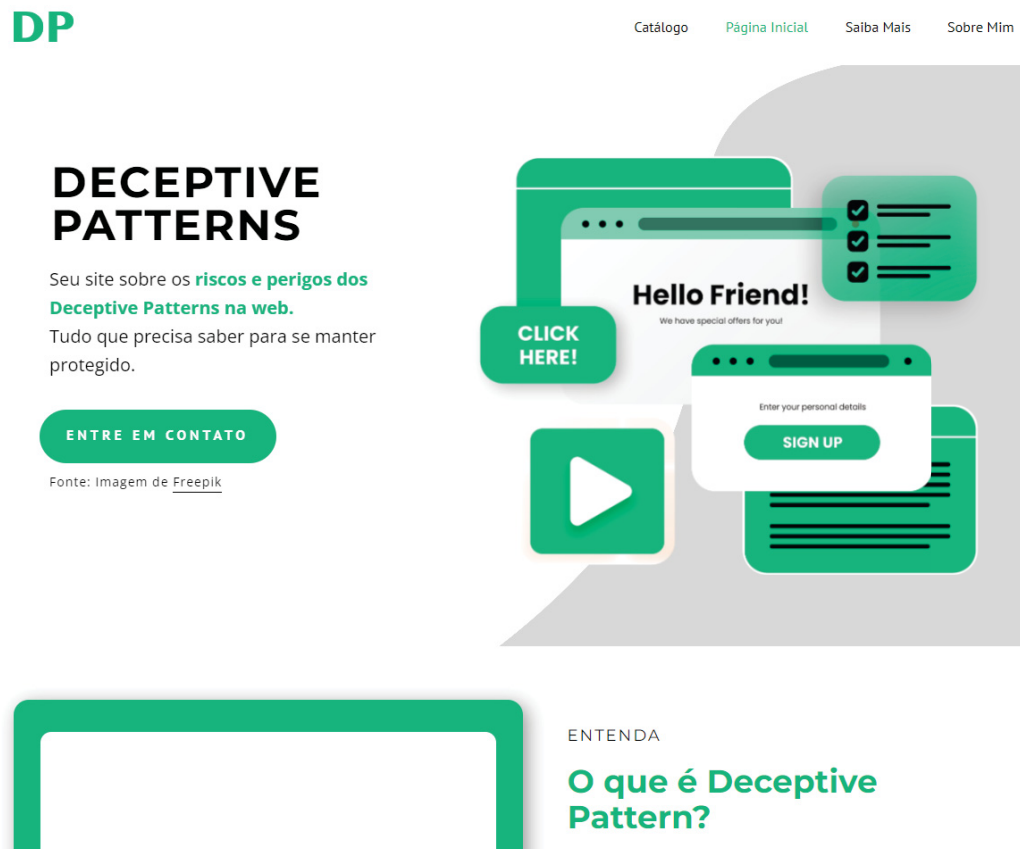


Figura 6.1: Tela inicial do website.

O catálogo é uma contribuição técnica cujo principal objetivo é apresentar de forma ordenada e organizada informações sobre os deceptive patterns já conhecidos na literatura, servindo assim de apoio para práticas de design e educação sobre esse fenômeno sociotécnico pouco conhecido pelo público fora das universidades.

Ao organizar e explicar de forma simplificada o funcionamento e os efeitos dos deceptive patterns, é possível apoiar os usuários no aprendizado sobre essa prática antiética se tornam mais preparados para evitar e se proteger dessa. E, também, torna mais fácil para profissionais que queiram aprender mais sobre o assunto e que estejam buscando formas de evitar esse tipo de design. O catálogo também foi avaliado por um grupo de pesquisadores em IHC quanto a sua Facilidade de Uso e sua Utilidade Percebida.

As 11 categorias apresentadas no catálogo foram criadas a partir de uma análise inspirada na Análise Temática Braun e Clarke (2012). Comparando os diferentes tipos encontrados entre si, e utilizando como base as categorias originais de Brignull, e as categorias de Mathur et

¹<https://deceptivepattern.nicepage.io/>

al.(Mathur e et al., 2019) e Gray et al.(Gray e et al., 2018), eu pude construir as 11 categorias diferentes



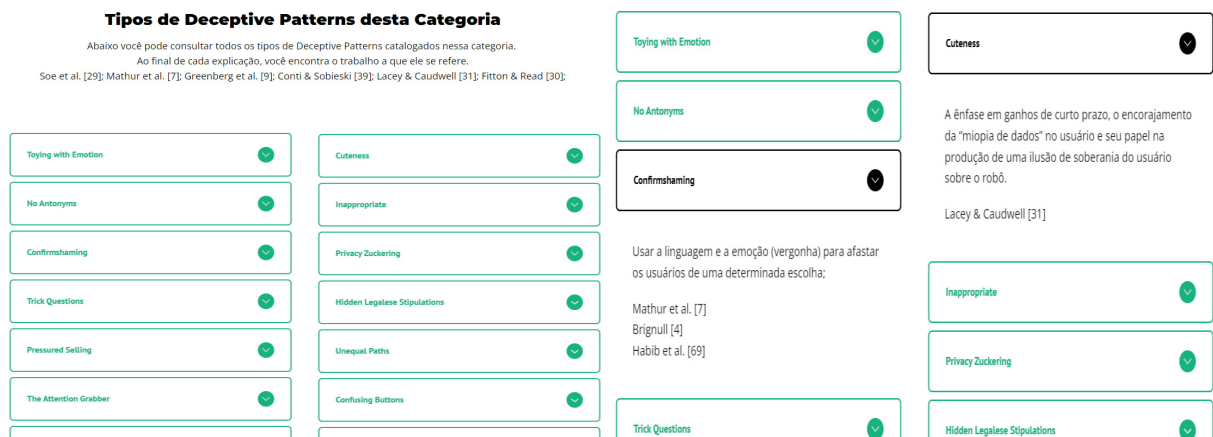
(a) Página do catálogo com algumas das categorias visíveis.

(b) Tela da categoria Desorientação.

Figura 6.2: Catálogo e categoria Desorientação.

6.1 PÁGINA INICIAL DO CATÁLOGO

Descrevendo a primeira parte da página principal (Figura 6.1) : no alto à direita está o menu com quatro opções: Catálogo (que leva ao catálogo de deceptive patterns), Página Inicial (que retorna a página inicial do site), Saiba Mais (que leva a uma página com mais informações sobre deceptive patterns e seu funcionamento), e Sobre Mim (que leva a mais informações sobre o autor do trabalho em questão). Logo abaixo do menu, à direita está uma imagem grande que já representa um deceptive pattern, e à esquerda está o título deceptive patterns e uma frase de abertura (Seu site sobre os riscos e perigos dos deceptive Patterns na web. Tudo que precisa saber para se manter protegido.). Abaixo da frase de abertura um botão escrito Entre em Contato.



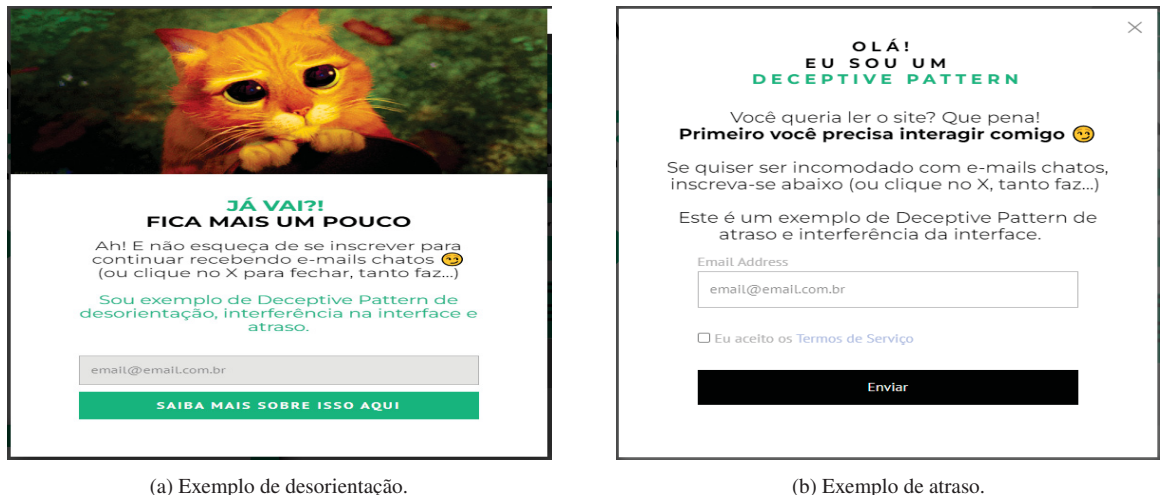
(a) Diferentes tipos de deceptive patterns da categoria Desorientação.

(b) Tipos Cuteness e Confirmshaming.

Figura 6.3: Tela da categoria Desorientação.

6.2 PÁGINA DO CATÁLOGO

Descrevendo a página do catálogo (a Figura 6.2(a) é uma captura do catálogo mostrando as diferentes categorias): no alto da página, abaixo do menu, está o título, escrito grande Catálogo e abaixo uma frase de abertura (“Navegue pelas categorias abaixo e descubra os tipos existentes de deceptive Patterns.”). Abaixo do título estão as onze categorias de deceptive patterns, separadas em caixinhas onde cada uma tem um botão que leva para uma página da categoria indicada.



(a) Exemplo de desorientação.

(b) Exemplo de atraso.

Figura 6.4: Exemplos práticos de deceptive patterns implementados no website do catálogo.

Quando o usuário clica em uma das categorias, ele é levado a uma tela que contém no título o nome da categoria, abaixo uma explicação dessa categoria, um exemplo prático dessa categoria e, mais abaixo, em duas colunas estão todos os diferentes tipos de deceptive patterns encontrados na literatura que se encaixam na categoria. A Figura 6.2(b) traz uma captura da tela da categoria Desorientação, mostrando um exemplo e uma breve explicação, e a Figura 6.3(a) traz os diferentes tipos dentro da categoria Desorientação, apresentados em duas colunas.

Quando o usuário clica em um tipo, uma explicação aparece para o usuário. A Figura 6.3(b) mostra a explicação dos tipos Confirmshamming e Cuteness (Fofura): Forced Enrolment: Coagir os usuários a criar contas ou compartilhar suas informações para concluir suas tarefas. Confirmshamming: Usar a linguagem e a emoção (vergonha) para afastar os usuários de uma determinada escolha; E Cuteness: A ênfase em ganhos de curto prazo, o encorajamento da “miopia de dados” no usuário e seu papel na produção de uma ilusão de soberania do usuário sobre robôs domésticos.

Exemplos práticos imitando deceptive patterns reais também foram implementados no website, a fim de criar uma experiência prática sobre deceptive pattern que seja educativa para aqueles que estiverem navegando. Na tela inicial, alguns segundos após abrir o site, e quando o usuário move o mouse para fora do site, um pop-up aparece bloqueando a tela e pedindo por um email do usuário (Figura 6.4).

6.3 ESTUDO PARA ENTENDIMENTO DA ACEITAÇÃO DO CATÁLOGO

Um estudo exploratório foi realizado visando observar a aceitação do catálogo de deceptive patterns. Esse estudo foi com pesquisadores de IHC, devido a sua . Para tanto, foi utilizado um questionário baseado no Modelo de Aceitação de Tecnologia - Technology Acceptance Model (TAM) [94,95], utilizando uma escala Likert de 5 pontos (1-Discordo

Objetivo	Avaliar preliminarmente o catálogo online de deceptive patterns por meio de uma análise da facilidade de uso e da utilidade percebida com profissionais de IHC;
Público alvo do estudo	Pesquisadores da computação, e profissionais do design e desenvolvimento de interfaces;
Duração total	1 hora e 5 minutos (45 minutos de atividade com questionário e 20 minutos de grupo focal);
Local	Laboratório 3 do Departamento de Informática da Universidade Federal do Paraná, Curitiba-PR;
Data	29 de setembro de 2022;
Participantes	Sete (7) profissionais com experiência em IHC;

Tabela 6.1: Resumo do estudo realizado com o catálogo.

Totalmente; 2-Discordo Parcialmente; 3-Indiferente; 4-Concordo Parcialmente; 5-Concordo Totalmente;) para avaliar a facilidade de uso e a utilidade percebida pelos participantes. O questionário contém 3 partes: as questões de caracterização dos participantes, as questões sobre a facilidade de uso, e as questões sobre a utilidade percebida. A Tabela 6.1 traz mais detalhes sobre o estudo.

6.3.1 Resultados do Estudo

Pelo questionário de caracterização é possível ver que os participantes do estudo representam parte do público alvo desejado para o catálogo de deceptive patterns: todos os participantes (7) afirmaram utilizar a internet todos os dias, portanto estão sob o risco de encontrar deceptive patterns e sofrer deles. E todos os participantes são formados em Ciência da Computação e atuam como pesquisadores em IHC. A Figura 6.5 traz um resumo da caracterização dos participantes do estudo.

As perguntas 4 e 5 do questionário de caracterização focaram no conhecimento dos participantes sobre deceptive patterns, antes e depois de usarem o catálogo. E seis dos sete participantes indicaram saber mais sobre deceptive patterns após o uso do catálogo.

6.3.2 Facilidade de Uso e Utilidade Percebida

Após o questionário de caracterização, os usuários responderam os questionários de Facilidade de Uso e de Utilidade Percebida do catálogo utilizando uma escala Likert de 5 pontos: 1-Discordo Totalmente; 2-Discordo Parcialmente; 3-Indiferente; 4-Concordo Parcialmente; 5-Concordo Totalmente;. As Imagens 6.6, 6.7, 6.9, 6.8 trazem as perguntas e respostas dos participantes.

Quanto à Facilidade de Uso (Figuras 6.6 e 6.7) o resultado do estudo mostra que o catálogo é fácil de ser utilizado e de aprender a ser usado. Seis dos participantes do estudo concordaram com as afirmações de que “é fácil aprender a navegar pelo catálogo” e de que “a interação com o catálogo foi clara e compreensível”. Todos os participantes concordaram que aprender sobre deceptive pattern utilizando o catálogo foi fácil. Três dos participantes deixaram comentários reafirmando essa facilidade:

- Participante 2 - “O catálogo está ótimo, bem fácil de usar.”;
- Participante 6 - “... fácil de interagir pelo design minimalista.”;

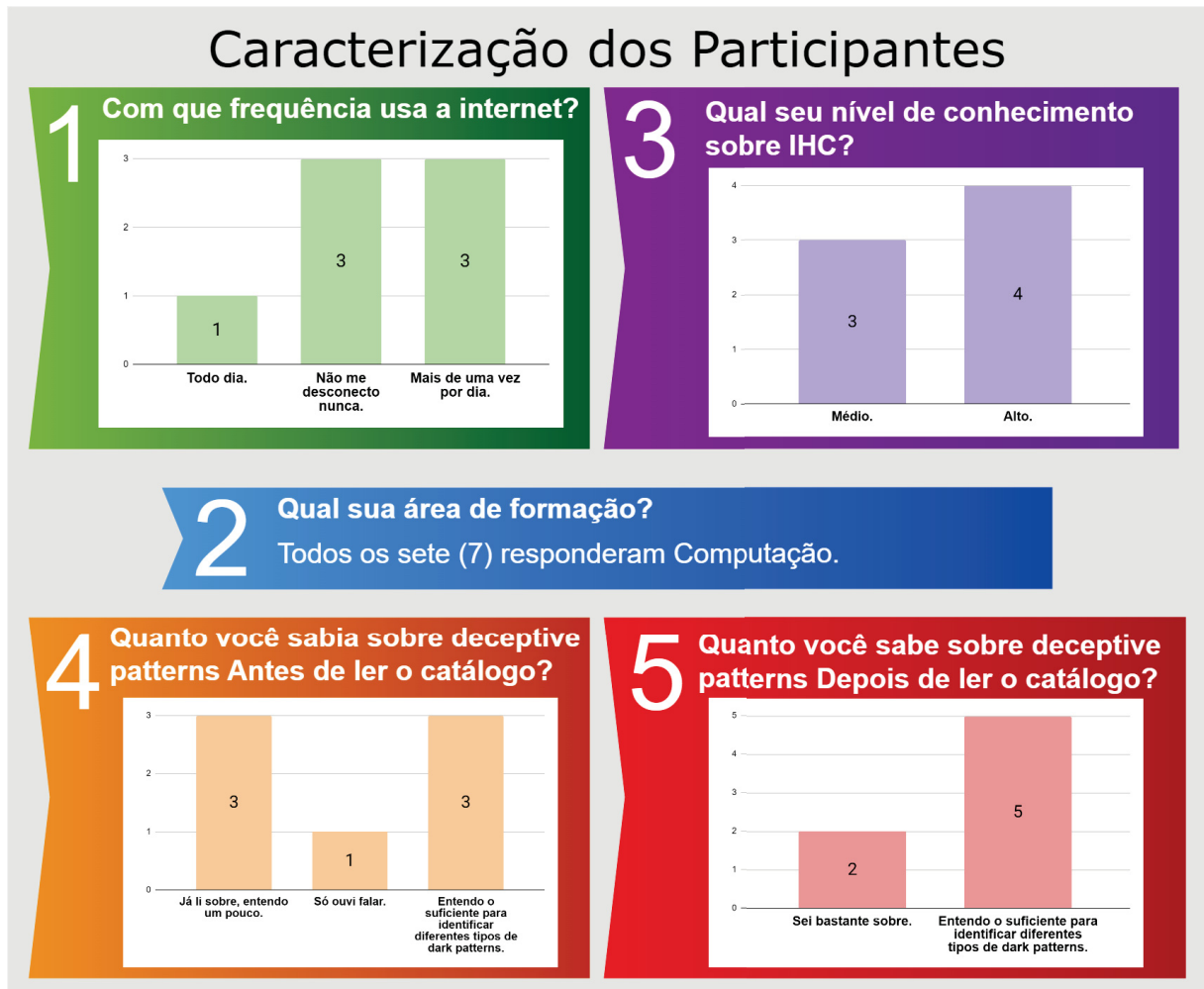


Figura 6.5: Questionário de caracterização e respostas dos participantes.

- Participante 7 - “Achei o catálogo fácil de navegar.”;

Quanto à Utilidade Percebida (Figuras 6.9 e 6.8), o resultado aponta que o catálogo serve de fato como ferramenta útil, que tornaria o trabalho/pesquisa mais fácil, de apoio para desenvolvedores e pesquisadores.

Todos os participantes afirmaram que os exemplos práticos de deceptive patterns implementados no site do catálogo ajudaram a aprender sobre deceptive patterns. Cinco participantes concordaram que usar o catálogo tornaria o trabalho/pesquisa deles mais fácil. Todos os participantes acreditam que o catálogo seria uma ótima ferramenta para desenvolvedores e pesquisadores. Seis participantes afirmaram que usariam o catálogo em seus trabalhos/pesquisas. Os resultados combinados apontam para a utilidade e facilidade do catálogo em ensinar sobre deceptive patterns para pessoas leigas no assunto, sejam elas usuários, pesquisadores, ou desenvolvedores (Figuras 6.9 e 6.8).

Alguns comentários de participantes confirmando a utilidade do catálogo:

- Participante 3 - “Talvez o catálogo de deceptive Patterns seja mais importante para usuários mais leigos, com a finalidade de educar sobre os deceptive Patterns.”;
- Participante 4 - “O catálogo me parece ser de grande utilidade.”;
- Participante 6 - “O site é muito útil para entender de forma didática, divertida e informativa sobre deceptive patterns.”;

Facilidade de Uso

- Aprender a navegar pelo catálogo de Dark Patterns foi fácil para mim.
- Minha interação com o catálogo de Dark Patterns foi clara e compreensível.
- Aprender sobre Dark Patterns pelo catálogo foi fácil para mim.

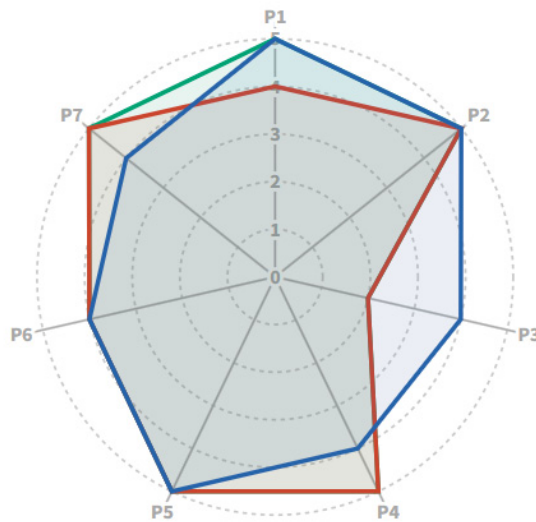


Figura 6.6: Facilidade de Uso.

- Participante 7 - “Consigo me enxergar usando esse catálogo de deceptive patterns ao desenvolver sistemas ou pesquisas sobre o tema. Também acredito que o catálogo pode ser útil num ambiente didático. Consigo imaginar esse catálogo sendo usado em uma discussão(sic) sobre design de interfaces, ou mesmo em uma aula de IHC.”;

6.3.3 Grupo Focal

E logo após a conclusão do questionário, todos os participantes também fizeram parte de um grupo focal, a fim de explicarem melhor as percepções que tiveram sobre o catálogo durante o estudo anterior, permitindo um melhor refinamento do produto final. A Tabela 6.2 traz mais detalhes sobre o grupo focal.

A dinâmica de interação utilizada foi de conversa aberta: o autor perguntou informalmente aos participantes o que acharam do estudo e do catálogo. Em sequência, cada participante contribuiu a partir da fala com a discussão sobre a aceitação do catálogo online. Essa conversa foi gravada via áudio e o áudio foi analisado e transcrito posteriormente para análise. No geral, os participantes se mostraram animados e interessados no catálogo, com falas positivas e oferecendo diversas ideias de como editar e melhorar o website e o catálogo. Alguns participantes se mostraram especialmente animados pelos exemplos práticos de deceptive patterns implementados no website do catálogo:

- “... navegando pelas categorias e lendo cada um dos diferentes deceptive patterns eu senti que foi uma maneira bastante interessante de explorar eles” ... “ver por cima o que cada um deles é, achei que é um jeito interessante de descobrir quais são e aprender um pouco sobre eles ...”;
- “Achei que ficou[sic] ótimo os deceptive patterns que apareceram no próprio website ...”;

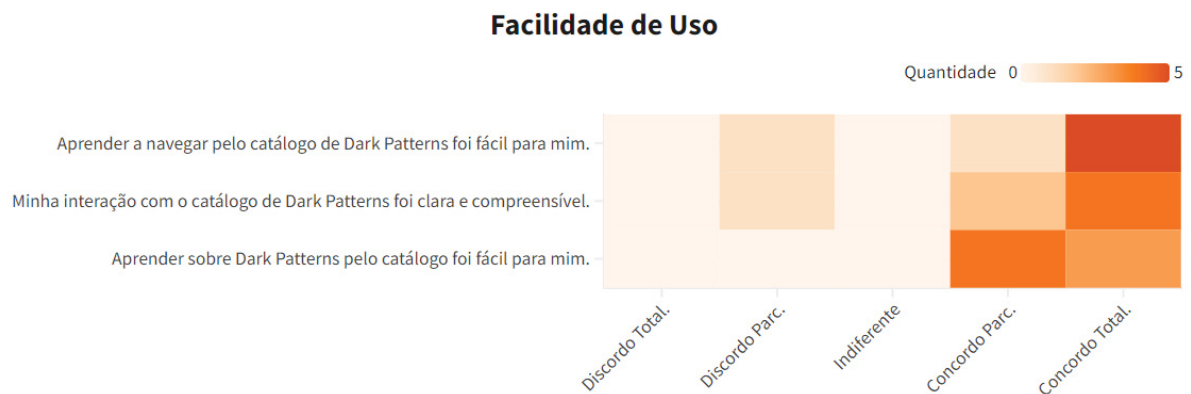


Figura 6.7: Questionário sobre a facilidade de uso.

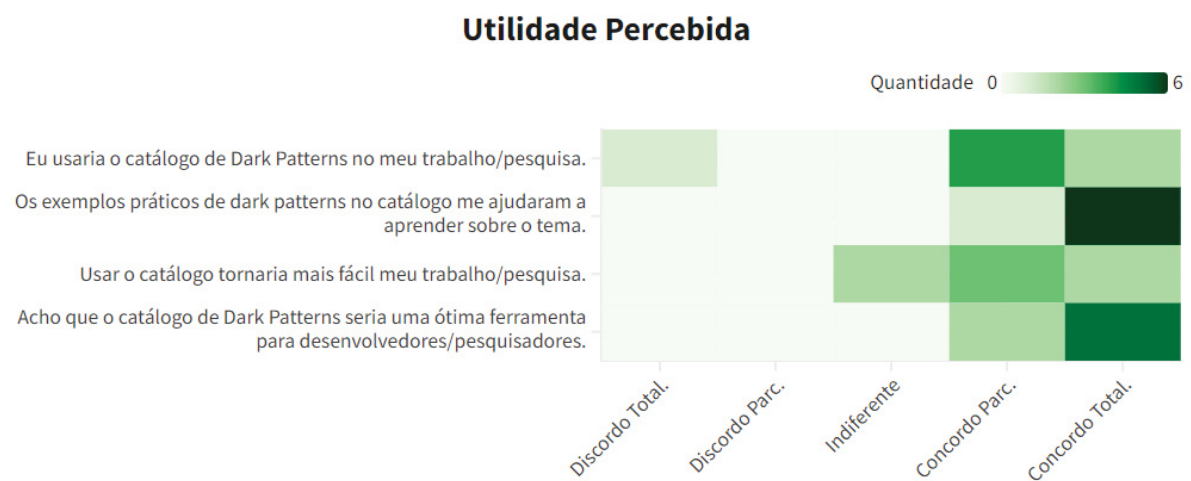


Figura 6.8: Questionário sobre Utilidade Percebida.

- “... o que brilha no site, além do conhecimento, é essa interação de você mostrar de forma didática ali o que que é um deceptive pattern” . . . “ em termos de usabilidade não é pra ter aquilo ali, mas se vc pensa em outros termos, da experiência do usuário, isso é fenomenal, super divertido de interagir com essas coisas . . . “.

Os participantes também ofereceram diversas dicas e sugestões de como alterar o website e o catálogo para torná-lo melhor, como por exemplo:

- Gifs animados em todos os exemplos de deceptive patterns;
- um Quiz sobre deceptive patterns para testar os visitantes do catálogo;
- jogos educativos experimentais sobre deceptive patterns;
- um questionário para descobrir qual deceptive pattern está afetando o usuário;
- ideias de como monetizar o catálogo;
- dentre outras;

Os participantes também pontuaram erros de escrita e implementação do website que encontraram durante o estudo, e que foram devidamente resolvidos.

Utilidade Percebida

- Eu usaria o catálogo de Dark Patterns no meu trabalho/pesquisa.
- Os exemplos práticos de dark patterns no catálogo me ajudaram a aprender sobre o tema.
- Usar o catálogo tornaria mais fácil meu trabalho/pesquisa.
- Acho que o catálogo de Dark Patterns seria uma ótima ferramenta para desenvolvedores/pesquisadores.

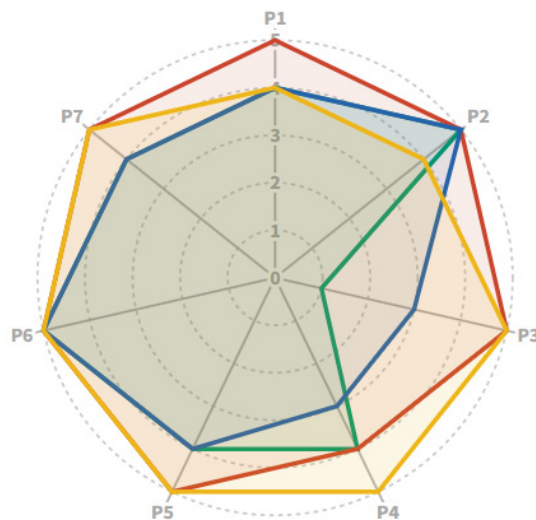


Figura 6.9: Utilidade Percebida.

Objetivo	Obter mais informações críticas e qualitativas sobre a aceitação do catálogo online de deceptive patterns pelos participantes.
Duração total	20 minutos de grupo focal.
Local	Laboratório 3 do Departamento de Informática da Universidade Federal do Paraná, Curitiba-PR;
Data	29 de setembro de 2022;
Participantes	Sete (7) profissionais com experiência em IHC, representantes do público-alvo do catálogo.

Tabela 6.2: Breve resumo do grupo focal.

7 CONCLUSÃO

Neste trabalho foi apresentado o problema de que a literatura traz discussões e análises focadas e limitadas a partes específicas do tema deceptive patterns como por exemplo: apenas listar e categorizar tipos de deceptive patterns, ou apresentar opiniões de usuários dessas interfaces, ou discutir temas ligados à sociedade como ética e valores desses deceptive patterns. Deixando assim de lado outros aspectos dos deceptive patterns que são fundamentais como por exemplo: quem criou/financiou a criação desses padrões, como as empresas se aproveitam das capacidades do meio de transmissão para atrair e manipular, e como esses padrões são capazes de se aproveitar até mesmo do meio físico do usuário.

Com isso, o objetivo deste trabalho foi: **“Caracterizar deceptive patterns como um fenômeno sociotécnico na Computação”**, e para alcançar esse objetivo foram cumpridos os seguintes objetivos específicos:

1. Analisar e caracterizar um deceptive pattern a partir de uma visão sociotécnica;
2. Mapear a literatura sobre deceptive patterns na computação;
3. Analisar os aspectos sociotécnicos considerados e negligenciados na literatura;
4. Elaborar um catálogo dos deceptive patterns mapeados.

Para cumprir os objetivos de forma satisfatória, a metodologia empregada neste trabalho foi baseada em uma investigação analítica e construtiva. A investigação analítica se deu em três etapas:

1. uma análise de um deceptive pattern fundamentada no Framework Semiótico [30];
2. um mapeamento sistemático da literatura sobre interfaces maliciosas nas principais bases de indexação de artigos de computação (ACM, IEEE, e Scopus);
3. uma análise dos aspectos sociotécnicos considerados e negligenciados na literatura, também fundamentada no Framework Semiótico.
4. na investigação construtiva, como contribuição técnica, um catálogo contendo os deceptive patterns mapeados da literatura científica foi organizado, construído, e avaliado por um grupo de sete profissionais com experiência em IHC.

Cumprindo primeiro o objetivo específico, na Seção 4.3: como resultado da análise e caracterização de um deceptive pattern como um fenômeno sociotécnico foi possível demonstrar, no Capítulo 4, a partir da análise do deceptive pattern Hotel de Baratas, como deceptive patterns exploram elementos da interface, da língua, e até da psicologia humana, e que vão desde o mundo social do usuário até o meio físico pelo qual o usuário interage com esse deceptive pattern, de forma sistêmica e interconectada.

E cumprindo o segundo objetivo específico, no Capítulo 5: a partir do mapeamento da literatura sobre deceptive patterns obteve-se um panorama rigoroso da área de deceptive patterns em Ciência da Computação: apesar de haver uma extensa literatura sobre deceptive patterns, a maior parte dela foi construída nos últimos 5 anos (de 2018 até agora). Apesar de ser uma extensa literatura, é possível perceber que a maioria dos autores falha em considerar os deceptive patterns

de forma sistemática, ou mesmo como um fenômeno sociotécnico; Há também discussões e análises exaustivas em torno de avisos de cookies e como estes funcionam e afetam os usuários;

Cumprindo o terceiro objetivo específico, na Seção 5.7: após analisar os aspectos sociotécnicos considerados e negligenciados pela literatura, descobriu-se que a maioria dos artigos favorecem os aspectos sociais dos deceptive patterns (aqueles nas camadas do Mundo Social, Pragmático, e Semântico), e desconsideram os aspectos técnicos das interfaces (nas camadas Sintático, Empírico, e Mundo Físico) maliciosas, e que são fundamentais para explicar como e porque elas existem e funcionam.

Por fim, cumprindo o quarto objetivo específico, no Capítulo 6: o catálogo contendo todos os deceptive patterns encontrados na literatura foi construído e então analisado quanto a sua facilidade de uso e utilidade percebida. O estudo contou com sete participantes que também participaram de um grupo focal após o estudo para melhor entender as opiniões dos participantes. Quanto à facilidade de uso, os participantes indicam que o catálogo é fácil de utilizar e de aprender a utilizar, e que aprender sobre deceptive patterns pelo catálogo também é fácil. Quanto à utilidade percebida, os participantes sugerem que o catálogo é uma ótima ferramenta para desenvolvedores e pesquisadores. Também descobriu-se que usar o catálogo tornaria o trabalho ou pesquisa dos participantes mais fácil, e que os participantes usariam o catálogo em seu trabalho ou pesquisa.

De acordo com os participantes do estudo, os exemplos práticos de deceptive patterns implementados no catálogo foram úteis para ensinar sobre deceptive patterns. Todos os participantes do estudo concordaram com a afirmação "Os exemplos práticos de dark patterns no catalogo me ajudaram a aprender sobre o tema.". Após o estudo, um participante afirmou que aprendeu mais com os exemplos práticos do que com o resto do catálogo. Isso demonstra o potencial didático que os exemplos práticos de deceptive patterns têm, sendo possível conscientizar sobre esse tema, dentro de um ambiente controlado, colocando os usuários em situações "reais" porém sem os riscos associados.

Os resultados desse trabalho, somados, indicam que deceptive patterns são um fenômeno perigoso para o bem-estar de todos que frequentam a internet, podendo causar impactos negativos sociais, emocionais, e até mesmo financeiros e temporais. Esses padrões atuam em favor das empresas e negócios, dos criadores de conteúdo online, de programadores e designers, sempre em detrimento do usuário, muitas vezes de forma que os usuários sequer percebem isso acontecendo. Esse fenômeno já ocorre há muito tempo nos mais variados tipos de interfaces de usuários do celular ao computador ao totem de autoatendimento, em mídias digitais e impressas, e até mesmo em espaços físicos, mas que apenas recentemente, há mais ou menos 6 anos, têm ganhado a devida atenção que merecem. Este trabalho portanto contribui ativamente com o avanço do entendimento sobre deceptive patterns e ajuda não só pesquisadores a entenderem mais sobre deceptive patterns como também usuários e desenvolvedores. Os resultados nos permitem observar os deceptive patterns como um fenômeno de proporções globais e que precisa ser combatido urgentemente.

7.1 ESTRATÉGIA DO CAPITALISMO

No fim, deceptive patterns são mais uma estratégia do capitalismo, resultado do modelo de produção vigente em nossa sociedade. Eles são o resultado de uma supervalorização do lucro a todo custo em detrimento do ser humano e dos impactos que essa busca pode causar. A busca incessante por formas de lucrar em cima de tudo que permeia nossa vida tem levado empresas e negócios a criarem métodos cada vez mais eficientes em capturar as mentes e os desejos das pessoas, tornando-as reféns de seus mais profundos instintos ou medos. Ou seja, os deceptive

patterns surgem quando as empresas e negócios ignoram que seus clientes são, em essência, seres humanos complexos com diferentes realidades e uma vida inteira de necessidades, vontades, responsabilidades, etc. Deceptive patterns surgem quando o ser humano é tratado apenas como "consumidor" ou "usuário" (Gonzatto e van Amstel (2022)). O resultado de uma comodificação da vida em sociedade.

Uma prática deletéria que só causa malefícios a sociedade, e traz pouco ou nenhum benefício a quem utiliza, visto que, da psicologia, quando uma pessoa recebe um reforço negativo (sendo enganada ou lesionada de qualquer forma seja monetária ou temporalmente) essa pessoa tende a evitar a situação que a deixou com uma sensação ruim. Portanto deceptive patterns são ruins não só pra quem sofre, mas a longo prazo são ruins para quem os usa também.

E, infelizmente, não há uma forma simples de nós, como sociedade, nos livrarmos deles sem uma boa dose de trabalho duro e conscientização. Pessoas tem sido enganadas há centenas de anos e ao que tudo indica continuarão a serem enganadas por muito mais tempo. Até o momento, uma solução que têm sido eficaz contra deceptive patterns em outros países é o direito, como no caso da GDPR e da CCPA que tem movido mudanças reais nos banners de cookies das páginas online. Se fazem necessárias leis que ditem especificamente sobre o comportamento predatório de interfaces e empresas nos meios virtuais/digitais, assim como fazem a GDPR europeia e a CCPA californiana. Através da regulação, fiscalização e controle dessas práticas, assim como já se faz de tantas outras práticas comumente conhecidas por violarem os direitos do consumidor, será possível reduzir os impactos dos deceptive patterns na sociedade e punir aqueles que os utilizam.

Porém, é fundamental também focar na conscientização das pessoas sobre essas práticas. Conhecimento é uma excelente forma de empoderar as pessoas a fim de que consigam, sozinhas, tomarem decisões que façam bem para suas vidas, e não caiem em golpes e propagandas enganosas.

7.2 LIMITAÇÕES E AMEAÇAS A VALIDADE

Os principais desafios e limitações deste trabalho foram: a língua utilizada no mapeamento foi limitada a inglês, o que pode ter deixado de fora artigos importantes de língua portuguesa; durante o mapeamento, a string de busca utilizada estava incompleta, deixando de fora o termo *manipulative* que poderia ter adicionado mais artigos de interesse da pesquisa; a análise sociotécnica foi realizada com apenas um padrão em específico, o que pode levar a uma compreensão parcial do todo.

Faltam pesquisas prévias que tenham analisado deceptive patterns apoiadas no Framework Semiótico, que pudessem apoiar essa pesquisa; o estudo de aceitação do catálogo foi realizado apenas com profissionais de IHC, o que limita as conclusões possíveis, sendo necessário um estudo posterior, mais amplo, para confirmação com o público geral.

7.3 CONTRIBUÇÕES E TRABALHOS FUTUROS

Como desdobramentos da pesquisa, este trabalho contribui com a ciência avançando o conhecimento da comunidade sobre deceptive patterns, baseado em uma visão sociotécnica: é destacado como os deceptive patterns podem explorar e impactar diferentes aspectos relacionados às plataformas de informação e comunicação (do hardware à linguagem) e às funções de informação humana (da capacidade de compreensão às expectativas e crenças) de forma interligada. Este trabalho também mostra como a comunidade acadêmica tende a focar mais em aspectos das funções humanas em detrimento da plataforma técnica, o que pode resultar em

análises ou conclusões incompletas, que deixam de lado pontos importantes ou do social ou do técnico, devido a natureza sistêmica dos deceptive patterns.

Espera-se também que o catálogo consiga ajudar usuários a ficarem atentos aos padrões de design criados para enganá-los e manipulá-los, reduzindo assim os impactos negativos em suas vidas. Também é capaz de conscientizar os profissionais responsáveis pelo design de interfaces sobre os impactos do seu trabalho no mundo real, e a importância de um trabalho ético.

Após a construção do catálogo e avaliação prévia de sua facilidade de uso e utilidade percebida, em um trabalho futuro será possível avaliar se o catálogo é capaz de apoiar a conscientização de usuários, com ajuda de um estudo de caso com usuários. Também será possível ampliar o website do catálogo, para conter mais deceptive patterns auto-explicativos, e também um quiz com perguntas e respostas, a fim de engajar mais os usuários servindo como exercício de reforço sobre o conteúdo aprendido no catálogo.

Este trabalho trouxe uma visão em largura sobre o tema deceptive patterns, olhando de forma geral tudo que está sendo feito na área. E como trabalho futuro, é possível utilizar o Framework Semiótico para se analisar em profundidade esse tema. Seja analisando outros deceptive patterns específicos, seja entrando mais a fundo em cada camada para se compreender melhor como funcionam os mecanismos internos dos deceptive patterns. Ou mesmo observar um panorama geral da literatura mais focado em cada camada.

Para pesquisas futuras, cada camada pode ser explorada em profundidade para revelar mais detalhes sobre a mecânica dos deceptive patterns. Olhar mais profundamente para as Funções da Informação Humana (Mundo Social, Pragmática, Semântica) pode nos ajudar a investigar os efeitos dos aspectos técnicos dos deceptive patterns em diferentes contextos e públicos, considerando como as características socioeconômicas e culturais se relacionam com os deceptive patterns.

Analisar mais profundamente a Plataforma Técnica (sintática, empírica, mundo físico), por sua vez, pode ajudar a entender como os deceptive patterns são construídos e espalhados e ajudar a descobrir características e estruturas comuns que podem ser usadas para identificar deceptive patterns manualmente ou automaticamente. A melhor compreensão do fenômeno possibilita formas socialmente responsáveis de mitigar suas práticas e efeitos.

Também será possível uma análise técnica ainda mais situada de sistemas e sites de empresas brasileiras identificando quais usam estratégias antiéticas e quais não, e talvez, criar um selo de garantia para aqueles que se esforcem em criar interfaces sem padrões enganosos e manipulativos.

REFERÊNCIAS

- (2018). Lei geral de proteção de dados pessoais (lgpd). Página inicial.
- (2020). California consumer privacy act (ccpa). Página inicial.
- Aagaard, J. e et al. (2022). A game of dark patterns: Designing healthy, highly-engaging mobile games. Em *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, páginas 1–8.
- Ackerman, F. (1995). The concept of manipulateness. *Philosophical Perspectives*, 9:335–340.
- Acquisti, A. e et al. (2017). Nudges for privacy and security: Understanding and assisting users’ choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41.
- Adar, E., Tan, D. S. e Teevan, J. (2013). Benevolent deception in human computer interaction. Em *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, páginas 1863–1872.
- Alexander, C. (1979). *The Timeless Way of Building*. Oxford University Press.
- Arkes, H. R. e Ayton, P. (1999). The sunk cost and concorde effects: Are humans less rational than lower animals? *Psychological Bulletin*, 125(5):591.
- Aydemir, F. B. e Dalpiaz, F. (2018). A roadmap for ethics-aware software engineering. Em *2018 IEEE/ACM International Workshop on Software Fairness (FairWare)*, páginas 15–21.
- Ballard, C. e et al. (2022). Conspiracy brokers: understanding the monetization of youtube conspiracy theories. Em *Proceedings of the ACM Web Conference 2022*, páginas 2707–2718.
- Bardzell, J. (2011). Interaction criticism: An introduction to the practice. *Interacting with computers*, 23(6):604–621.
- Baroni, L. A. e et al. (2021). Dark patterns: Towards a socio-technical approach. Em *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*, páginas 1–7.
- Basili, V. R. e Rombach, H. D. (1988). The tame project: Towards improvement-oriented software environments. *IEEE Transactions on Software Engineering*, 14(6):758–773.
- Bauer, J. M., Bergstrøm, R. e Foss-Madsen, R. (2021). Are you sure, you want a cookie?—the effects of choice architecture on users’ decisions about sharing private online data. *Computers in Human Behavior*, 120:106729.
- Beck, K. e Cunningham, W. (1987). Using pattern languages for object oriented programs. Em *OOP-SLA-87 Workshop on Specification and Design for Object-Oriented Programming*.
- Bem, D. J. (1967). Self-perception: An alternative interpretation of cognitive dissonance phenomena. *Psychological review*, 74(3):183.
- Bermejo Fernández, C. e et al. (2021). This website uses nudging: Mturk workers’ behaviour on cookie consent notices. *Proceedings of the ACM on human-computer interaction*, 5(CSCW2):1–22.

- Bhoot, A. M., Shinde, M. A. e Mishra, W. P. (2020). Towards the identification of dark patterns: An analysis based on end-user reactions. Em *IndiaHCI'20: Proceedings of the 11th Indian Conference on Human-Computer Interaction*, páginas 24–33.
- Bongard-Blanchy, K. e et al. (2021). "i am definitely manipulated, even when i am aware of it. it's ridiculous!-dark patterns from the end-user perspective. Em *Designing Interactive Systems Conference*, páginas 763–776.
- Borning, A. e et al. (2020). Surveillancecapitalism@ chi: Civil conversation around a difficult topic. Em *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, páginas 1–6.
- Boyd, d. (2008). Understanding socio-technical phenomena in a web2.0 era. MSR New England Lab Opening, Cambridge MA, September 22.
- Braun, V. e Clarke, V. (2012). *Thematic analysis*. American Psychological Association.
- Brignull, H., Leiser, M., Santos, C. e Doshi, K. (2023). Deceptive patterns – user interfaces designed to trick you.
- Bösch, C. e et al. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4):237–254.
- Chang, D. e et al. (2016). Engineering information disclosure: Norm shaping designs. Em *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, páginas 587–597.
- Chaudhary, A. e et al. (2022). “are you still watching?”: Exploring unintended user behaviors and dark patterns on video streaming platforms. Em *Designing Interactive Systems Conference*, páginas 776–791.
- Chaudhry, S. e Kulkarni, C. (2021). Design patterns of investing apps and their effects on investing behaviors. Em *Designing Interactive Systems Conference 2021*, páginas 777–788.
- Chen, J. X. e et al. (2022). Trauma-informed computing: Towards safer technology experiences for all. Em *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, páginas 1–20.
- Chivukula, S. S. e et al. (2019). "nothing comes before profit"asshole design in the wild. Em *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, páginas 1–6.
- Chivukula, S. S., Gray, C. M. e Brier, J. A. (2019). Analyzing value discovery in design decisions through ethicography. Em *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, páginas 1–12.
- Cho, H. e et al. (2021). Reflect, not regret: Understanding regretful smartphone use with app feature-level analysis. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–36.
- Chromik, M. e et al. (2019). Dark patterns of explainability, transparency, and user control for intelligent systems. Em *IUI Workshops*.

- Clemons, E. K. e et al. (2022). Computing and social welfare: Minimizing societal harm from digital transformation while preserving the benefits of innovation in online businesses. *Electronic Markets*, 32(2):417–436.
- Conti, G. e Sobiesk, E. (2009). Malicious interfaces and personalization’s uninviting future. *IEEE Security Privacy*, 7(3):64–67.
- Conti, G. e Sobiesk, E. (2010). Malicious interface design: Exploiting the user. Em *Proceedings of the 19th International Conference on World Wide Web*, páginas 271–280.
- Cornelius, K. B. (2019). Zombie contracts, dark patterns of design, and ‘documentisation’. *Internet Policy Review*, 8(2):1–25.
- Cranor, L. F. (2022). Cookie monster. *Communications of the ACM*, 65(7):30–32.
- Das, M. e et al. (2022). Platform governance: Past, present and future. *GetMobile: Mobile Computing and Communications*, 26(1):14–20.
- Datta, S., Kollnig, K. e Shadbolt, N. (2022). Mind-proofing your phone: Navigating the digital minefield with greaseterminator. Em *27th International Conference on Intelligent User Interfaces*, páginas 523–536.
- Davis, F. D. (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*. Tese de doutorado, Massachusetts Institute of Technology.
- Davis, J. (2009). Design methods for ethical persuasive computing. Em *Proceedings of the 4th International Conference on Persuasive Technology*, páginas 1–8.
- Di Geronimo, L. e et al. (2020). Ui dark patterns and where to find them: A study on mobile applications and user perception. Em *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, páginas 1–14.
- Dickinson, R., Semertzidis, N. e Mueller, F. F. (2022). Machine in the middle: Exploring dark patterns of emotional human-computer integration through media art. Em *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, páginas 1–7.
- Dreyer, J. e et al. (2022). ‘informed’ consent in popular location based services and digital sovereignty. *Journal of Location Based Services*, 16(4):312–342.
- Fansher, M., Chivukula, S. S. e Gray, C. M. (2018). darkpatterns: Ux practitioner conversations about ethical design. Em *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, páginas 1–6.
- Farooq, U. e Grudin, J. (2016). Human-computer integration. *Interactions*, 23(6):26–32.
- Ferrari, B. e et al. (2019). Design socialmente consciente de jogos: Relato de uma oficina prática para o entendimento do problema e prospecção de ideias. Em *Anais do I Workshop sobre Interação e Pesquisa de Usuários no Desenvolvimento de Jogos*, páginas 11–20. SBC.
- Fitton, D. e Read, J. C. (2019). Creating a framework to support the critical consideration of dark design aspects in free-to-play apps. Em *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, páginas 407–418.

- Fogg, B. J. (1998). Captology: the study of computers as persuasive technologies. Em *CHI 98 Conference Summary on Human Factors in Computing Systems*, página 385.
- Fogg, B. J. (1999). Persuasive technologies. *Communications of the ACM*, 42(5):26–29.
- Friedman, B. e Hendry, D. G. (2019). *Value Sensitive Design: Shaping Technology with Moral Imagination*. MIT Press.
- Friedman, B., Kahn Jr, P. H. e Börning, A. (2008). Value sensitive design and information systems. Em *The Handbook of Information and Computer Ethics*, páginas 69–101.
- Gonzatto, R. F. e Van Amstel, F. M. (2017). Designing oppressive and libertarian interactions with the conscious body. Em *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems*, páginas 1–10.
- Gonzatto, R. F. e van Amstel, F. M. (2022). User oppression in human-computer interaction: a dialectical-existential perspective. *Aslib Journal of Information Management*.
- Gray, C. M. e Chivukula, S. S. (2019). Ethical mediation in ux practice. Em *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, páginas 1–11.
- Gray, C. M., Chivukula, S. S. e Lee, A. (2020). What kind of work do "asshole designers" create? describing properties of ethical concern on reddit. Em *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, páginas 61–73.
- Gray, C. M. e et al. (2018). The dark (patterns) side of ux design. Em *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, páginas 1–14.
- Gray, C. M. e et al. (2021a). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. Em *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–18.
- Gray, C. M. e et al. (2021b). End user accounts of dark patterns as felt manipulation. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–25.
- Gray, C. M., Santos, C. e Bielova, N. (2023). Towards a preliminary ontology of dark patterns knowledge. Em *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, páginas 1–9.
- Greenberg, S. e et al. (2014). Dark patterns in proxemic interactions: A critical perspective. Em *Proceedings of the 2014 Conference on Designing Interactive Systems*, páginas 523–532.
- Gugenheimer, J. e et al. (2022). Novel challenges of safety, security and privacy in extended reality. Em *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, páginas 1–5.
- Gunawan, J. e et al. (2021). A comparative study of dark patterns across web and mobile modalities. volume 5, páginas 1–29.
- Habib, H. e et al. (2022a). Identifying user needs for advertising controls on facebook. Em *Proceedings of the ACM on Human-Computer Interaction*, volume 6, páginas 1–42.

- Habib, H. e et al. (2022b). “okay, whatever”: An evaluation of cookie consent interfaces. Em *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, páginas 1–27.
- Hadi Mogavi, R. e et al. (2022). When gamification spoils your learning: A qualitative case study of gamification misuse in a language-learning app. Em *Proceedings of the Ninth ACM Conference on Learning@ Scale*, páginas 175–188.
- Hu, X., Sastry, N. e Mondal, M. (2021). Cccc: Corraling cookies into categories with cookiemonster. Em *13th ACM Web Science Conference 2021*, páginas 234–242.
- Ilany Tzur, N., Zalmanson, L. e Oestreicher-Singer, G. (2016). The dark side of user participation-the effect of calls to action on trust and information revelation. *Available at SSRN 2814903*.
- Johnson, E. J., Bellman, S. e Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing letters*, 13:5–15.
- Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9):697.
- Kai-Ineman, D. e Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2):363–391.
- Kampanos, G. e Shahandashti, S. F. (2021). Accept all: The landscape of cookie banners in greece and the uk. Em *ICT Systems Security and Privacy Protection: 36th IFIP TC 11 International Conference, SEC 2021, Oslo, Norway, June 22–24, 2021, Proceedings*, páginas 213–227, Cham. Springer.
- Kender, K. e Frauenberger, C. (2022). The shape of social media: Towards addressing (aesthetic) design power. Em *Designing Interactive Systems Conference*, páginas 365–376.
- Kitchenham, B. e Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Relatório técnico.
- Kitkowska, A., Högberg, J. e Wästlund, E. (2022). Online terms and conditions: Improving user engagement, awareness, and satisfaction through ui design. Em *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, páginas 1–22.
- Koenig, A. (1998). Patterns and antipatterns. *The Patterns Handbook: Techniques, Strategies, and Applications*, 13:383.
- Kollnig, K., Datta, S. e van Kleek, M. (2021). I want my app that way: Reclaiming sovereignty over personal devices. Em *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–8.
- Kotut, L. e McCrickard, D. S. (2022). The tl; dr charter: Speculatively demystifying privacy policy documents and terms agreements. *Proceedings of the ACM on Human-Computer Interaction*, 6(GROUP):1–14.
- Krisam, C. e et al. (2021). Dark patterns in the wild: Review of cookie disclaimer designs on top 500 german websites. Em *Proceedings of the 2021 European Symposium on Usable Security*, páginas 1–8.

- Lacey, C. e Caudwell, C. (2019). Cuteness as a 'dark pattern' in home robots. Em *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, páginas 374–381.
- Landis, J. R. e Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, páginas 159–174.
- Landwehr, M., Borning, A. e Wulf, V. (2019). The high cost of free services: Problems with surveillance capitalism and possible alternatives for it infrastructure. Em *Proceedings of the Fifth Workshop on Computing within Limits*, páginas 1–10.
- Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology*, 32(2):311.
- Loomes, G. e Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. *The economic journal*, 92(368):805–824.
- Lovett, F. (2006). Rational choice theory and explanation. *Rationality and Society*, 18(2):237–272.
- Lukoff, K. e et al. (2021a). How the design of youtube influences user sense of agency. Em *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–17.
- Lukoff, K. e et al. (2021b). What can chi do about dark patterns? Em *Extended abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–6.
- Ma, E. e Birrell, E. (2022). Prospective consent: The effect of framing on cookie consent decisions. Em *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, páginas 1–6.
- Maier, M. e Harr, R. (2020). Dark design patterns: An end-user perspective. *Human Technology*, 16(2).
- Maike, V. R., Buchdid, S. B. e Baranauskas, M. C. C. (2015). Designing natural user interfaces scenarios for all and for some: An analysis informed by organizational semiotics artifacts. Em *International Conference on Informatics and Semiotics in Organisations*, páginas 92–101.
- Mathur, A. (2021). Identifying and measuring manipulative user interfaces at scale on the web. Em *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–5.
- Mathur, A. e et al. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32.
- Mathur, A., Kshirsagar, M. e Mayer, J. (2021). What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. Em *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–18.
- Mildner, T. e Savino, G.-L. (2021). Ethical user interfaces: Exploring the effects of dark patterns on facebook. Em *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–7.
- Mittone, L. e Savadori, L. (2009). The scarcity bias. *Applied Psychology*, 58(3):453–468.

- Monahan, T. (2016). Built to lie: Investigating technologies of deception, surveillance, and control. *The Information Society*, 32(4):229–240.
- Monge Roffarello, A. e De Russis, L. (2022). Towards understanding the dark patterns that steal our attention. Em *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, páginas 1–7.
- Monge Roffarello, A. e et al. (2022). Designing for meaningful interactions and digital wellbeing. Em *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, páginas 1–2.
- Morkonda, S. G., Chiasson, S. e van Oorschot, P. C. (2021). Empirical analysis and privacy implications in oauth-based single sign-on systems. Em *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, páginas 195–208.
- Moser, C., Schoenebeck, S. Y. e Resnick, P. (2019). Impulse buying: Design practices and consumer needs. Em *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, páginas 1–15.
- Mäkelä, V. e et al. (2019). Acceptance and perceptions of interactive location-tracking displays. Em *Proceedings of the 8th ACM International Symposium on Pervasive Displays*, páginas 1–7.
- Narayanan, A. e et al. (2020). Dark patterns: Past, present, and future: The evolution of tricky user interfaces. *Queue*, 18(2):67–92.
- Nelissen, L. e Funk, M. (2022). Rationalizing dark patterns: Examining the process of designing privacy ux through speculative enactments. *International Journal of Design*, 16(1):75–92.
- Norval, C. e et al. (2018). Reclaiming data: Overcoming app identification barriers for exercising data protection rights. Em *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, páginas 921–930.
- Nouwens, M. e et al. (2020). Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. Em *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, páginas 1–13.
- Nystrom, T. (2021). Exploring the darkness of gamification: You want it darker? Em *Intelligent Computing*, páginas 491–506, Cham. Springer.
- Nyström, T. e Stibe, A. (2020). When persuasive technology gets dark? Em *European, Mediterranean, and Middle Eastern Conference on Information Systems*, páginas 331–345.
- O'Connor, S. e et al. (2021). (un)clear and (in)conspicuous: The right to opt-out of sale under ccpa. Em *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, páginas 59–72.
- Oulasvirta, A. e Hornbæk, K. (2016). Hci research as problem-solving. Em *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, páginas 4956–4967.
- Paay, J. e Rogers, Y. (2019). The dark side of interaction design: Nudges, dark patterns and digital addiction: Panel presented at ozchi 2019. Em *Proceedings of the 31st Australian Conference on Human-Computer-Interaction*, páginas 2–2.

- Petrovskaya, E., Deterding, S. e Zendle, D. I. (2022). Prevalence and salience of problematic microtransactions in top-grossing mobile and pc games: a content analysis of user reviews. Em *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, páginas 1–12.
- Pinder, C. (2017). The anti-influence engine: Escaping the diabolical machine of pervasive advertising. Em *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, páginas 770–781.
- Przybylski, A. K. e et al. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, 29(4):1841–1848.
- Puska, A., Baroni, L. A., Canal, M. C., Piccolo, L. S. e Pereira, R. (2020). Whatsapp and false information: a value-oriented evaluation. Em *Proceedings of the 19th Brazilian Symposium on Human Factors in Computing Systems*, páginas 1–10.
- Rogers, Y. e et al. (2020). The dark side of interaction design. Em *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, páginas 1–4.
- Rogers, Y. e et al. (2021). The dark side of interaction design. Em *Extended abstracts of the 2021 CHI conference on human factors in computing systems*, páginas 1–2.
- Rosenberger, R. (2020). On hostile design: Theoretical and empirical prospects. *Urban Studies*, 57(4):883–893.
- Rychwalska, A. (2022). Shadow (profiles) in the dark (patterns): Who locked your digital self? *IEEE Technology and Society Magazine*, 41(2):78–83.
- Sanchez-Rola, I. e et al. (2019). Can i opt out yet? gdpr and the global illusion of cookie control. Em *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, páginas 340–351.
- Savic, S. e Savicic, G. (2014). Unpleasant design. designing out unwanted behaviour. Em *Proceedings of the 5th STS Italia Conference: A Matter of Design. Making Society through Science and Technology*, páginas 975–988.
- Seymour, W. e van Kleek, M. (2021). Exploring interactions between trust, anthropomorphism, and relationship development in voice assistants. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–16.
- Sherif, M. (1936). *The psychology of social norms*.
- Singh, A. e et al. (2022). Erasing labor with labor: Dark patterns and lockstep behaviors on google play. Em *Proceedings of the 33rd ACM Conference on Hypertext and Social Media*, páginas 186–191.
- Soe, T. H. e et al. (2020). Circumvention by design-dark patterns in cookie consent for online news outlets. Em *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, páginas 1–12.
- Stamper, R. (1993). A semiotic theory of information and information systems. Em *Invited Papers for the ICL/University of Newcastle Seminar on Information*.

- Tahaei, M. e Vania, K. (2021). “developers are responsible”: What ad networks tell developers about privacy. Em *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–11.
- Trice, M. e Potts, L. (2018). Building dark patterns into platforms: How gamergate perturbed twitter’s user experience. *Present Tense: A Journal of Rhetoric in Society*, 6(3).
- Tversky, A. e Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *Science*, 185(4157):1124–1131.
- Tversky, A. e Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, 211(4481):453–458.
- Union, E. (2022). General data protection regulation (gdpr) – official legal text.
- Utz, C. e et al. (2019). (un)informed consent: Studying gdpr consent notices in the field. Em *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, páginas 973–990.
- Vilaza, G. N. e et al. (2022). A scoping review of ethics across sigchi. Em *Designing Interactive Systems Conference*, páginas 137–154.
- Voigt, C., Schlögl, S. e Groth, A. (2021). Dark patterns in online shopping: Of sneaky tricks, perceived annoyance and respective brand trust. Em *HCI in Business, Government and Organizations: 8th International Conference, HCIBGO 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings*, páginas 143–155.
- Westin, F. e Chiasson, S. (2019). Opt out of privacy or "go home" understanding reluctant privacy behaviours through the fomo-centric design paradigm. Em *Proceedings of the New Security Paradigms Workshop*, páginas 57–67.
- Westin, F. e Chiasson, S. (2021). “it’s so difficult to sever that connection”: The role of fomo in users’ reluctant privacy behaviours. Em *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–15.
- Widdicks, K. (2020). When the good turns ugly: Speculating next steps for digital wellbeing tools. Em *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, páginas 1–6.
- Widdicks, K., Pargman, D. e Bjork, S. (2020). Backfiring and favouring: How design processes in hci lead to anti-patterns and repentant designers. Em *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, páginas 1–12.
- Zagal, J. P., Björk, S. e Lewis, C. (2013). Dark patterns in the design of games. Em *Foundations of Digital Games 2013*.
- Zeng, E., Kohno, T. e Roesner, F. (2021). What makes a "bad" ad? user perceptions of problematic online advertising. Em *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, páginas 1–24.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

APÊNDICE A – ARTIGOS SELECIONADOS NO MAPEAMENTO SISTEMÁTICO

Artigos encontrados no mapeamento (com ID e ano).

ID	Título	Ano
A1	'Informed' consent in popular location based services and digital sovereignty (Dreyer e et al., 2022);	2022
A2	"Nothing Comes Before Profit": Asshole Design In the Wild (Chivukula e et al., 2019);	2019
A3	"Are You Still Watching?": Exploring Unintended User Behaviors and Dark Patterns on Video Streaming Platforms (Chaudhary e et al., 2022);	2022
A4	"Okay, Whatever": An Evaluation of Cookie Consent Interfaces (Habib e et al., 2022b);	2022
A5	(Un)clear and (In)conspicuous: The Right to Opt-out of Sale under CCPA (O'Connor e et al., 2021);	2021
A6	(Un)informed Consent: Studying GDPR Consent Notices in the Field (Utz e et al., 2019);	2019
A7	#darkpatterns: UX Practitioner Conversations About Ethical Design (Fansher et al., 2018);	2018
A8	A Comparative Study of Dark Patterns Across Web and Mobile Modalities (Gunawan e et al., 2021);	2021
A9	A Game of Dark Patterns: Designing Healthy, Highly-Engaging Mobile Games (Aagaard e et al., 2022);	2022
A10	A roadmap for ethics-aware software engineering (Aydemir e Dalpiaz, 2018);	2018
A11	A Scoping Review of Ethics Across SIGCHI (Vilaza e et al., 2022);	2022
A12	Accept All: The Landscape of Cookie Banners in Greece and the UK (Kampanos e Shahandashti, 2021);	2021
A13	Acceptance and perceptions of interactive location-tracking displays (Mäkelä e et al., 2019);	2019
A14	Analyzing Value Discovery in Design Decisions Through Ethicography (Chivukula et al., 2019);	2019
A15	Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data (Bauer et al., 2021);	2021
A16	Backfiring and favouring: how design processes in HCI lead to anti-patterns and repentant designers (Widdicks et al., 2020);	2020
A17	Benevolent deception in human computer interaction (Adar et al., 2013);	2013
A18	Built to lie: Investigating technologies of deception, surveillance, and control (Monahan, 2016);	2016

ID	Título	Ano
A19	Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control (Sanchez-Rola e et al., 2019);	2019
A20	CCCC: Corraling Cookies into Categories with CookieMonster (Hu et al., 2021);	2021
A21	Circumvention by design - dark patterns in cookie consent for online news outlets (Soe e et al., 2020);	2020
A22	Computing and Social Welfare: Minimizing societal harm from digital transformation while preserving the benefits of innovation in online businesses (Clemons e et al., 2022);	2022
A23	Conspiracy Brokers: Understanding the Monetization of YouTube Conspiracy Theories (Ballard e et al., 2022);	2022
A24	Cookie Monster (Cranor, 2022);	2022
A25	Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps (Fitton e Read, 2019);	2019
A26	Cuteness as a 'dark pattern' in home robots (Lacey e Caudwell, 2019);	2019
A27	Dark design patterns: An end-user perspective (Maier e Harr, 2020);	2020
A28	Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence (Nouwens e et al., 2020);	2020
A29	Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective (Gray e et al., 2021b);	2021
A30	Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites (Mathur e et al., 2019);	2019
A31	Dark Patterns in Online Shopping: of Sneaky Tricks, Perceived Annoyance and Respective Brand Trust (Voigt et al., 2021);	2021
A32	Dark patterns in proxemic interactions: a critical perspective (Greenberg e et al., 2014);	2014
A33	Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites (Krisam e et al., 2021);	2021
A34	Dark patterns of explainability, transparency, and user control for intelligent systems (Chromik e et al., 2019);	2019
A35	Dark patterns: past, present, and future (Narayanan e et al., 2020);	2020
A36	Dark Patterns: Towards a Socio-Technical Approach (Baroni e et al., 2021);	2021
A37	Design methods for ethical persuasive computing (Davis, 2009);	2009

ID	Título	Ano
A38	Design Patterns of Investing Apps and Their Effects on Investing Behaviors (Chaudhry e Kulkarni, 2021);	2021
A39	Designing for Meaningful Interactions and Digital Wellbeing (Monge Roffarello e et al., 2022);	2022
A40	Developers Are Responsible: What Ad Networks Tell Developers About Privacy (Tahaei e Vania, 2021);	2021
A41	Empirical Analysis and Privacy Implications in OAuth-Based Single Sign-On Systems (Morkonda et al., 2021);	2021
A42	End User Accounts of Dark Patterns as Felt Manipulation (Gray e et al., 2021b);	2021
A43	Engineering Information Disclosure: Norm Shaping Designs (Chang e et al., 2016);	2016
A44	Erasing Labor with Labor: Dark Patterns and Lockstep Behaviors on Google Play (Singh e et al., 2022);	2022
A45	Ethical Mediation in UX Practice (Gray e Chivukula, 2019);	2019
A46	Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook (Mildner e Savino, 2021);	2021
A47	Exploring Interactions Between Trust, Anthropomorphism, and Relationship Development in Voice Assistants (Seymour e van Kleek, 2021);	2021
A48	Exploring the Darkness of Gamification: You Want It Darker? (Nystrom, 2021);	2021
A49	How the Design of YouTube Influences User Sense of Agency (Lukoff e et al., 2021a);	2021
A50	I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous! - Dark Patterns from the End-User Perspective (Bongard-Blanchy e et al., 2021);	2021
A51	I Want My App That Way: Reclaiming Sovereignty Over Personal Devices (Kollnig et al., 2021);	2021
A52	Identifying and Measuring Manipulative User Interfaces at Scale on the Web (Mathur, 2021);	2021
A53	Identifying Manipulative Advertising Techniques in XR Through Scenario Construction (Mathur, 2021);	2021
A54	Identifying User Needs for Advertising Controls on Facebook (Habib e et al., 2022a);	2022
A55	Impulse Buying: Design Practices and Consumer Needs (Moser et al., 2019);	2019

ID	Título	Ano
A56	It's So Difficult to Sever That Connection: The Role of FoMO in Users' Reluctant Privacy Behaviours (Westin e Chiasson, 2021);	2021
A57	Machine In The Middle: Exploring Dark Patterns of Emotional Human-Computer Integration Through Media Art (Dickinson et al., 2022);	2022
A58	Malicious interface design: exploiting the user (Conti e Sobiesk, 2010);	2010
A59	Malicious Interfaces and Personalization's Uninviting Future (Conti e Sobiesk, 2009);	2009
A60	Mind-Proofing Your Phone: Navigating the Digital Minefield with GreaseTerminator (Datta et al., 2022);	2022
A61	Novel Challenges of Safety, Security and Privacy in Extended Reality (Gugenheimer e et al., 2022);	2022
A62	Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online (Acquisti e et al., 2017);	2017
A63	Online Terms and Conditions: Improving User Engagement, Awareness, and Satisfaction through UI Design (Kitkowska et al., 2022);	2022
A64	Opt out of privacy or "go home": understanding reluctant privacy behaviors through the FoMO-centric design paradigm (Westin e Chiasson, 2019);	2019
A65	Persuasive technologie301398 (Fogg, 1999);	1999
A66	Platform Governance: Past, Present and Future (Das e et al., 2022);	2022
A67	Prevalence and Salience of Problematic Microtransactions in Top-Grossing Mobile and PC Games: A Content Analysis of User Reviews (Petrovskaya et al., 2022);	2022
A68	Prospective Consent: The Effect of Framing on Cookie Consent Decisions (Ma e Birrell, 2022)	2022
A69	Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments (Nelissen e Funk, 2022);	2022
A70	RECLAIMING Data: Overcoming App Identification Barriers for Exercising Data Protection Rights (Norval e et al., 2018);	2018
A71	Reflect, Not Regret: Understanding Regretful Smartphone Use with App Feature-Level Analysis (Cho e et al., 2021);	2021
A72	Shadow (Profiles) in the Dark (Patterns): Who Locked Your Digital Self? (Rychwalska, 2022);	2022

ID	Título	Ano
A73	SurveillanceCapitalism@CHI: Civil Conversation around a Difficult Topic (Borning e et al., 2020);	2020
A74	That's Dastardly Ingenious: Ethical Argumentation Strategies on Reddit (Gray e et al., 2021b);	2021
A75	The Anti-Influence Engine: Escaping the Diabolical Machine of Pervasive Advertising (Pinder, 2017);	2017
A76	The Dark (Patterns) Side of UX Design (Gray e et al., 2018);	2018
A77	The Dark Side of Interaction Design (Rogers e et al., 2020);	2020
A78	The Dark Side of Interaction Design (Rogers e et al., 2021);	2021
A79	The Dark Side of Interaction Design: Nudges, Dark Patterns and Digital Addiction: Panel Presented at OZCHI 2019 (Paay e Rogers, 2019);	2019
A80	The dark side of user participation-the effect of calls to action on trust and information revelation (Ilany Tzur et al., 2016);	2016
A81	The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure (Landwehr et al., 2019);	2019
A82	The Shape of Social Media: Towards Addressing (Aesthetic) Design Power (Kender e Frauenberger, 2022);	2022
A83	The TL;DR Charter: Speculatively Demystifying Privacy Policy Documents and Terms Agreements (Kotut e McCrickard, 2022);	2022
A84	This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices (Bermejo Fernández e et al., 2021);	2021
A85	Towards the Identification of Dark Patterns: An Analysis Based on End-User Reactions (Bhoot et al., 2020);	2020
A86	Towards Understanding the Dark Patterns That Steal Our Attention (Monge Roffarello e et al., 2022);	2022
A87	Trauma-informed computing: Towards safer technology experiences for all (Chen e et al., 2022);	2022
A88	UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception (Di Geronimo e et al., 2020);	2020
A89	User oppression in human-computer interaction: a dialectical-existential perspective (Gonzatto e van Amstel, 2022);	2022
A90	What Can CHI Do About Dark Patterns? (Lukoff e et al., 2021b);	2021

ID	Título	Ano
A91	What Kind of Work Do "Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit (Gray et al., 2020);	2020
A92	What Makes a “Bad” Ad? User Perceptions of Problematic Online Advertising (Zeng et al., 2021);	2021
A93	What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods (Mathur et al., 2021);	2021
A94	When Gamification Spoils Your Learning: A Qualitative Case Study of Gamification Misuse in a Language-Learning App (Hadi Mogavi e et al., 2022);	2022
A95	When Persuasive Technology Gets Dark? (Nyström e Stibe, 2020);	2020
A96	When the Good Turns Ugly: Speculating Next Steps for Digital Wellbeing Tools (Widdicks, 2020);	2020
A97	Zombie contracts, dark patterns of design, and ‘documentisation’ (Cornelius, 2019);	2019

APÊNDICE B – VEÍCULOS DE PUBLICAÇÃO E QUANTIDADES DE VEZES QUE APARECERAM

Evento	ACM Asia Conference on Computer and Communications Security	1
Journal	ACM Communications	3
Journal	ACM Computing Surveys	1
Evento	ACM Conference on Hypertext and Social Media	1
Evento	ACM Conference on Learning @ Scale	1
Evento	ACM Designing Interactive Systems Conference	6
Journal	ACM Human-Computer Interaction	9
Evento	ACM International Conference on Interaction Design and Children	1
Evento	ACM International Symposium on Pervasive Displays	1
Evento	ACM SIGSAC Conference on Computer and Communications Security	1
Evento	ACM Web Conference	1
Evento	ACM Web Science Conference	1
Evento	ACM/IEEE International Conference on Human-Robot Interaction	1
Journal	Aslib Journal of Information Management	1
Evento	Australian Conference on Human-Computer-Interaction	1
Evento	Brazilian Symposium on Human Factors in Computing Systems	1
Evento	CEUR Workshop Proceedings	1
Evento	CHI Conference on Human Factors in Computing Systems	34
Journal	Computers in Human Behavior	1
Evento	Conference on Designing interactive systems	1
Journal	Electronic Markets	1
Evento	European Symposium on Usable Security 2021	1
Journal	GetMobile: Mobile Comp. and Comm.	1
Journal	Human Technology	1
Journal	IEEE Security & Privacy	1
Journal	IEEE Technology and Society Magazine	1
Evento	IFIP Advances in Information and Communication Technology	1
Evento	Indian Conference on Human-Computer Interaction	1
Journal	Information Society	1
Evento	International Conference on Advanced Visual Interfaces	1
Evento	International Conference on Information Systems	1
Evento	International Conference on Intelligent User Interfaces	1
Evento	International Conference on Persuasive Technology	1
Evento	International conference on World wide web	1
Journal	International Journal of Design	1
Evento	International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers	1
Evento	International Workshop on Software Fairness	1
Journal	Internet Policy Review	1
Journal	Journal of Location Based Services	1
Evento	Lecture Notes in Business Information Processing	1

Evento	ACM Asia Conference on Computer and Communications Security	1
Evento	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	1
Evento	Lecture Notes in Networks and Systems	1
Evento	New Security Paradigms Workshop	1
Evento	Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society	3
Evento	Workshop on Computing within Limits	1
Evento	Workshop on Privacy in the Electronic Society	2

APÊNDICE C – LISTA DE DECEPTIVE PATTERNS SEPARADOS POR CATEGORIA

Categorias	Tipos	Descrição	Trabalhos
Ação Forçada	<i>Forced Action.</i>	Qualquer situação em que os usuários são obrigados a realizar uma ação específica para acessar (ou continuar acessando) uma funcionalidade específica.	Gray et al. ;
Ação Forçada	<i>Forced Enrollment.</i>	Coagir os usuários a criar contas ou compartilhar suas informações para concluir suas tarefas;	Mathur et al. ;
Ação Forçada	<i>Making personal information public;</i>	À medida que a pessoa entra em uma determinada área, o sistema torna as informações pessoais dessa pessoa publicamente visíveis.	Greenberg et al. ;
Ação Forçada	<i>We never forget;</i>	Os sistemas podem marcar qualquer interação proxêmica como indicando um relacionamento permanente, persistente (e indesejável) que nunca é esquecido.	Greenberg et al. ;
Ação Forçada	<i>The milk factor.</i>	O sistema proxêmico obriga você a se deslocar ou ir a um local específico para obter um serviço.	Greenberg et al. ;
Ação Forçada	<i>Coercion;</i>	Ameaçar ou obrigar a conformidade do usuário.	Conti & Sobieski ;
Ação Forçada	<i>Forced Work;</i>	Aumentar deliberadamente o trabalho para o usuário.	Conti & Sobieski;
Ação Forçada	<i>Gamification;</i>	A gamificação descreve situações em que certos aspectos de um serviço só podem ser "ganhos" por meio do uso repetido (e talvez indesejado) de aspectos do serviço.	Gray et al.; Di Geronimo et al.; Nyström; Mogavi et al.;
Ação Forçada	<i>Forced registration process</i>	Forçar um indivíduo a fornecer mais informações pessoais ou a se inscrever em uma conta apenas para exercer seus direitos.	Bösch et al.; Norval et al.
Ação Forçada	<i>Auto-play</i>	Quando novos conteúdos como vídeos ou histórias são reproduzidos de forma sequencial e automática sem a necessidade de interação de nenhum usuário.	Alter; Lukoff et al.; Roffarello & De Russis; Chaudhary et al.;
Ação Forçada	<i>Forced consent</i>	Coagir os usuários a aceitar termos legais fixos em troca de acesso ao serviço.	Chatellier et al.;
Ação Forçada	<i>No bulk options for settings;</i>	Forçar as pessoas a usar exclusivamente controles granulares, o que leva tempo, aumenta o custo do esforço de fazer alterações e, portanto, pode desencorajar as pessoas a alterar os padrões que são benéficos para o serviço.	Gunawan et al.;
Interferência na interface	<i>Interface Interference</i>	Qualquer manipulação da interface do usuário que privilegie ações específicas sobre outras, confundindo o usuário ou limitando a descoberta de possibilidades de ação importantes (affordances falsas ou ocultas). A interferência de interface se manifesta como inúmeras decepções visuais e interativas individuais.	Gray et al.;
Interferência na interface	<i>Hidden Information</i>	Defini-se informações ocultas como opções ou ações relevantes para o usuário, mas não imediatamente ou prontamente acessíveis. Informações ocultas podem se manifestar como opções ou conteúdo oculto em letras pequenas, texto descolorido ou declaração de termos e condições de um produto. O principal motivador por trás das informações ocultas é o disfarce de informações relevantes como irrelevantes. Quando um usuário se registra em uma conta, ele tem a opção de aceitar os termos e condições acima de uma longa lista de pequenos textos. Escondido dentro deste texto está uma pequena caixa de seleção para recusar que o site venda as informações do usuário.	Gray et al.;
Interferência na interface	<i>Aesthetic Manipulation,</i>	Manipulação estética é qualquer manipulação da interface do usuário que lida mais diretamente com a forma do que com a função. Isso inclui escolhas de design que focam a atenção do usuário em uma coisa para distraí-lo ou convencê-lo de outra coisa.	Gray et al.;

Categorias	Tipos	Descrição	Trabalhos
Interferência na interface	<i>False Hierarchy</i>	A hierarquia falsa dá a uma ou mais opções a precedência visual ou interativa sobre outras, especialmente quando os itens devem estar em paralelo em vez de hierárquicos. Isso convence o usuário a fazer uma seleção que ele sente ser a única opção ou a melhor opção. Ao instalar os utilitários do aplicativo, o usuário pode decidir entre a instalação "expressa", rotulada como "recomendada", ou a instalação "personalizada", rotulada como "avançada". A opção "personalizada" está em texto cinza, mas ainda é clicável, dando ao usuário a falsa impressão de que a opção está desabilitada.	Gray et al.;
Interferência na interface	<i>Preselection,</i>	Entende-se pré-seleção como qualquer situação em que uma opção é selecionada por padrão antes da interação do usuário. A pré-seleção geralmente se manifesta como uma escolha padrão que o acionista do produto deseja que o usuário escolha; no entanto, essa escolha geralmente é contrária aos interesses do usuário ou pode trazer consequências não intencionais. É mais provável que o usuário concorde com a opção padrão se acreditar que o produto tem seus melhores interesses em mente.	Gray et al.;
Interferência na interface	<i>Widget inequality;</i>	A opção de negação de consentimento tem um formato diferente da aceitação.	Soe et al. [67];
Interferência na interface	<i>Unlabeled sliders;</i>	Os avisos de consentimento usam controles deslizantes, mas não é rotulado qual lado do controle é aceito/ligado ou rejeitado/desligado.	Soe et al.;
Interferência na interface	<i>Countdown Timer;</i>	Indicando aos usuários que uma oferta ou desconto irá expirar usando um cronômetro de contagem regressiva;	Mathur et al.;
Interferência na interface	<i>Limited-time Message;</i>	Indicar aos usuários que um negócio ou venda irá expirar em breve sem especificar um prazo;	Mathur et al.;
Interferência na interface	<i>Visual Interference;</i>	Usar estilo e apresentação visual para direcionar escolhas dos usuários;	Mathur et al.;
Interferência na interface	<i>Low-stock Message;</i>	Indicar aos usuários que há quantidades limitadas de um produto;	Mathur et al.;
Interferência na interface	<i>High-demand Message;</i>	Indicar aos usuários que um produto está em alta demanda e provavelmente esgotará em breve;	Mathur et al.;
Interferência na interface	<i>Manipulating Navigation;</i>	Criar arquiteturas de informação e mecanismos de navegação que orientem o usuário na realização das tarefas do designer de interface.	Conti & Sobieski;
Interferência na interface	<i>Disguised Ads;</i>	Anúncios que aparecem projetados para não parecer anúncios que desafiam deliberadamente as habilidades de alfabetização em publicidade.	Fitton & Read [45]; Brignull; Zeng et al; Mhadali & Schaub;
Interferência na interface	<i>Calls to action"</i>	As chamadas para ação podem levar os usuários a inferir que o site é confiável e decidir revelar suas informações pessoais.	Ilany-Tzur et al.;
Interferência na interface	<i>Attention quicksand</i>	Chamam a atenção do usuário e os desviam do que poderia ser um comportamento online diferente.	Chaudhary et al.; Roffarello & De Russis;
Interferência na interface	<i>Pull-to-refresh</i>	Usuários podem "puxar" uma interface, por exemplo, deslizando para baixo em um aplicativo móvel, para recarregar manualmente o status do sistema e ver se há novo conteúdo, por exemplo, a postagem de um novo amigo no feed de notícias do Facebook.	Roffarello & De Russis;
Interferência na interface	<i>Infinite scrolling</i>	Rolar passivamente e sem pensar o feed de notícias de uma rede social é um aspecto do uso da tecnologia que influencia negativamente o bem-estar digital dos usuários [20, 33].	Roffarello & De Russis; Chaudhary et al.;
Interferência na interface	<i>Too Many Ads</i>	Muitos ads no aplicativo, em toda parte.	Singh et al. [117];
Interferência na interface	<i>Progress Manipulation</i>	Se o usuário tiver que fazer o download do aplicativo novamente, a pontuação acumulada pelo usuário é perdida.	Singh et al.;

Categorias	Tipos	Descrição	Trabalhos
Desorientação	<i>Toying with Emotion;</i>	Brincar com a emoção inclui qualquer uso de linguagem, estilo, cor ou outros elementos semelhantes para evocar uma emoção a fim de persuadir o usuário a uma ação específica. Isso pode se manifestar como imagens fofas ou assustadoras, ou como linguagem atraente ou assustadora. Em um site de compras, ao finalizar a compra, é mostrado ao usuário um cronômetro de contagem regressiva que supostamente garante a entrega em 2-4 semanas se o usuário comprar o produto dentro da janela de tempo; no entanto, se o usuário deixar o cronômetro chegar a 0, o cronômetro será reiniciado. Em outro exemplo o site solicita que o usuário se inscreva em um boletim informativo. A opção para recusar é a frase humilhante: "Não, obrigado, vou jantar no microondas hoje à noite", usando um texto que evoque emoção e talvez incentive o usuário a alterar a ação pretendida.	Gray et al.;
Desorientação	<i>No antonyms;</i>	O uso de palavras claras como "concordo", "consentimento", "sim" para rotular a opção de consentimento e não usar seus antônimos para rotular a opção de negação de consentimento.	Soe et al.;
Desorientação	<i>Confirmshaming;</i>	Usar a linguagem e a emoção (vergonha) para afastar os usuários de uma determinada escolha;	Mathur et al.; Brignull; Habib et al.;
Desorientação	<i>Trick Questions;</i>	Usar uma linguagem confusa;	Mathur et al.; Brignull;
Desorientação	<i>Pressured Selling;</i>	Pré-selecionar variações mais caras de um produto, ou pressionar o usuário a aceitar as variações mais caras de um produto e produtos relacionados;	Mathur et al.;
Desorientação	<i>The attention grabber;</i>	O sistema toma uma ação deliberada para atrair e manter a atenção dessa pessoa.	Greenberg et al.;
Desorientação	<i>Bait and Switch;</i>	O sistema atrai o espectador com algo desejável, mas o muda para outra coisa depois que a pessoa se aproxima. O padrão Bait and Switch torna aparente que uma determinada ação causará um determinado resultado, apenas para causar um resultado diferente e provavelmente indesejado.	Greenberg et al.; Brignull; Gunawan et al.;
Desorientação	<i>Confusion;</i>	Fazer perguntas ao usuário ou fornecer informações que ele não entenda.	Conti & Sobieski;
Desorientação	<i>Distraction;</i>	Atrair a atenção do usuário para longe de sua tarefa atual..	Conti & Sobieski;
Desorientação	<i>Exploiting Errors;</i>	Aproveitar os erros do usuário para facilitar os objetivos do designer de interface.	Conti & Sobieski;
Desorientação	<i>Shock;</i>	Apresentar conteúdo perturbador ao usuário.	Conti & Sobieski;
Desorientação	<i>Trick;</i>	Enganar o usuário ou outras tentativas de engano.	Conti & Sobieski;
Desorientação	<i>Cuteness;</i>	A ênfase em ganhos de curto prazo, o encorajamento da "miopia de dados" no usuário e seu papel na produção de uma ilusão de soberania do usuário sobre o robô.	Lacey & Caudwell;
Desorientação	<i>Inappropriate;</i>	Aspectos de um aplicativo inadequados para a faixa etária do usuário.	Fitton & Read;
Desorientação	<i>Privacy Zuckering</i>	As configurações de privacidade são desnecessariamente complicadas, excessivamente granulares ou incompreensíveis para o usuário. O usuário acaba desistindo ou faz alterações não intencionais em suas configurações de privacidade.	Bösch et al.; Brignull; Mildner & Savino;
Desorientação	<i>Hidden Legalese Stipulations</i>	Os termos e condições são obrigatórios por lei. No entanto, a maioria dos usuários não os lê, pois geralmente são longos e escritos em um jargão jurídico complicado. Este jargão jurídico é necessário para fornecer concisão e clareza, mas não é fácil de usar.	Bösch et al.;
Desorientação	<i>Unequal paths</i>	A interface tinha caminhos de interação desiguais para as opções de maior e menor proteção à privacidade.	Habib et al.;
Desorientação	<i>Confusing buttons</i>	A interface tem um posicionamento não intuitivo de botões para confirmar as preferências de cookies dos usuários e permitir todos os cookies.	Habib et al.;
Desorientação	<i>Disruptions of agency;</i>	Monitoramento em tempo real da fisiologia emocional, em última análise, interrompendo a privacidade ou mesmo a agência do indivíduo sob o pretexto de aumentar a empatia e a transparência.	Dickinson et al.;

Categorias	Tipos	Descrição	Trabalhos
Desorientação	<i>Extraneous notification badges</i>	Direcionam a atenção das pessoas para elementos de interface que não requerem atenção imediata, especialmente se o resultado final da interação com o elemento de interface do usuário com emblema for um conteúdo que beneficie o serviço.	Gunawan et al.;
Desorientação	<i>Inboxes/message centers</i>	Considera-se um centro de mensagens desnecessário se, em nossa observação, ele contiver principalmente anúncios de spam do provedor de serviços, especialmente se o serviço em questão não foi projetado especificamente para mensagens.	Gunawan et al.;
Desorientação	<i>Only Initial Payouts</i>	Funciona por uma semana, e então passa a demorar e não funcionar como de início.	Singh et al.;
Desorientação	<i>Permission Override</i>	Ao dar permissão a um aplicativo, ele toma controle de outros aplicativos e reduz o desempenho geral do celular.	Singh et al.;
Desorientação	<i>Sponsored recommendation</i>	Recomendações patrocinadas estavam sendo usadas para atrair sistematicamente os clientes cada vez mais para produtos de Marca Própria (marca do site de compras) nas categorias examinadas.	Das et al.;
Desorientação	<i>Disparity in “buybox”;</i>	O algoritmo buybox pode ser usado para evitar a concorrência entre vendedores e direcionar os usuários para os vendedores que têm um relacionamento especial com o site de compras.	Das et al.;
Monetário	<i>Intermediate Currency;</i>	A moeda intermediária é outro subtipo de obstrução em que os usuários gastam dinheiro real para comprar uma moeda virtual que é gasta em um bem ou serviço. O objetivo desse padrão é desconectar os usuários do valor real do dólar gasto para fazer com que o usuário interaja de maneira diferente com a moeda virtual. Isso pode fazer com que os usuários gastem a moeda de maneira diferente do que fariam com a moeda fiduciária. Esse padrão normalmente se manifesta como uma compra no aplicativo para jogos para dispositivos móveis.	Gray et al.;
Monetário	<i>Pay to Skip</i>	Em vez de incentivar um jogador a pagar mais para continuar, eles permitem que os jogadores paguem para progredir no jogo.	Zagal et al.; Fitton & Read;
Monetário	<i>Pre-Delivered Content</i>	É um padrão em que determinado conteúdo ou funcionalidade do jogo é fornecido na compra de um jogo (ou seja, os arquivos já estão no disco ou incluídos no executável baixado), mas fica indisponível até que o jogador pague uma taxa adicional.	Zagal et al.; Fitton & Read;
Monetário	<i>Monetized Rivalries</i>	É um padrão que explora a competitividade do jogador; incentivando-os a gastar dinheiro que não gastariam de outra forma para alcançar status no jogo, como uma colocação alta em uma tabela de classificação.	Zagal et al.; Fitton & Read;
Monetário	<i>Microtransactions</i>	Várias técnicas de design usadas para impulsionar a monetização são antiéticas, manipulam, coagem, enganam, exploram ou podem até prejudicar ativamente o bem-estar do jogador ao induzir gastos excessivos.	Petrovskaya et al.;
Monetário	<i>Withdrawal Limit</i>	O limite para saque dentro do aplicativo é alto demais, sendo quase impossível do usuário atingir o mínimo.	Singh et al.;
Monetário	<i>Cannot Redeem</i>	O aplicativo não deixa que o usuário faça o saque dos créditos.	Singh et al.;
Monetário	<i>Paid Offers</i>	O usuário faz um depósito esperando uma recompensa no aplicativo e não recebe nada.	Singh et al.;
Atraso	<i>Nagging;</i>	Um pequeno redirecionamento da funcionalidade esperada que pode persistir em uma ou mais interações.	Gray et al.;
Atraso	<i>No choice;</i>	Todos os links e botões incluídos levam a uma página que instrui para outras páginas que detalham os ajustes das configurações do navegador, direcionam o usuário para entrar em contato com serviços de terceiros ou apenas “explica” cookies e propósitos.	Soe et al.; Habib et al.;
Atraso	<i>Multiple choice panels;</i>	O consentimento do usuário é solicitado em diferentes painéis de avisos.	Soe et al.;
Atraso	<i>Choice cascade;</i>	A negação de consentimento só é alcançada seguindo uma série de links ou botões que oferecem mais informações.	Soe et al.;
Sem consentimento	<i>Does not count;</i>	O consentimento não foi dado (ainda ou foi negado), mas os dados são coletados mesmo assim.	Soe et al.;

Categorias	Tipos	Descrição	Trabalhos
Sem consentimento	<i>Sneak into Basket;</i>	O padrão Sneak into Basket adiciona itens não escolhidos pelo usuário ao carrinho de compras on-line, muitas vezes alegando ser uma sugestão com base em outros itens comprados. Isso pode fazer com que o usuário compre involuntariamente esses itens se não os notar antes da finalização da compra.	Mathur et al.; Brignull;
Sem consentimento	<i>Disguised data collection;</i>	As informações coletadas para fornecer um determinado serviço são usadas para construir um perfil, sem o consentimento dos usuários.	Greenberg et al.;
Sem consentimento	<i>Unintended relationships;</i>	O sistema rastreia suas relações próximas com os outros e constrói uma rede social na suposição de que você está de alguma forma socialmente relacionado quando não há relacionamento.	Greenberg et al.;
Sem consentimento	<i>Institutional Malware;</i>	Espionagem e coleta de dados de usuários, funcionários e familiares;	Monahan;
Sem consentimento	<i>No consent checkbox is provided</i>	<i>Apresente um link para os Termos do Serviço, mas não ofereça uma caixa de seleção para consentir.</i>	Gunawan et al.;
Sem consentimento	<i>Privacy Violations</i>	Ao colocar seu número de celular no aplicativo, você passa a ser bombardeado por spam e mensagens, sem seu consentimento.	Singh et al.;
Obstrução	<i>Obstruction;</i>	Impedimento de um fluxo de tarefa, tornando a interação mais difícil do que ela inerentemente precisa ser com a intenção de dissuadir uma ação.	Gray et al.;
Obstrução	<i>Roach Motel</i>	Descreve uma situação que é fácil de entrar, mas difícil de sair. Isso geralmente ocorre quando um usuário se inscreve em um serviço facilmente, mas fechar uma conta ou cancelar o serviço é difícil ou impossível. Um padrão típico de interações exige que o usuário ligue para um número de telefone para cancelar sua conta, onde será ainda mais pressionado a manter sua conta. Os sites também ocultam essas informações na seção de perguntas frequentes para dificultar o cancelamento do serviço. Este exemplo indica com o Roach Motel pode invocar outros tipos de padrões escuros, neste caso, informações ocultas, para servir ao seu propósito.	Gray et al.; Gunawan et al.;
Obstrução	<i>Price Comparison Prevention</i>	O padrão de Prevenção de Comparação de Preços procura atenuar o efeito da competição de mercado, dificultando as comparações diretas de preços entre produtos e serviços. As táticas podem incluir tornar as informações importantes do produto (ID do produto, preço) não copiáveis, para evitar que os usuários colem essas informações em uma barra de pesquisa ou em outro site.	Brignull;
Obstrução	<i>Hard to Cancel;</i>	Facilitar o cadastro do usuário em um serviço, mas dificultar o cancelamento;	Mathur et al.;
Obstrução	<i>Interruption;</i>	Interromper o fluxo de tarefas do usuário.	Conti & Sobieski;
Obstrução	<i>Restricting Functionality;</i>	Limitar ou omitir controles que facilitem a realização das tarefas do usuário.	Conti & Sobieski;
Obstrução	<i>Service denial;</i>	Usuários com altos padrões de preservação de privacidade são frequentemente vistos como “não rentáveis” e com serviço negado.	Westin & Chiasson;
Obstrução	<i>Immortal Accounts</i>	O provedor de serviços exige que novos usuários se inscrevam em contas para usar o serviço. Depois que os usuários decidirem parar de usar o serviço, eles podem querer excluir suas contas e dados associados. No entanto, o provedor de serviços impede que o usuário faça isso – complicando desnecessariamente a experiência de exclusão de conta ou não fornecendo nenhuma opção de exclusão de conta. Além disso, o provedor de serviços pode enganar o usuário no processo de exclusão fingindo excluir a conta inteira, enquanto ainda retém (alguns) dados da conta.	Bösch et al.;

Categorias	Tipos	Descrição	Trabalhos
Obstrução	<i>Consent Wall</i>	Uma parede de consentimento é uma escolha de design que bloqueia o acesso ao site até que o usuário expresse sua escolha em relação ao consentimento. Esta escolha de design permite que um usuário selecione entre aceitação e recusa; no entanto, o uso concreto do site é bloqueado até que uma escolha seja feita.	Gray et al.;
Obstrução	<i>Reduced Service</i>	O uso de serviço reduzido refere-se à prática de um site que oferece funcionalidade reduzida—por exemplo, permitir que um usuário acesse apenas um número limitado de páginas em um site—com base em suas opções de configuração de consentimento.	Gray et al.;
Obstrução	<i>Hidden log out</i>	Promovem estratégias de ocultação de recursos restritivos de uso na interface do usuário padrão.	Chaudhary et al.;
Obstrução	<i>No notification settings;</i>	Serviços que não oferecem opções para controlar as notificações.	Gunawan et al.;
Obstrução	<i>No privacy settings</i>	Serviços que não oferecem opções para controlar a coleta de dados privados.	Gunawan et al.;
Obstrução	<i>Unclear deactivation/deletion options</i>	Serviço comunica insuficientemente o que acontecerá se uma pessoa desativar ou excluir sua conta.	Gunawan et al.;
Escondendo	<i>Sneaking</i>	Tentativa de ocultar, disfarçar ou retardar a divulgação de informações relevantes para o usuário. Sneaking geralmente ocorre para fazer o usuário realizar uma ação à qual ele pode se opor se tiver conhecimento disso. Comportamentos furtivos podem incluir custos adicionais não divulgados ou efeitos indesejados de uma ação específica.	Gray et al.;
Escondendo	<i>Unmarked X;</i>	Quando o painel tem um botão “x” no canto superior direito e não explica se clicar neste “x” conta como consentimento ou não.	Soe et al.;
Escondendo	<i>Hidden Costs;</i>	Revelar cobranças previamente não divulgadas aos usuários logo antes de entregarem uma compra; O padrão de custos ocultos fornece aos usuários uma divulgação tardia de determinados custos. Nesse padrão, um determinado preço é anunciado para um bem ou serviço, apenas para ser alterado posteriormente devido à adição de impostos e taxas, condições de tempo limitadas ou custos de envio excepcionalmente altos.	Mathur et al.; Brignull; Gunawan et al.; Singh et al.;
Escondendo	<i>Hidden Subscription;</i>	Cobrar aos usuários uma taxa recorrente sob o pretexto de uma taxa única ou de um teste gratuito;	Mathur et al.; Di Geronimo et al.; Brignull; Gunawan et al.;
Escondendo	<i>The captive audience;</i>	O sistema detecta a pessoa no local e inicia uma ação não solicitada (e potencialmente indesejada).	Greenberg et al.;
Escondendo	<i>Obfuscation;</i>	Ocultar informações e elementos de interface desejados.	Conti & Sobieski;
Escondendo	<i>Sneaky Ads;</i>	Propagandas que são na verdade tentativas de engano.	Fitton & Read; Zeng et al; Mhaidli & Schaub;
Escondendo	<i>Placebo buttons;</i>	Botões que dão uma falsa sensação de controle ao usuário;	Monahan;
Escondendo	<i>Decoys in the data hunt;</i>	Características arquitetônicas “disfarçadas” em áreas públicas que possam coletar dados de transeuntes;	Monahan;
Escondendo	<i>Bad Defaults</i>	Ao criar uma conta, as opções padrão às vezes são mal escolhidas no sentido de facilitar ou incentivar o compartilhamento de informações pessoais. Assim, muitas vezes sem saber, os usuários compartilham mais informações pessoais do que pretendem.	Bösch et al.; Habib et al.;
Escondendo	<i>Address Book Leeching;</i>	Quando o usuário importa a lista, o serviço executa uma pesquisa em seu próprio banco de dados. Em seguida, ele fornece sugestões de conexões para o usuário. No entanto, o provedor de serviços armazena a lista de todos os contatos como registros de dados internos para processamento posterior, incluindo propósitos que não foram declarados inicialmente.	Bösch et al.;
Escondendo	<i>Loss-gain framing</i>	Uma divulgação seletiva de informações que enquadra positivamente as consequências de uma ação, omitindo os riscos envolvidos.	Boush et al.;
Escondendo	<i>Bundled consent</i>	Obtendo consentimento para várias configurações por meio de uma única ação.	Bongard-Blanchy et al.; Santos et al.;
Escondendo	<i>Feature fog</i>	Induz o desconhecimento reduzindo a autonomia de monitoramento do tempo gasto pelo usuário.	Chaudhary et al.;

Categorias	Tipos	Descrição	Trabalhos
Escondendo	<i>ToS not mentioned during registration</i>	Deixar de mencionar a existência dos Termos do Serviço.	Gunawan et al.;
Pressão social	<i>Social Pyramid,</i>	O Social Pyramid exige que os usuários recrutem outros usuários para usar o serviço. Este é um método comumente usado em aplicativos de mídia social e jogos online. Os usuários podem convidar seus amigos para usar o serviço e são incentivados com os benefícios da plataforma. Por exemplo, um jogo incentiva os usuários a convidar seus amigos para jogar, tornando alguns recursos ou objetivos inacessíveis caso não hajam amizades online no jogo.	Gray et al.;
Pressão social	<i>Activity Message;</i>	Informar o usuário sobre atividades no site (por exemplo, compras, visualizações, visitas);	Mathur et al.;
Pressão social	<i>Testimonials;</i>	Depoimentos suspeitos;	Mathur et al.;
Pressão social	<i>Social;</i>	Compartilhamento de forma que coloque em risco a privacidade e compartilhamento de forma que possa prejudicar a reputação do usuário.	Fitton & Read;
Pressão social	<i>Short-term benefits;</i>	Por pressão social s usuários acabam escolhendo benefícios de curto prazo em vez de benefícios de privacidade de longo prazo.	Westin & Chiasson;
Pressão social	<i>Social isolation avoided;</i>	Os usuários continuarão a escolher uma opção que os deixe desconfortáveis se a alternativa parecer mais isolante socialmente.	Westin & Chiasson;
Pressão social	<i>Community norms;</i>	Os usuários são motivados a se comportar de acordo com as normas da comunidade.	Westin & Chiasson;
Pressão social	<i>Social capital;</i>	O gerenciamento de impressões e o ganho de capital social são os principais motivos para usar as mídias sociais.	Westin & Chiasson;
Pressão social	<i>Attention-economic logic;</i>	Os serviços dependem dos usuários para “reproduzir” sua lógica de economia da atenção. Quando um serviço é grátis, o usuário paga com tempo, atenção e dados pessoais.	Westin & Chiasson;
Pressão social	<i>Infrastructure informs community;</i>	As normas comunitárias surgem da infraestrutura digital das tecnologias. A estrutura fornecida para uma comunidade informa suas expectativas.	Westin & Chiasson;
Pressão social	<i>Incentivize impulse buying;</i>	As características comuns incluem aquelas que: (a) reduzem o risco percebido de transações on-line, (b) alavancam a influência social, (c) aumentam a proximidade percebida com o produto e (d) aumentam a proximidade temporal percebida com o produto.	Moser et al.;
Pressão social	<i>Shadow User Profiles;</i>	Embora os usuários registrados tenham optado deliberadamente por uma conta de usuário e um perfil associado, o provedor de serviços pode coletar informações e manter registros sobre indivíduos que não usam o serviço. Por exemplo, em uma rede social, o gráfico social pode ser complementado com pessoas que não são membros da rede, mas são conhecidas da rede com base nos dados dos membros (por exemplo, catálogos de endereços importados, metadados de conteúdo ou menções). Esses não membros enriquecem o gráfico e melhoram a qualidade dos algoritmos, como sugestões de contato.	Bösch et al.;
Pressão social	<i>Social Pyramid Schemes;</i>	Muitos jogos incentivam os jogadores a convidar seus amigos para participar. Nem todos eles, no entanto, fornecem benefícios tangíveis no jogo para isso, nem exigem implicitamente que os jogadores façam uso de suas conexões sociais para progredir adequadamente em um jogo.	Zagal et al.;
Pressão social	<i>Impersonation</i>	Quando o jogo se faz passar por outros jogadores, comunicando ações que eles nunca realizaram, enganando assim o jogador sobre as atividades de seus amigos no jogo.	Zagal et al.;
Pressão social	<i>Social Investment</i>	Métricas sociais como número de reações, comentários, seguidores e visualizações podem “vincular” usuários à plataforma subjacente. Tal mecanismo influencia os usuários incutindo a ideia de que eles devem continuar usando a plataforma para não perder os progressos alcançados.	Roffarello & De Russis;
Capitalismo de vigilância	<i>Surveillance capitalism;</i>	Esse modelo de negócios envolve publicidade personalizada e manipulação de comportamento, impulsionada pela coleta intensiva e correlação cruzada de informações pessoais.	Landwehr et al.;

Categorias	Tipos	Descrição	Trabalhos
Capitalismo de vigilância	<i>Reductionism of human emotion;</i>	As máquinas recuperam cada vez mais dados sobre o estado afetivo de seu usuário em tempo real, até mesmo informando como se sentiram ou quão ‘bem’ estão. Normalmente, os dados são reduzidos a um conjunto de representações numéricas.	Dickinson et al.;
Capitalismo de vigilância	<i>Parasitic symbiosis;</i>	Uma forma de simbiose na qual a emoção humana é objetificada para sustentar o sistema cibernético do capitalismo de vigilância à medida que o sujeito é objetificado, digitalizado, rastreado e guiado por meio de “jornadas do usuário” dirigidas por algoritmos.	Dickinson et al.;
Temporal	<i>Temporal;</i>	Desperdício de tempo para o usuário e tentativas de testar a paciência de um usuário.	Fitton & Read [45];
Temporal	<i>Grinding</i>	É uma maneira de coagir o jogador a gastar tempo desnecessariamente em um jogo com o único propósito de estender a duração do jogo: “matar repetidamente os mesmos inimigos usando a mesma estratégia apenas para ganhar um nível de experiência e acesso a novos recursos”	Zagal et al.;
Temporal	<i>Playing by Appointment;</i>	Jogos com esse padrão sombrio exigem que os jogadores joguem em horários específicos (e/ou datas) conforme definido pelo jogo, em vez dos jogadores.	Zagal et al.; Fitton & Read;

APÊNDICE D – TEORIAS E CONCEITOS QUE APARECERAM NOS ARTIGOS

ID	Teorias/Conceitos
A29	<i>Interaction Criticism</i> (Bardzell, 2011): por Jeffrey Bardzell, prática que permite que profissionais de design se envolvam mais com a estética da interação, ajudando-os a desenvolver ideias críticas mais sensíveis a projetos.
A42	Manipulativeness (Ackerman, 1995): de um ponto de vista filosófico, de acordo com Felicia Ackerman, para um ato ser considerado manipulador, ele deve primeiro “fazer alguém ir contra o que ele considera natural ou apropriado ou está inclinado a fazer”.
A72,A73, A81	Surveillance Capitalism (Zuboff, 2019): termo popularizado por Shoshana Zuboff, é um conceito da economia política que denota a ampla coleta e comercialização de dados pessoais por empresas privadas.
A3,A27,A85	Dual Process Theory (Kahneman, 2003) : proposta por Daniel Kahneman, traz uma explicação de como o pensamento pode surgir de duas maneiras diferentes, padrões de pensamento conscientes (controlados, atentos) ou inconscientes (automáticos, irracionais).
A68	Prospect Theory (Kai-Ineman e Tversky, 1979): criada por Daniel Kahneman e Amos Tversky em 1979, é um modelo comportamental de como as pessoas tomam decisões na presença de risco.
A71	Regret Theory (Loomes e Sugden, 1982): o arrependimento é um sentimento contrafactual baseado em uma inferência contrafactual de que “o passado poderia ter se desenrolado de forma diferente, particularmente se uma decisão diferente tivesse sido tomada”.
A82	Aesthetic Design Power (Kender e Frauenberger, 2022): a influência intencional e não intencional que a forma de um artefato projetado tem, consciente e inconscientemente, sobre os usuários, para se comportar de uma certa maneira em suas interações com o artefato e além. Não é “bom” nem “mau” por natureza e, apesar de estar nas mãos dos criadores, também é negociado, contra-agido e manejado pelos usuários.

ID	Teorias/Conceitos
A2,A7,A10,A14, A27,A31,A37, A45,A55,A74, A76,A91	Value Sensitive Design (Friedman et al., 2008; Friedman e Hendry, 2019): desenvolvido por Batya Friedman e Peter Kahn, é uma abordagem teoricamente fundamentada para o projeto de tecnologia que considera os valores humanos de uma maneira compreensiva e abrangente.
A65	Captology (Fogg, 1998): Termo criado por B.J. Fogg, é o estudo de computadores como tecnologias persuasivas capazes contribuir de forma positiva com a vida das pessoas, mas que também podem ser utilizados para o mal como manipulação, coerção e alteração de comportamentos.
A80	Self-perception theory (Bem, 1967): proposta por Daryl Bem, a teoria da autopercepção afirma que as pessoas desenvolvem suas atitudes (quando não houve atitude prévia por falta de experiência, e a resposta emocional é ambígua) observando seu próprio comportamento e concluindo quais atitudes devem tê-lo causado.
A89	Userism (Gonzatto e Van Amstel, 2017): conceito que explica como as pessoas são reduzidas apenas ao papel de usuários, negando as possibilidades de grupos sociais historicamente oprimidos de usar e produzir tecnologias para projetar seus meios de existência e desenvolver novas condições de ser humano.

ID	Teorias/Conceitos
A30	Viéses cognitivos: Anchoring Effect (Tversky e Kahneman, 1974): A tendência dos indivíduos de confiar excessivamente em uma informação inicial – a ‘âncora’ – em decisões futuras. Bandwagon Effect (Sherif, 1936): A tendência dos indivíduos de valorizar algo mais porque os outros parecem valorizá-lo. Default Effect (Johnson et al., 2002): A tendência dos indivíduos de se aterem às opções que lhes são atribuídas por padrão devido à inércia. Framing Effect (Tversky e Kahneman, 1981): A tendência dos indivíduos de chegar a decisões diferentes a partir da mesma informação, dependendo de como ela é apresentada. Scarcity Bias (Mittone e Savadori, 2009): A tendência dos indivíduos de valorizar mais as coisas que são escassas. Sunk Cost Fallacy (Arkes e Ayton, 1999): A tendência dos indivíduos de continuar uma ação se eles investiram recursos nela, mesmo que essa ação possa piorá-los.
A22	Social Welfare Computing (Clemons e et al., 2022): como uma disciplina que busca possibilitar as contribuições das grandes empresas de tecnologia, minimizando os danos à sociedade.
A57	Human-Computer Integration (Farooq e Grudin, 2016): conceito que explica como humanos e computadores estão se movendo cada vez mais em direção a uma trajetória na qual os dois inevitavelmente se fundirão em um organismo simbiótico.
A32	Proxemic interactions (Greenberg e et al., 2014): as interações proxêmicas (em proximidade física) ocorrem com dispositivos com conhecimento refinado de pessoas próximas e outros dispositivos (como sua posição, identidade, movimento, orientação, etc) e como esse conhecimento pode ser explorado para projetar técnicas de interação.

ID	Teorias/Conceitos
A64,A56	FoMO - Fear of Missing Out (Przybylski e et al., 2013): o “medo de ficar de fora” ou “medo de perder algo” é um conceito da psicologia que descreve um comportamento, identificado em usuários de redes sociais, de medo de não conseguir acompanhar as atualizações e eventos, compelindo o usuário a manter-se conectado às redes sociais.
A94	Rational Choice Theory (RCT) (Lovett, 2006): afirma que os indivíduos usam seus próprios interesses para fazer escolhas que lhes proporcionem o maior benefício. As pessoas avaliam suas opções e fazem a escolha que acham que será melhor para elas.
A18	Illusion of control (Langer, 1975): é a tendência de as pessoas superestimarem sua capacidade de controlar eventos.

APÊNDICE E – EXPERIMENTOS E ESTUDOS ENCONTRADOS NOS ARTIGOS

ID	Quem	Qtd	O quê foi avaliado	Como	Onde (contexto)
A45	<i>designers profissionais</i>	3	princípios éticos e valores	estudo observacional entrevistas	indústria
A14	<i>estudantes de design</i>	24	intenções éticas e valores no processo de criação	sessões de design estudo observacional thinking aloud	design de interfaces
A69	<i>estudantes de design</i>	33	explora, avalia e reflete sobre o processo de design de interfaces de usuário no contexto dos avisos de consentimento do General Data Protection Regulation.	sessões de design audio e video	aviso de consentimento
A58	<i>usuários</i>	27 61 47	sua própria frustração grau de frustração tolerável e de frustração esperada a facilidade de uso e eficácia	questionário escala Likert	universitário /conferencia hacker
A13	<i>usuários</i>	24	uso do software, especialmente sobre suas preocupações com o rastreamento de localização	questionário online entrevista	sistema de transferência de conteúdo
A25	<i>usuários</i>	39	aborrecimentos e interrupções como os usuários lidavam com esses aborrecimentos ou interrupções	em pares dinâmica usando cartolina e post-its, respondendo um questionário	aplicativos e jogos móveis gratuitos
A27	<i>usuários</i>	9	percebe, experimenta e responde a padrões obscuros	grupos focais perguntas exploratórias entrevistas individuais semi estruturadas	internet
A55	<i>consumidores</i>	151	entender ferramentas para ajudar no autocontrole compras online	questionário online	compras online
A85	<i>usuários</i>	310	susceptibilidade dos usuários aos diferentes tipos de padrões obscuros	questionário	internet, aplicativos moveis
A88	<i>usuários</i>	589	falta de consciência dos usuários para o design malicioso	questionário online	internet
A31	<i>usuários</i>	204	nível percebido de aborrecimento, confiança expressa na marca e afinidade com a tecnologia	questionário usando escala Likert	internet
A38	<i>Pesquisadores e designers</i>	5	aplicativos, violações e feedback sobre quaisquer possíveis pontos cegos das diretrizes	feedback verbal	diretrizes de design para aplicativos de investimento
A40	<i>um pesquisador e um desenvolvedor</i>	2	revisaram os guias de início rápido e as informações vinculadas de quatro redes de propagandas	um passo a passo com dois revisores	redes de propagandas
A42	<i>usuários</i>	169	identificar a interação diária dos usuários com interfaces manipulativas, reações emocionais à manipulação e percepção sobre os criadores dessas manipulações tecnológicas.	questionário entrevistas	interfaces manipulativas
A46	<i>usuários</i>	116	motivação atual/passada para usar o Facebook e quais os recursos mais usados, satisfação com o tempo gasto no Facebook, e recursos específicos e atitudes dos participantes em relação às preocupações com a privacidade.	questionário perguntas abertas e com escala Likert	Facebook
A47	<i>usuários</i>	500	a confiança, antropomorfismo ou desenvolvimento de relacionamento com assistentes de voz.	questionário com escala Likert	assistentes por voz
A56	<i>usuários</i>	25	compreensão das situações em que os usuários comprometem relutantemente sua privacidade em relação ao Fear of Missing Out (Medo de perder).	entrevistas semi-estruturadas	mídias sociais

ID	Quem	Qtd	O quê foi avaliado	Como	Onde (contexto)
A71	usuários	29	arrependimento imediato após o uso do smartphone, tipos de recompensas obtidas com o uso de aplicativos de mídia social e recompensas alternativas ao uso de smartphones, relatos detalhados de usos arrependidos e reflexão sobre o uso acumulado.	entrevistas semi-estruturadas	mídias sociais, smartphone
A92	usuários	1060	motivos e opiniões sobre o que os usuários gostam ou não no conteúdo de anúncios online atuais, e se eles usam um bloqueador de anúncios e por quê.	questionário escala Likert questões abertas	propaganda online
A3	usuários	180	o processo de pensamento dos usuários enquanto selecionam uma interação e, posteriormente, para entender suas tendências emocionais após a conclusão de um vídeo.	questionnaire multiple choice open-ended semi-structured interviews	vídeos online
A9	usuários	16	como os deceptive patterns são experimentados pelos jogadores de jogos para dispositivos móveis, o papel de diversas partes interessadas da indústria na elaboração de deceptive patterns, como é possível de fato moldar a adoção e a experiência de deceptive patterns em prol do bem-estar.	workshops entrevistas semi-estruturadas individuais	jogos móveis
A54	Prolific Amazon-MTurk	173	frequência de uso do Facebook, frequência do encontro de anúncios no Facebook, preferência de dispositivo ao usar o Facebook, sentimentos dos usuários em relação aos anúncios que veem no Facebook.	questionário múltipla escolha, questões abertas escala Likert	mídias sociais, propaganda online
A50	usuários	406	consciência e preocupações sobre a influência potencial dos designs online, frequência de uso de serviços online e disposição para manipulação, capacidade de reconhecer diferentes tipos de padrões escuros.	questionário online escala Likert	internet
A43	Amazon-MTurk	387	como observar os comportamentos dos outros pode influenciar as crenças pessoais sobre a divulgação de informações pessoais	questionário	internet
A94	usuários	15	identificar os motivos ativos (competitividade, excesso de diversão e desafio ao sistema) e passivos ("dark" nudges de gamificação, compulsão e arrebanhamento) pelos quais os usuários tendem a usar mal a gamificação.	entrevistas semi-estruturadas	Duolingo
A84	usuários Amazon-MTurk	1100	os efeitos do nudging (sugestões subconscientes) nas respostas de avisos de consentimento dos usuários; como os deceptive patterns afetam a eficácia de avisos construídos com nudges.	questionário online logs de interação	aviso de consentimento
A28	usuários	40	efeitos de banners de consentimento na taxa de consentimento	interações dos participantes com os banners foram registradas e analisadas questionário	internet
A6	usuários	80.000	influência nos usuários: posição dos banners de consentimento; tipo de escolha no banner (binária, única, múltiplas, etc); forma de transmissão do conteúdo (técnico ou informal);	-Ações dos usuários foram registradas em logs e analisadas -questionário indicando as razões por ter clicado ou não no banner	internet
A80	Amazon MTurk	149	como os "apelos à ação" (calls to action) afetam a confiança dos usuários em um site	questionário usando escala likert	internet
A5	usuários (Google Ads, Amazon MTurk)	4357	como as opções de design afetam o comportamento dos usuários e a taxa na qual os usuários exercem seu direito de optar por não vender seus dados.	questionário logs de observação	internet
A15	usuários	1493	o efeito do design de banner de cookie deliberadamente manipulador nas escolhas do usuário	logs de interação	internet

ID	Quem	Qtd	O quê foi avaliado	Como	Onde (contexto)
A49	usuários (Amazon-MTurk(120))	120 13	como os mecanismos existentes no aplicativo móvel do YouTube dão suporte ou prejudicam o senso de agência, como as mudanças nesses mecanismos podem influenciar o senso de agência.	questionário online sessões individuais de think-aloud	youtube
A4	usuários	1109	o impacto de diferentes parâmetros de design em interfaces de consentimento.	logs de interação questionário	compras online
A63	usuários	987	como diferentes exibições de Termos e Condições de contratos online influenciam a conscientização e a satisfação do usuário.	questionário questões tipo Likert	contratos de Termos e Condições online
A68	usuários (Google Ads)	1557	impacto da inclinação e enquadramento, dois aspectos textuais dos banners de cookies, nas decisões de consentimento dos usuários.	logs de interação	aviso de consentimento
A86	usuários	7	investiga a influência de um deceptive pattern de captação de atenção tipicamente adotado por redes sociais no Facebook.	3 fases com questionário semanal logs	Facebook
A19	pesquisadores	-	análise do comprimento e da legibilidade de políticas de privacidade	testes de legibilidade de Flesch-Kincaid (Flesch Reading Ease Score e Flesch-Kincaid Reading Level)	políticas de privacidade