

UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE COMPUTAÇÃO
DEPARTAMENTO DE CIÊNCIAS DA COMPUTAÇÃO

PATRÍCIA RAPOSO SANTANA LIMA

**INVESTIGAÇÃO DA COMUNICABILIDADE E USO DE *DARK PATTERNS* COM
FOCO EM PRIVACIDADE NO INSTAGRAM**

Niterói
2021

PATRÍCIA RAPOSO SANTANA LIMA

**INVESTIGAÇÃO DA COMUNICABILIDADE E USO DE *DARK PATTERNS* COM
FOCO EM PRIVACIDADE NO INSTAGRAM**

Trabalho de conclusão de curso
apresentado ao curso de Bacharelado
em Ciências da Computação, como
requisito parcial para conclusão do
curso.

Orientadora:
Prof.^a Dr.^a Luciana Cardoso de Castro Salgado

Niterói
2021

PATRÍCIA RAPOSO SANTANA LIMA

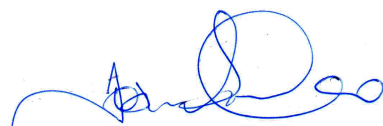
**INVESTIGAÇÃO DA COMUNICABILIDADE E USO DE *DARK PATTERNS* COM
FOCO EM PRIVACIDADE NO INSTAGRAM**

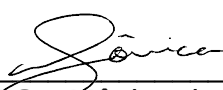
Trabalho de conclusão de curso
apresentado ao curso de Bacharelado
em Ciências da Computação, como
requisito parcial para conclusão do
curso.

Aprovada em 16 de setembro de 2021.

BANCA EXAMINADORA


Prof.^a Dr.^a Luciana Cardoso de Castro Salgado (Orientadora) - UFF


Prof. Dr. José Viterbo Filho - UFF


M.Sc. Mônica da Silva - UFF

Niterói
2021

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

L732i Lima, Patrícia Raposo Santana
INVESTIGAÇÃO DA COMUNICABILIDADE E USO DE DARK PATTERNS COM
FOCO EM PRIVACIDADE NO INSTAGRAM / Patrícia Raposo Santana
Lima ; Luciana Cardoso de Castro Salgado, orientadora.
Niterói, 2021.
68 f.

Trabalho de Conclusão de Curso (Graduação em Ciência da
Computação)-Universidade Federal Fluminense, Instituto de
Computação, Niterói, 2021.

1. Interação homem-máquina. 2. Ética. 3. Produção
intelectual. I. Salgado, Luciana Cardoso de Castro,
orientadora. II. Universidade Federal Fluminense. Instituto de
Computação. III. Título.

CDD -

AGRADECIMENTOS

Gostaria de agradecer em primeiro lugar aos meus pais, Nelson Ricardo e Marília, por terem me ensinado a importância do conhecimento e por sempre terem me incentivado e apoiado a estudar.

Agradeço também a Beatriz Toledo e Jacqueline Amaro por desde o primeiro grau me darem apoio emocional e psicológico para atravessar todos os momentos de estresse que uma formação exige.

Agradeço aos meus colegas de graduação que em diversos momentos se mostraram meus verdadeiros companheiros, combinando disciplinas para cursarmos juntos, tirando minhas dúvidas, se reunindo na sala de estudos antes das avaliações, me dando diversas dicas e tornando o dia a dia na universidade mais leve. Sem vocês não teria sido possível.

Agradeço a minha orientadora, Luciana Salgado, por todos os puxões de orelha e também por toda a compreensão que foram essenciais nessa caminhada rumo a monografia.

Gostaria de agradecer também a todos os meus amigos que não me deixaram desistir. E por último, gostaria de agradecer a mim mesma por ter resistido até aqui, apesar de tudo.

RESUMO

Uma das categorias de software mais utilizados e que continua ganhando espaço são as redes sociais. A exposição onipresente a sistemas sociais em todas as áreas da nossa vida nos afetou de diferentes formas e devido a essa crescente exposição a quantidade de dados sendo inseridos na internet está crescendo rapidamente, sem previsão para que isso mude. O Instagram, por exemplo, possui mais de 1 bilhão de usuários ativos mensalmente e 500 milhões de usuários ativos diariamente. Com isso, são mais de 4.2 bilhões de *"likes"*, 100 milhões de *uploads* de fotos e 400 milhões de *stories* por dia. Esses diferentes tipos de dados constituem uma fonte de informação disponível aos sistemas *Big Data*, podendo portanto serem usados para acúmulo de conhecimento por parte de empresas e governos. Pesquisas têm alertado que ataques contra a privacidade, ou seja, inferência ou descoberta de atributos privados, podem ocorrer através desses dados e que mesmo dados anônimos podem ser re-identificados. Isso levanta o debate sobre a privacidade e a propriedade desses dados. Este estudo investigou a rede social Instagram, avaliando a comunicabilidade dele sobre os seguintes princípios éticos de privacidade: consentimento informado, controle sobre o uso de dados e direito a restringir processamento. Para atingir esse objetivo foi aplicado o Método de Inspeção Semiótica para buscar estratégias de comunicação destes princípios éticos de privacidade e foram identificados rastros de uso de *Dark Patterns* nessas estratégias. Os principais resultados indicam potenciais violações nesses princípios éticos de privacidade.

Palavras-chave: Engenharia Semiótica. Privacidade. Ética. Redes Sociais. Interação Humano-Computador. Padrões Obscuros.

ABSTRACT

One of the most used software categories and one that continues to gain space is social networks. The ubiquitous exposure to social systems in all areas of our lives has affected us in different ways. Because of this growing exposure, the amount of data fed into the internet proliferates, with no forecast of change. Instagram, for example, has over 1 billion active users monthly and 500 million active users daily. With that, there are more than 4.2 billion likes, 100 million photo uploads, and 400 million stories per day. These different types of data constitute a source of information available to Big Data systems and can therefore be used for knowledge accumulation by companies and governments. Research has warned that privacy attacks, i.e., inference or discovery of private attributes, can occur through this data. Even anonymous data can be re-identified, which raises the debate over the privacy and ownership of that data. This study investigated the Instagram social network, evaluating its communicability on the following ethical privacy principles: informed consent, control over data use, and the right to restrict processing. For that to happen, we applied the Semiotic Inspection Method to seek strategies to communicate these ethical principles of privacy and identified traces of Dark Patterns' use in these strategies. The main results indicate potential violations of these ethical privacy principles.

Keywords: Semiotic Engineering. Privacy. Ethics. Social Networks. Human-Computer Interaction. Design Patterns.

LISTA DE FIGURAS

Figura 1 – Tela para criar conta.....	30
Figura 2 – Inserir e-mail para cadastro.....	31
Figura 3 – Inserir código de confirmação ao cadastrar-se.....	31
Figura 4 – Inserir data de nascimento ao cadastrar-se.....	31
Figura 5 – Inserir nome no cadastro.....	32
Figura 6 – Confirmar o cadastro.....	32
Figura 7 – Encontrar amigos ao cadastrar-se.....	33
Figura 8 – Encontrar amigos ao cadastrar-se após clicar em “pular”.....	33
Figura 9 – Encontrar contatos ao cadastrar-se	34
Figura 10 – Encontrar contatos ao cadastrar-se após clicar em “pular”.....	34
Figura 11 – Adicionar foto de perfil durante o cadastro.....	35
Figura 12 – Ativar notificações durante o cadastro.....	35
Figura 13 – Ativar notificações depois de clicar em ativar.....	36
Figura 14 – Sugestões de contas para seguir durante o cadastro.....	36
Figura 15 – Configurações de Segurança do Instagram.....	42
Figura 16 – Login para acessar dados.....	43
Figura 17 – Primeira parte de acessar dados.....	44
Figura 18 – Segunda parte de acessar dados.....	44
Figura 19 – Terceira parte de acessar dados.....	45
Figura 20 – Quarta parte de acessar dados.....	45
Figura 21 – Acesso aos dados de histórico de pesquisa.....	46
Figura 22 – Solicitar download de dados.....	47
Figura 23 – Inserir senha para download.....	47
Figura 24 – Confirmação de solicitação de download.....	48
Figura 25 – Primeira parte de “Editar Perfil”.....	51
Figura 26 – Segunda parte de “Editar Perfil”.....	51
Figura 27 – Desativar conta.....	52

Figura 28 – Desativar conta porque segunda conta foi criada.....	53
Figura 29 – Desativar conta por causa de anúncios em excesso.....	53
Figura 30 – Desativar conta por outro motivo.....	53
Figura 31 – Desativar conta por precisar de um tempo.....	53
Figura 32 – Desativar conta porque não consegue achar pessoas para seguir.....	53
Figura 33 – Desativar conta por questões de privacidade.....	53
Figura 34 – Desativar conta por problemas para começar.....	54
Figura 35 – Desativar conta porque quer remover algo.....	54
Figura 36 – Desativar conta porque ocupa muito tempo.....	54
Figura 37 – Inserir senha para desativar.....	54
Figura 38 – Confirmar que quer desativar conta.....	55

LISTA DE QUADROS

Quadro 1 – Lições aprendidas com os trabalhos relacionados.....	25
---	----

LISTA DE ABREVIATURAS

CCPA	California Consumer Privacy Act
GDPR	Regulamento Geral sobre a Proteção de Dados
IA	Inteligência Artificial
IOS	Sistema Operacional da Apple Inc.
LGPD	Lei Geral de Proteção de Dados Pessoais
MAC	Método de Avaliação da Comunicabilidade
MIS	Método de Inspeção Semiótica
PbD	<i>Privacy by Design</i>
SI	Sistemas Informacionais

SUMÁRIO

1. INTRODUÇÃO	11
1.1. PRIVACIDADE E REDES SOCIAIS.....	12
1.2. OBJETIVOS.....	14
1.3. METODOLOGIA.....	14
1.4. ORGANIZAÇÃO DO TRABALHO.....	15
2. FUNDAMENTAÇÃO TEÓRICA.....	16
2.1. PRINCÍPIOS ÉTICOS EM COMPUTAÇÃO.....	16
2.2. <i>PRIVACY BY DESIGN</i> E PRINCÍPIOS DE PRIVACIDADE.....	17
2.3. <i>DARK PATTERNS</i>	21
3. TRABALHOS RELACIONADOS	23
4. ESTUDOS REALIZADOS	27
4.1. A REDE SOCIAL INSTAGRAM.....	27
4.2. INSPEÇÃO SEMIÓTICA DO INSTAGRAM.....	27
4.2.1. Consentimento Informado.....	29
4.2.1.1 Reconstrução da metacomunicação no Cenário 1.....	36
4.2.1.2. Análise e identificação de estratégias de design do Cenário 1.....	40
4.2.2. Controle Sobre o Uso de Dados.....	41
4.2.2.1 Reconstrução da metacomunicação no Cenário 2.....	48
4.2.2.2. Análise e identificação de estratégias de design do Cenário 2.....	50
4.2.3. Direito a Restringir Processamento.....	51
4.2.3.1 Reconstrução da metacomunicação no Cenário 3.....	55
4.2.3.2. Análise e identificação de estratégias de design do Cenário 3.....	56
4.3. DISCUSSÃO	57
5. CONCLUSÃO	60
5.1. LIMITAÇÕES	61
5.2. TRABALHOS FUTUROS.....	61
REFERÊNCIAS BIBLIOGRÁFICAS	62

1. INTRODUÇÃO

Uma das categorias de software mais utilizados e que continua ganhando espaço são as redes sociais. De acordo com Recuero (2007) uma rede social é definida como um conjunto de dois elementos, sendo o primeiro os atores da rede (pessoas, instituições ou grupos) e o segundo suas conexões. Essa estrutura dos atores e suas conexões através da Internet é intermediada por dispositivos e computadores.

Segundo levantamento realizado pela WeAreSocial¹, uma agência de marketing digital especializada em mídias sociais, em parceria com GlobalWebIndex² e App Annie³, em 2019, 89% da população entre 16 e 64 anos que acessa a internet relatou utilizar aplicativos de redes sociais (Kemp, 2020a). Além disso, em 2019, na Google Play, a categoria de aplicativos “Social” foi a quinta mais baixada e a segunda mais utilizada, enquanto que, para o **sistema** operacional móvel da Apple Inc. (IOS), a categoria “Social Networking” foi a sexta mais baixada e a terceira mais utilizada (Kemp, 2020a). E esses números provavelmente cresceram. Se em 2019 o número de usuários de redes sociais era de 3.8 bilhões, em outubro de 2020 alcançamos a marca de 4.14 bilhões de usuários (Kemp, 2020b).

No Brasil, pessoas entre 16 e 64 anos gastam em média 3 horas e 31 minutos diariamente acessando redes sociais em qualquer dispositivo (Kemp, 2020a). A exposição onnipresente a sistemas sociais em todas as áreas da nossa vida (seja na educação, no trabalho, nos cuidados ou no entretenimento) pode alterar a nossa concepção de ação social ou afetar as nossas relações e laços sociais. Ao mesmo tempo que afastou as pessoas do convívio social presencial, diversificou a interação tornando-a instantânea e globalizada. Além disso, afetou os meios de comunicação e propagação de ideias, estabelecendo uma inter-relação por duplo canal onde o receptor tem a possibilidade de responder imediatamente. (Kohn & Moraes; 2007)

Devido a essa crescente exposição, a quantidade de dados sendo inseridos na internet está crescendo rapidamente, sem previsão de que isso mude. O

1 <https://wearesocial.com/>

2 <https://www.gwi.com/>

3 <https://www.appannie.com/en/>

Instagram⁴, por exemplo, possui mais de 1 bilhão de usuários ativos mensalmente e 500 milhões de usuários ativos diariamente. Com isso, são mais de 4.2 bilhões de “likes”, 100 milhões de *uploads* de fotos e 400 milhões de “stories” por dia. (Ahlgren, 2021)

Esses diferentes tipos de dados constituem uma fonte de informação disponível aos sistemas de *Big Data*, podendo portanto serem usados para acúmulo de conhecimento por parte de empresas e governos. Segundo Erl, Khattak e Buhler (2016), *Big Data* é um campo de análise, processamento e armazenamento de grande volume de dados que atende a requisitos distintos, como a combinação de conjuntos de dados não relacionados, processamento de grande quantidade de dados não estruturados e coleta de informações sem transparência e que são sensíveis.

Existem cinco características que podem ajudar a diferenciar *Big Data* de outros tipos de dado: Volume, ou seja, a quantidade de dados prevista em um sistema *Big Data* é grande e está em constante crescimento; Velocidade, ou seja, enormes conjuntos de dados podem se acumular em curtos períodos de tempo; Variedade, ou seja, os dados estão em diferentes formatos e tipos; Veracidade, ou seja, a qualidade dos dados deve ser verificada resolvendo dados inválidos e removendo o ruído; e Valor, ou seja, os dados devem possuir relevância para o problema. (Erl, Khattak e Buhler, 2016)

1.1 PRIVACIDADE E REDES SOCIAIS

Pesquisas têm alertado que ataques contra a privacidade, ou seja, inferência ou descoberta de atributos privados, podem ocorrer através das informações oriundas dessa utilização de redes sociais (Lindamood et al, 2009). Cientistas da computação têm mostrado repetidamente que mesmo dados anônimos podem ser re-identificados e atribuídos a indivíduos específicos (Ohm, 2010, Mooney & Pejaver, 2018). Além disso, através de diferentes tipos de dados como textos (Chen et al,

4 <https://www.instagram.com/>

2014), imagens (Wang & Kosinski, 2018), e inclusive “likes” (Kosinski, 2012), informações como gênero, sexualidade, dentre outras, podem ser deduzidas através, inclusive, de técnicas de Inteligência Artificial (IA) (Bindu, 2017). Isso levanta o debate sobre a privacidade e a propriedade desses dados.

Adicionalmente, outras pesquisas investigam sobre a necessidade de mecanismos para apoiar a tomada de decisão individual relacionada à Privacidade (Almeida, 2019). Bier et. al (2016), por exemplo, discutem formas de apoio ao exercício da privacidade de dados. Sistemas on-line têm adotado políticas de dados com as quais os usuários precisam consentir antes de utilizar um determinado sistema. Contudo, apesar de existirem tais políticas, geralmente apresentadas ao usuário durante o cadastro nesses serviços, estas muitas vezes servem apenas como isenção de responsabilidade para as empresas, sem de fato explicar especificamente como os dados serão usados ou combinados para gerar outras informações (Majedi & Barker, 2021).

Outra prática é dar aos usuários opções de configuração de sua privacidade e acesso de seus dados nas redes, para dar mais controle para eles. Contudo, o trabalho de Cavusoglu (2016), tendo como objeto de estudo o Facebook, mostrou que dar aos usuários mais controle sobre o alcance de postagens no mural resultou em uma divulgação mais aberta de conteúdo. Ou seja, dar aos usuários mais controle sobre as informações de seu perfil pessoal pode ter como consequência uma maior divulgação de informações pessoais.

Essas problemáticas estão relacionadas aos princípios éticos de privacidade (Fjeld et al, 2020), uma vez que apontam para uma maior produção e disponibilidade de dados que podem ser utilizados por estes sistemas, através de um consentimento prejudicado por falta de informação disponível aos usuários. Tais princípios são apresentados no capítulo de fundamentação teórica e analisados dentro do Instagram no presente trabalho.

1.2 OBJETIVOS

Portanto, o presente trabalho tem como objetivo geral identificar as estratégias de comunicação dos princípios éticos no Instagram. Os sub-objetivos incluem:

- Avaliar a comunicabilidade do Instagram em relação à privacidade sobre os seguintes princípios éticos de Privacidade: consentimento informado, controle sobre o uso de dados e direito a restringir processamento;
- Avaliar se e de que forma o Instagram falha em promover um relacionamento ético com seus usuários e a sociedade;
- Identificar se há rastros do uso de Dark Patterns em alguma das estratégias de comunicação dos princípios éticos no Instagram.

1.3. METODOLOGIA

Este projeto de pesquisa delimitou-se em coletar evidências empíricas sobre a utilização, ou não, de princípios de privacidade éticos no Instagram. Portanto, buscou-se reunir dados com o propósito de responder ao seguinte problema de pesquisa: O Instagram proporciona um relacionamento negativo com seus usuários pela falta de aplicação de princípios de privacidade? De que forma?

Ao longo de todo o estudo foi investigada a presença de falhas nos seguintes princípios éticos de privacidade: consentimento, controle sobre o uso dos dados e habilidade de restringir o processamento de dados. Esses princípios foram escolhidos por conveniência, visto que eram os que mais se encaixavam com possíveis cenários de uso do Instagram, que poderiam ser verificados através da utilização da aplicação, sem acesso a seus algoritmos.

A coleta de dados foi feita por meio de pesquisa qualitativa preditiva (Lewis, 2015) por meio do Método de Inspeção Semiótica (MIS) (De Souza & Leitão, 2009), dado que o critério para a identificação dos resultados não é numérico e depende de interpretação crítica e subjetiva. O problema foi direcionando a pesquisa para a área de Interação Humano-Computador.

1.4. ORGANIZAÇÃO DO TRABALHO

No Capítulo 2, é descrita a fundamentação teórica do trabalho, são apresentados os princípios éticos de privacidade escolhidos para avaliar o Instagram, assim como uma discussão de Privacidade.

No Capítulo 3, são discutidos trabalhos relacionados.

No Capítulo 4, apresenta-se os resultados da inspeção preliminar e do MIS e discute-se os resultados apresentados apontando possíveis quebras em princípios de privacidade, com a finalidade de responder a pergunta problema.

No Capítulo 5, conclui-se o trabalho e discutem-se as limitações dele e possíveis trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo discute os conceitos de Ética e Privacidade, assim como o de *Privacy by Design* e princípios éticos de Privacidade. Além disso, o capítulo aborda o conceito de *Dark Patterns*.

2.1. PRINCÍPIOS ÉTICOS EM COMPUTAÇÃO

Para Moor (1985), ética em computação é a análise da natureza e do impacto social de tecnologias computacionais, formulando políticas pessoais e sociais para o uso ético dessas tecnologias. Para o autor, existe uma lacuna política em como a tecnologia computacional deveria ser usada, visto que computadores fornecem novas habilidades, nos dando novas escolhas de ação para as quais não existem políticas adequadas.

A principal preocupação da ética em IA é identificar como ela pode melhorar ou causar preocupações para a sociedade, seja em termos de qualidade de vida dos indivíduos ou de autonomia e liberdade humana necessárias para uma sociedade democrática. Para que cada vez mais tarefas sejam delegadas à IA é necessário garantir que esses sistemas produzem impacto equitativo na vida das pessoas, de que agem de acordo com valores irredutíveis e que existem processos de responsabilização para assegurar isso (AI, HLEG; 2020).

Santoro e Da Costa (2021) argumentam que situações que envolvem o desenvolvimento ou o uso de Sistemas Informacionais (SI) devem ser analisadas do ponto de vista ético utilizando um processo bem definido. Esse processo, criado por elas, é dividido em sete etapas que ajudam na tomada de decisões. São eles: (A) Identificar e descrever os fatos, buscando informações em fontes seguras, já que a visão correta da situação pode ajudar com uma solução; (B) Definir o dilema, reconhecendo o conflito e identificando os valores envolvidos; (C) Identificar as partes interessadas; (D) Identificar alternativas, ou seja, diferentes implementações

que podem suprimir o dilema; (E) Identificar consequências de cada uma dessas alternativas; (F) Adotar uma posição, geralmente se utilizando de um ou mais princípios filosóficos; e (G) Publicar os resultados com grupos diversos e com a sociedade para promover mudanças.

Na seção seguinte, será apresentado o tema da Privacidade, foco deste trabalho, além dos princípios éticos ligados a ele.

2.2. *PRIVACY BY DESIGN* E PRINCÍPIOS DE PRIVACIDADE

A privacidade é um direito fundamental garantido pela Declaração Universal dos Direitos Humanos, proclamada pela Organização das Nações Unidas, em seu Artigo 12º “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação.[...]” No Brasil, a Constituição brasileira de 1988 no art.5º, inciso X, inclui o direito à privacidade considerando invioláveis “[...] a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Segundo documento publicado pela Unesco (2017):

“O direito geral à privacidade está relacionado a muitas questões distintas, como a liberdade e habilidade de definir o espaço pessoal separado do espaço público; de se proteger de intromissões indesejadas; e de controlar o acesso ou a divulgação não autorizada de informações pessoais. Esse direito também se encontra associado aos conceitos de identidade e confidencialidade, anonimato e dignidade humana”.

De acordo com Vianna (2006), o direito à privacidade reveste-se de interesse não apenas individual, mas também e principalmente de interesse público. Ele torna-se um dos fundamentos do Estado Democrático de Direito, visto que a tríade ver-saber-poder, elementos fundamentais do controle social, se manifesta nas sociedades do controle como monitorar-registrar-reconhecer. Ou seja, o direito à

privacidade deve ser concebido como uma tríade de direitos: direito de não ser monitorado, direito de não ser registrado e direito de não ser reconhecido.

Algumas legislações foram criadas ao longo do tempo para proteção de dados pessoais e da privacidade como o Regulamento Geral sobre a Proteção de Dados (GDPR) (UE)2016/679, em proteção a todos os indivíduos na União Européia, a Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei nº 13.709/2018, em proteção dos cidadãos brasileiros, e o California Consumer Privacy Act of 2018 (CCPA) nos Estados Unidos da América.

Segundo Kizza (2007), a privacidade, tradicionalmente considerada valiosa, ganhou ainda mais importância na era da informação, visto que protege a identidade pessoal de um indivíduo, preserva sua autonomia e torna relações sociais possíveis. Considerando esses três pontos (identidade pessoal, autonomia e relações sociais) como seus atributos, Kizza (2007) introduz a classificação de privacidade em três diferentes tipos: Privacidade pessoal, que envolve nada nem ninguém se envolver ou se intrometer no espaço pessoal alheio, como em buscas físicas, gravações de vídeo ou voz e qualquer tipo de vigilância; Privacidade Institucional, que envolve a proteção de dados privados de instituições e organizações; e Privacidade da Informação, que envolve a proteção de quaisquer dados e informações relacionadas a algum indivíduo, seja ela pessoal, financeira, médica, digital, dentre outros. A Privacidade da Informação é o principal tipo de privacidade com o qual o presente trabalho se relaciona.

Dentre as violações da privacidade levantadas por Kizza (2007) estariam a intrusão (como quando hackers invadem um sistema), o mal uso da informação (coleta de informações para uso não autorizado), a interceptação de informação (quando um terceiro ganha acesso não autorizado a informações compartilhadas entre duas ou mais partes) e a combinação de informações (como ligar informações com outras informações erradas, roubadas ou provenientes de bancos de dados distintos).

De acordo com a GDPR, *Privacy by Design (PbD)* é obrigatório. *Privacy by Design* é a ideia, que já existe há mais de 20 anos, de que os dados de um indivíduo devem ser protegidos por design e seu objetivo final é garantir que a proteção dos dados esteja presente desde os primeiros estágios de desenvolvimento ao invés de

ser implementada como uma camada adicionada a um produto ou sistema (AEPD, 2019).

O *PbD* é fundamentado em 7 princípios: (1) “**Proativo**, não reativo; **Preventivo**, não corretivo”, que implica o reconhecimento e a antecipação de políticas de privacidade ruins e suas consequências, para corrigir impactos negativos antes mesmo que eles ocorram; (2) “Privacidade como **Configuração padrão**”, ou seja, a garantia de que dados pessoais são automaticamente protegidos em qualquer sistema, sem a necessidade de que o indivíduo tome ação para isso, sendo garantido ao usuário o máximo possível de privacidade como padrão; (3) “Privacidade **incorporada** ao design”, o que implica que a privacidade é inseparável dos sistemas, aplicações, produtos e serviços, sendo considerado um requisito não-funcional; (4) “Funcionalidade total”, ou seja, a privacidade não deve competir com outros interesses legítimos, como a segurança, mas sim ser incorporada de forma que não comprometa a plena funcionalidade do sistema; (5) “Segurança de ponta a ponta”; ou seja, o *PbD* se aplica a todo ciclo de vida dos dados envolvidos; (6) “Visibilidade e Transparência”, fundamental para responsabilização e confiança, o sistema deve estar poder ser sujeito a verificações; e (7) “Respeito pela privacidade do usuário”, que pressupõe o máximo zelo pelos interesses do usuário. (Cavoukian, 2009)

De acordo com Fjeld et al (2020), a privacidade é impactada significativamente por tecnologias de IA, visto que tais tecnologias são usadas em diversos contextos sensíveis, tendo então acesso a dados também sensíveis. A questão da privacidade, contudo, não aparece apenas em relação a utilização desses sistemas, mas também durante o seu desenvolvimento e treinamento dos modelos de IA.

Segundo Dwivedi et al (2019), os sistemas de IA estão sendo cada vez mais usados em uma variedade de setores, incluindo saúde, transporte e cadeia de produção e podem representar desafios sociais, econômicos, políticos, éticos, dentre outros, significativos para governos e organizações à medida que o escopo em que podem ser aplicados aumenta. Devido ao seu poderoso impacto em vários domínios sociais, a IA gerou amplo debate sobre os princípios e valores que devem guiar seu desenvolvimento e uso (Bostrom & Yudkowsky 2014, Ryan & Stahl 2020).

Diferentes definições de IA têm sido apresentadas pela literatura, cada uma encapsulando conceitos de inteligência não-humana programada para realizar tarefas específicas. Russell e Norvig (2010) definiram o termo IA como um sistema que imita funções cognitivas geralmente associadas a atributos humanos como resolução de problemas, conhecimento, raciocínio, planejamento e aprendizagem.

Uma definição mais completa é a da Comissão Europeia de Peritos de Alto Nível sobre a IA, que conceitua sistemas de IA como sistemas de software (e eventualmente de hardware) que atuam percebendo seu ambiente, interpretando dados recolhidos (estruturados ou não), raciocinando sobre o conhecimento ou processando informações advindas desses dados e decidindo as melhores ações a adotar para atingir um determinado objetivo (AI, HLEG; 2020).

Princípios Éticos de IA são diretrizes criadas para fixar regras e recomendações com o objetivo de promover que sistemas de IA sejam desenvolvidos assegurando a centralidade na pessoa humana. Existe uma gama de documentos disponíveis que definem esses princípios, embora tenham um objetivo em comum, diferem muito entre si como em relação a sua composição, público alvo, profundidade e escopo (Fjeld et al, 2020). Os Princípios Éticos de Privacidade partem da ideia de que sistemas de IA devem respeitar a privacidade individual, tanto no uso de dados para desenvolvimento de sistemas quanto ao fornecer agência ao indivíduo sobre seus dados e decisões tomadas (Fjeld et al, 2020).

Neste trabalho foram explorados no Instagram três princípios éticos de privacidade: consentimento informado, controle sobre o uso dos dados e habilidade de restringir processamento dos dados.

Consentimento é definido pela LGPD, no art.5º, inciso XII, como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados para uma finalidade determinada”. Esse consentimento também deverá poder ser revogado a qualquer momento. Para Fjeld et al (2020), consentimento é o princípio segundo o qual os dados de um indivíduo não devem ser usados sem seu conhecimento e permissão e consentimento informado é um princípio mais robusto em que, além de conhecimento e permissão para o uso dos dados do usuário, também é necessário que ele esteja ciente dos riscos, benefícios e alternativas deste uso.

Consentimento informado, em *PbD*, é um padrão de design que dá suporte a duas estratégias de design de privacidade: controlar e informar. Informar consiste em manter o indivíduo informado sobre a natureza e as condições do processamento de seus dados, e tem dentre suas táticas fornecer, explicar e notificar. Já controlar consiste em dar controle efetivo para o indivíduo sobre seus dados pessoais, tendo como algumas de suas estratégias o consentimento, a atualização e a deleção. (AEPD, 2019)

O controle sobre o uso dos dados também é apontado em trabalhos relacionados. Nos Princípios Éticos de Privacidade (Fjeld et al, 2020), é definido como sendo o princípio segundo o qual indivíduos possuem algum grau de influência em relação a como e porquê dados sobre ele são usados. Paralelos às estratégias vistas no parágrafo anterior, consentimento, direito de retificar dados e direito de apagar dados são princípios que podem ser pensados como parte de “controle sobre o uso dos dados” visto que são formas de exercer este controle (Fjeld et al, 2020).

Na definição de interação humano-dados de Mortier (2014), o controle sobre os dados é explicado pelo conceito de agência, que consiste em fornecer aos indivíduos meios para gerenciar seus dados e seu acesso por terceiros, bem como buscar formas eficazes de atuação nesses sistemas, na medida em que os indivíduos acham apropriado.

Habilidade de restringir processamentos é o princípio que se refere ao direito de um indivíduo restringir o uso e a conexão de dados relacionados a ele com o sistema (Fjeld et al, 2020). Segundo a GDPR, no art. 13(2)(b), o responsável pelo tratamento dos dados deve assegurar ao titular o direito de solicitar restrição de processamento desses dados, assim como retificação e apagamento deles.

2.3. DARK PATTERNS

Segundo Brignull (2010), *Dark Patterns* são truques usados em sites e aplicativos que levam o usuário a fazer coisas que ele não pretendia realmente. Ou seja, *Dark Patterns* é um termo usado para designar instâncias onde o design usa

do seu conhecimento sobre o comportamento humano (como psicologia) e os desejos dos usuários finais para implementar funcionalidades que não estão a favor dos interesses do usuário (Gray et al., 2018)

Brignull separou em alguns tipos, sendo os *Roach Motel* e *Misdirection* relevantes para o presente trabalho. *Roach Motel* é o tipo de *Dark Patterns* em que o design faz com que seja fácil entrar em determinada situação, mas não tão fácil sair dela, como por exemplo, quando o usuário se cadastra em um site, mas não é possível excluir sua conta, ou então para excluir sua conta ele precisa enviar algum e-mail ou realizar um telefonema (Gray et al., 2018).

Misdirection, por sua vez, é o tipo de *Dark Patterns* em que o design propositalmente chama o foco da atenção do usuário para alguma parte da interface para que ele não note outra (Gray et al., 2018).

O conceito de *Dark Patterns* é importante para esse trabalho, porque analisamos as potenciais violações de privacidade no Instagram à luz dos princípios éticos de privacidade, mas do ponto de vista do design.

3. TRABALHOS RELACIONADOS

A privacidade em redes sociais é um assunto complexo e pode ser estudado de diversas perspectivas. A seguir será feita a revisão de trabalhos que exploraram a perspectiva de Design e/ou de IA.

O trabalho de Zheleva & Gettor (2009) estudou as implicações da mistura de perfis públicos e privados em redes sociais. O estudo aponta que, mesmo que um perfil seja privado, as relações com outros perfis e a participação em grupos dentro de redes sociais podem levar ao vazamento de informações. Com isso, tanto entidades comerciais quanto governamentais podem utilizar esta vulnerabilidade para empregar ataques de inferência de dados através de classificação relacional com o objetivo de marketing direcionado, monitoramento político, dentre outros. Embora não tenham sido utilizados os algoritmos das próprias redes sociais analisadas no estudo, os resultados demonstram a possibilidade de que estes também consigam inferir informações. Entretanto, esse estudo não explora nem associa a interface das redes sociais e o seu respectivo uso em tempo de interação com questões de privacidade.

Os trabalhos de De Carvalho et al (2012) e de Terto et al (2012) possuem propostas parecidas ao discutir a interface das Configurações de Privacidade de “Marcação de Publicações e Fotos” do Facebook utilizando métodos baseados na Engenharia Semiótica. Ambos os trabalhos demonstraram falhas de comunicabilidade nas questões de privacidade do Facebook, apontando problemas com as informações de ajuda e dificuldade por parte dos usuários em encontrar, entender e utilizar as configurações de privacidade. Embora os trabalhos tenham um escopo pequeno, analisando apenas uma tarefa, e tenham sido realizados no Facebook, eles são relevantes por se proporem a relacionar questões de interface com questões de privacidade. Contudo, os trabalhos não exploram os princípios éticos de privacidade como o presente trabalho.

Já o trabalho de De Rezende Xavier (2014), realizado no Facebook com foco em usuários brasileiros, buscou entender o quão pessoal é uma informação, o seu compartilhamento nos mundos físico e virtual e o entendimento dos usuários sobre

privacidade on-line. Ao contrastar como os usuários lidam com a privacidade on-line e off-line ela notou que há uma homogeneização dos patamares de compartilhamento off-line quando se trata de redes sociais, ou seja, um grupo de pessoas que no mundo físico são tratados com diferentes níveis de confiança, no mundo virtual são tratadas como sendo de um único nível. Neste estudo observou-se também que embora haja uma tendência de que quanto mais pessoal é uma informação menor a chance dela ser publicada, alguns tipos de informação não seguem essa tendência. A partir de uma inspeção utilizando o MIS da interface do Facebook, notaram que algumas decisões de interface parecem incentivar a divulgação dessas informações através de diversas estratégias como solicitar a mesma informação em vários lugares distintos e pedir informações em locais de destaque. Além disso, o estudo mostrou que os usuários não têm uma boa noção dos impactos de suas configurações de privacidade e podem ser levados a acreditar que suas informações sensíveis estão protegidas quando não estão.

Por último, o estudo de Dos Santos, Barbosa e Barbosa (2016) buscou avaliar a interface do Instagram para identificar e caracterizar a proposta de privacidade do sistema. Essa avaliação foi realizada utilizando o MIS, tendo em vista identificar as decisões do projetista que refletem em estratégias de privacidade. Notaram que apesar do Instagram fazer uso da maioria das estratégias de privacidade encontradas por eles na literatura (como ser possível manter mais de uma conta, excluir informações pessoais, ocultar informações pessoais, dentre outros) os usuários nem sempre percebem ou utilizam os recursos disponíveis por meio das configurações oferecidas. A avaliação foi realizada em tarefas distintas das avaliadas no presente trabalho, inspecionando (1) pesquisar e seguir usuários, (2) publicar e visualizar conteúdo, (3) interagir socialmente com os seguidores através dos recursos do sistema, e (4) configurar aspectos de privacidade relacionados às três tarefas anteriores.

Quadro 1 - Lições aprendidas com os trabalhos relacionados

Estudo	Foco do estudo	Principais resultados	Relevância
Zheleva & Gettor (2009)	Consequências da mistura de perfis públicos e privados em redes sociais.	Mesmo um perfil privado pode ter suas informações vazadas através das relações com outros perfis.	Mostra que é possível inferir informações através de algoritmos de IA.
De Carvalho et al (2012)	Identificar problemas nas configurações de privacidade do Facebook para marcação em fotos	A funcionalidade de configuração de privacidade não é familiar aos usuários que realizaram os testes, o que mostra a existência de falhas de comunicabilidade	O estudo utiliza o MIS para entender questões de privacidade.
Terto et al (2012)	Avaliar a comunicabilidade das configurações de privacidade do Facebook com foco nos recursos de controle e remoção de marcação em fotos	Foram encontradas rupturas de comunicação que podem levar o usuário a não conseguir acessar e/ou alterar suas configurações de privacidade	O estudo utiliza o MIS para entender questões de privacidade.
De Rezende Xavier (2014)	Entender quão pessoal é uma informação, o seu compartilhamento	Algumas decisões de interface incentivam divulgação de informações pessoais	O estudo investiga a comunicabilidade do Facebook em relação à

	nos mundos físico e virtual e a percepção dos usuários sobre privacidade on-line	e os usuários não entendem os impactos das configurações de privacidade	privacidade.
Dos Santos, Barbosa & Barbosa(2016)	Caracterizar a proposta de privacidade do Instagram	O Instagram faz uso da maior parte das estratégias de privacidade, contudo os usuários nem sempre percebem/usam os recursos oferecidos	O estudo analisa questões de privacidade no Instagram através do MIS, contudo inspeciona partes diferentes da interface.

Concluindo, os trabalhos descritos nesta seção deixam como principais lições aprendidas quais são os possíveis riscos da não aplicação de princípios éticos de privacidade e a importância do papel do design ao promover a privacidade.

4. ESTUDOS REALIZADOS

Este capítulo apresenta os passos para coleta de evidências para respondermos à pergunta: “ O Instagram proporciona um relacionamento negativo com seus usuários pela falta de aplicação de princípios de privacidade? De que forma?

A seção 4.1 apresenta o objeto de estudo deste trabalho, o Instagram.. Na seção 4.2 é descrita a inspeção preliminar e a aplicação do MIS (De Souza & Leitão, 2009).

4.1. A REDE SOCIAL INSTAGRAM

Lançado em outubro de 2010 e pertencente a Facebook Inc., o Instagram é uma rede social para compartilhamento de fotos e vídeos entre seus usuários, através de postagens, *stories* ou via mensagem. Os usuários podem seguir outros perfis para que as publicações deste apareçam em seu feed e podem interagir com as publicações ao curtir, comentar, compartilhar e salvar postagens ou ao responder ou reagir a um *story*. Os usuários também têm a possibilidade de conversarem de forma privada e enviarem fotos e vídeos que ficam indisponíveis após uma ou duas visualizações, de acordo com a vontade destes.

Analogamente, também é possível buscar e seguir tags para visualizar no feed publicações relacionadas a tópicos de interesse, como arte, música e notícias.

4.2. INSPEÇÃO SEMIÓTICA DO INSTAGRAM

Fundamentado na Engenharia Semiótica (de Souza, 2005), o MIS avalia a comunicabilidade de um sistema interativo por meio de inspeção (de Souza et al.,

2006). “O objetivo da inspeção semiótica é avaliar a qualidade da emissão da metacomunicação do designer codificada na interface” (BARBOSA & SILVA, 2010).

Antes da inspeção o avaliador identifica quais são os perfis de usuários da aplicação e seus objetivos nela, para a partir disso definir o escopo da inspeção e os cenários de interação. O método consiste em reconstruir a metamensagem emitida pelo design através da inspeção de signos estáticos, dinâmicos e metalinguísticos, um tipo por vez. As escolhas do design da aplicação comunicam o que este pensa sobre os usuários e é essa mensagem que o avaliador irá buscar ao longo da inspeção, preenchendo o seguinte template de metacomunicação genérico (de Souza, 2005):

*Este é o meu entendimento, como designer, de **quem você, usuário, é**, do que aprendi que você **quer ou precisa fazer**, de **que maneiras prefere fazer**, e **porquê**. Este, portanto, é o sistema que projetei para você, e esta é **a forma como você pode ou deve utilizá-lo** para alcançar uma gama de objetivos que se encaixam nesta visão.*

O resultado do preenchimento do template de metacomunicação costuma ser utilizado para avaliar se há incoerências entre os diversos tipos de signos ou entre o design da aplicação e a proposta de seus desenvolvedores. Depois o avaliador deve contrastar e comparar as três metamensagens reconstruídas e avaliar se há consistência mútua; distribuição da carga de metacomunicação; e as estratégias/estilos de metacomunicação dos designers. Finalmente, na etapa final, julgar se a comunicabilidade do sistema é satisfatória. Em outras palavras, a pessoa avaliadora faz um diagnóstico se há pontos em que esta comunicação pode se interromper. Se houver: Ilustra e explica o problema; e Elabora recomendações de como corrigi-lo. (de Souza et al., 2006)

Antes da execução da inspeção no Instagram foi realizada uma inspeção preliminar no aplicativo da rede social para sistemas IOS e na sessão de ajuda do site com o objetivo de identificar partes da aplicação em que existe a necessidade de aplicar princípios éticos de privacidade. Foram identificadas três partes, cada uma correspondendo a um princípio ético, sendo eles consentimento informado, controle sobre o uso de dados e direito a restringir processamento de dados.

Foram então realizadas três inspeções, através de três cenários de interação que serão apresentados nas sessões seguintes, sendo utilizada a mesma conta do Instagram para todos. O e-mail utilizado no cadastro foi criado especificamente para este trabalho, nunca tendo sido utilizado anteriormente.

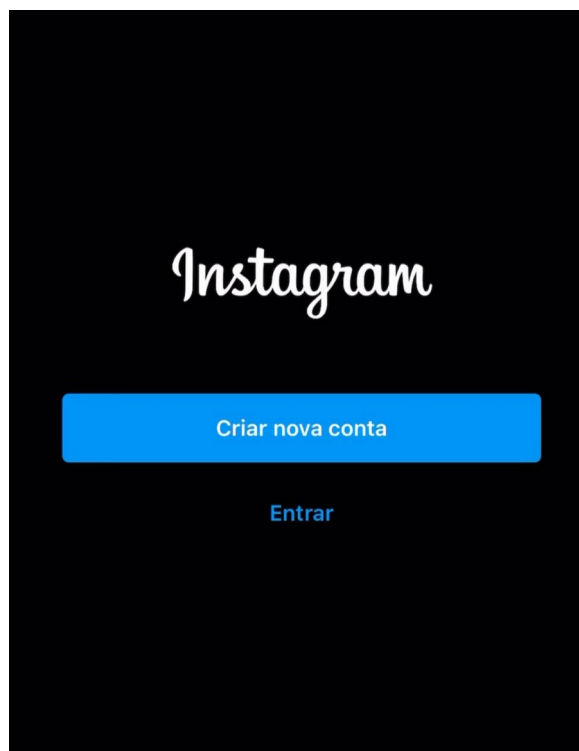
O perfil de usuário elaborado foi o de um adulto, com certa familiaridade com tecnologia. Para todos os cenários foi utilizada a seguinte persona: Luiza Torres tem 43 anos e é formada em Psicologia. Ela ama filmes de comédia e gosta de ouvir música. Ela não possui redes sociais e nunca utilizou o Instagram.

4.2.1. Consentimento Informado

Para este princípio foi elaborado o seguinte cenário: “ Sara tem 14 anos e gosta muito de ler livros e ver séries. Suas amigas frequentemente perguntam quando ela vai criar uma conta no Instagram. Então ela tem insistido muito e a várias semanas para que Luiza, sua mãe, a permita criar uma conta. Depois de tantos pedidos, Luiza decidiu pensar sobre o assunto e para tomar melhor essa decisão decidiu criar uma conta para si no aplicativo que sua filha baixou em seu celular.”

Neste cenário existe apenas uma tarefa a ser inspecionada: criar uma conta no Instagram através do aplicativo para sistemas IOS. Logo ao baixar o aplicativo é oferecida a opção de criar uma nova conta junto com a opção de fazer login com uma conta existente, como mostra a figura 1. O usuário deve clicar em “criar nova conta” para iniciar a tarefa.

Figura 1-Tela para criar conta



Fonte: Instagram.com

Analisando a distribuição dos signos nas interfaces apresentadas durante a inspeção da tarefa, nota-se uma predominância dos signos metalinguísticos em relação aos estáticos e dinâmicos. Durante toda a inspeção pequenas explicações são apresentadas, auxiliando o usuário. A tarefa de criação de conta é composta pelas seguintes ações: inserir e-mail ou telefone para cadastro, informar o código de confirmação, informar nome, informar data de nascimento, confirmar cadastro, escolher se conectar com o Facebook, escolher se conectar com a agenda, escolher receber notificações e avaliar as sugestões de perfis para seguir. Adicionalmente, foram consideradas as ações após a confirmação do cadastro como parte dessa tarefa, visto que são necessárias para que a pessoa usuária possa começar a utilizar o Instagram.

A realização de todas essas ações para a conclusão da tarefa de criação de contas é distribuída em diversas telas. Após a segunda etapa (inserir o código de confirmação) não é possível retornar a etapas anteriores.

Figura 2-Inserir e-mail para cadastro

The screenshot shows a dark-themed registration screen. At the top left is a back arrow. The title is "Insira o telefone ou email". Below it are two tabs: "Telefone" and "Email", with "Email" being the active tab. Under the "Email" tab is a text input field with the placeholder "Endereço de email". Below the input field is a blue button labeled "Avançar".

Fonte: Instagram.com

Figura 3- Inserir código de confirmação ao cadastrar-se

The screenshot shows a dark-themed registration screen. At the top left is a back arrow. The title is "Inserir código de confirmação". Below it is a paragraph: "Insira o código de confirmação que enviamos para luizacenariotcc@gmail.com. [Reenviar código.](#)". Below this is a text input field with the placeholder "Código de confirmação". Below the input field is a blue button labeled "Avançar". At the bottom is a numeric keypad with digits 1-9, 0, and a backspace icon.

Fonte: Instagram.com

Figura 4- Inserir data de nascimento ao cadastrar-se

The screenshot shows a dark-themed registration screen. At the top is a birthday cake icon with balloons. The title is "Adicione sua data de nascimento". Below it is a paragraph: "Isso não fará parte do seu perfil público. Por que preciso informar minha data de nascimento?". Below this is a date picker showing "1 de julho de 1977" and "44 anos". Below the date picker is a blue button labeled "Avançar". At the bottom is a calendar grid showing months and years. The selected date is "1 julho 1977".

Fonte: Instagram.com

Figura 5- Inserir nome no cadastro

Adicione seu nome

Adicione seu nome para que seus amigos possam encontrar você.

Nome completo

Avançar

q w e r t y u i o p
a s d f g h j k l
↑ z x c v b n m ↵
123 espaço seguinte
😊 🎤

Fonte: Instagram.com

Figura 6- Confirmar o cadastro

Cadastrar-se como luizacenariotcc?

Você poderá alterar seu nome de usuário depois.

Cadastre-se

[Alterar nome de usuário](#)

Ao tocar em Cadastre-se, você concorda com nossos Termos, com a Política de Dados e com a Política de Cookies.

Já tem uma conta? [Entrar.](#)

Fonte: Instagram.com

Figura 7- Encontrar amigos ao cadastrar-se



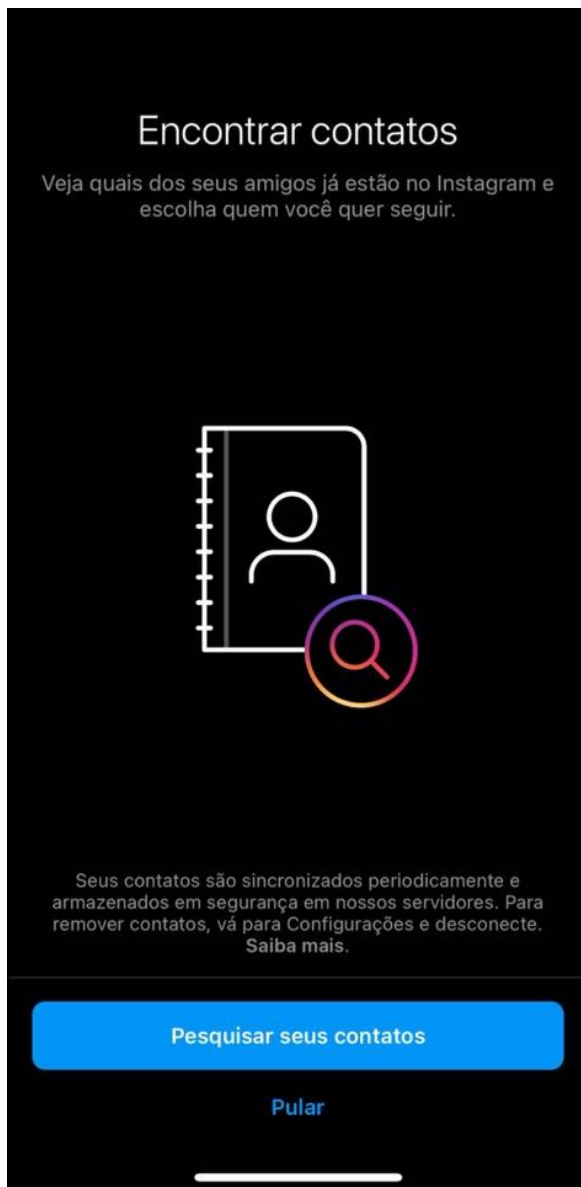
Fonte: Instagram.com

Figura 8- Encontrar amigos ao cadastrar-se após clicar em “pular”



Fonte: Instagram.com

Figura 9-Encontrar contatos ao cadastrar-se



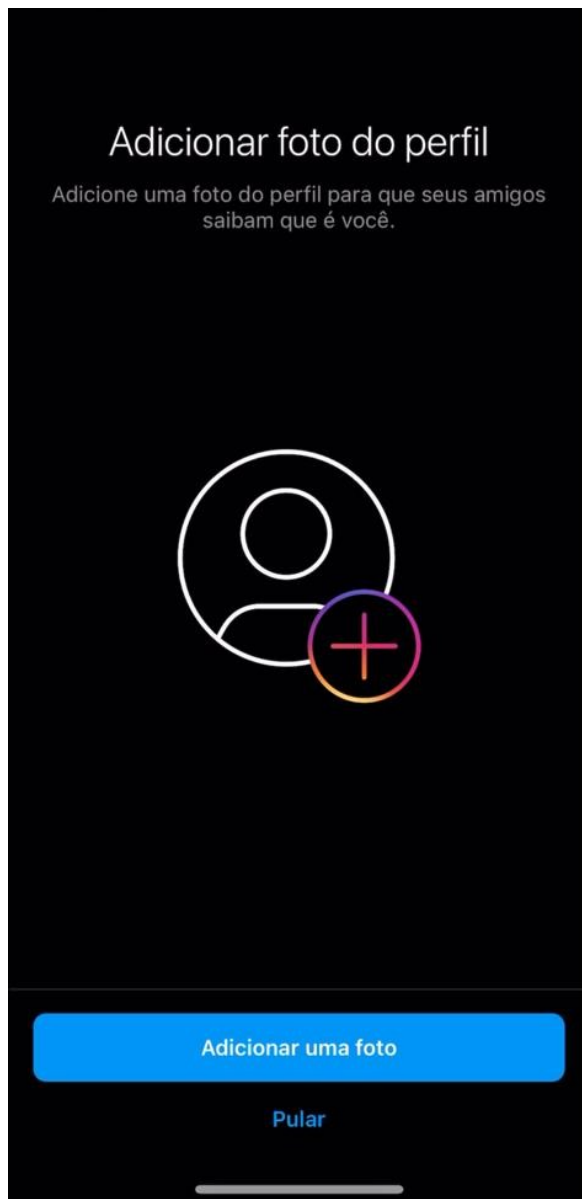
Fonte: Instagram.com

Figura 10-Encontrar contatos ao cadastrar-se depois de clicar em "pular"



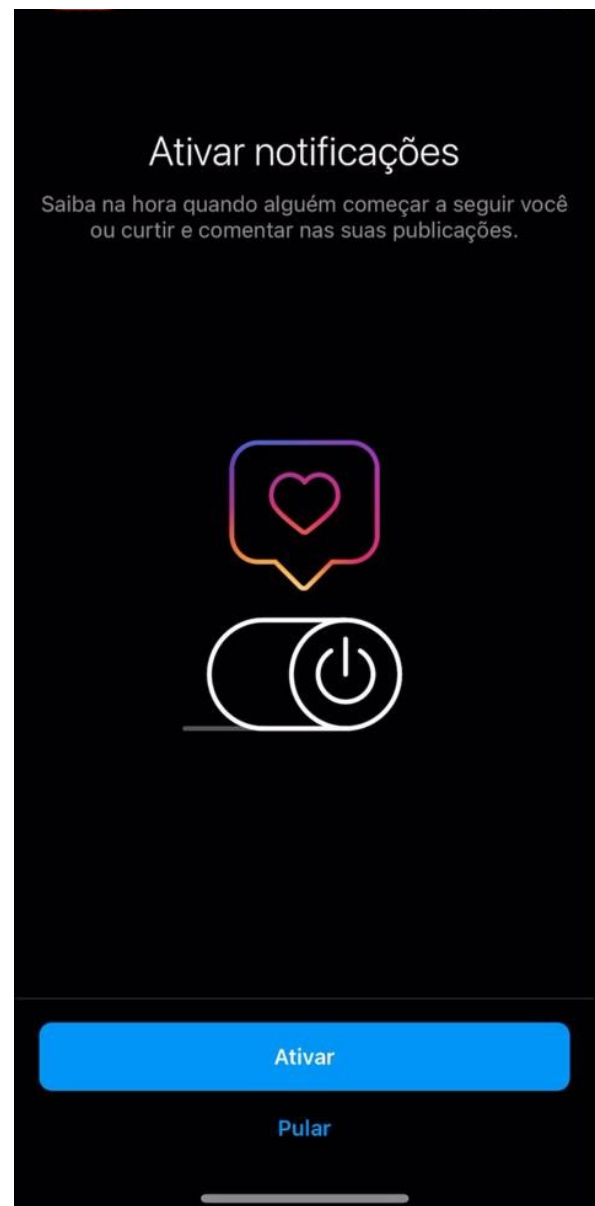
Fonte: Instagram.com

Figura 11-Adicionar foto ao perfil durante o cadastro



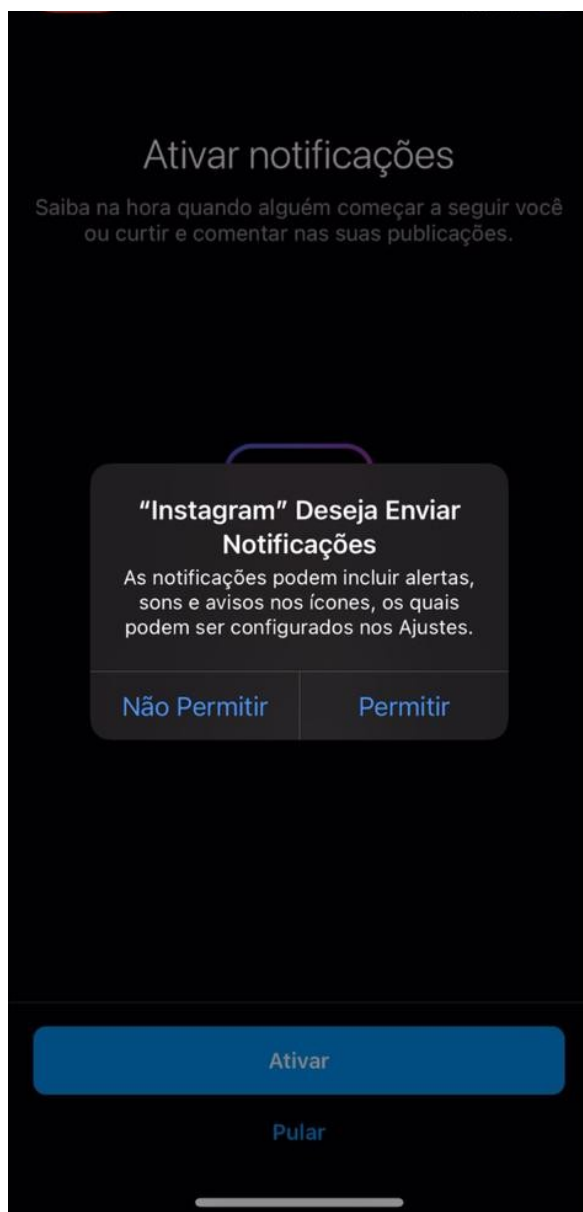
Fonte: Instagram.com

Figura 12-Ativar notificações durante o cadastro



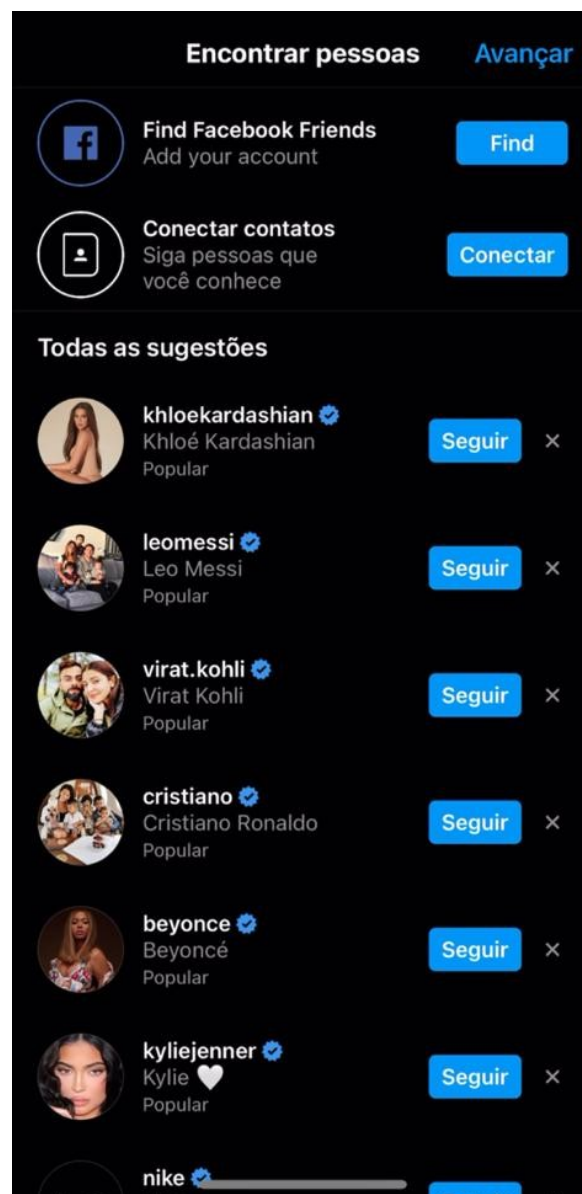
Fonte: Instagram.com

Figura 13- Ativar notificações depois de clicar em ativar



Fonte: Instagram.com

Figura 14- Sugestões de contas para seguir durante o cadastro



Fonte: Instagram.com

4.2.1.1. Reconstrução da Metacomunicação no Cenário 1

A seguir a reconstrução da metamensagem, começando pelos signos metalinguísticos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê:

Você gostaria de criar um cadastro, que pode ser particular, para sua empresa ou seu animal de estimação etc, e quer ter diferentes opções para fazê-lo. Você quer se divertir usando o aplicativo e também quer que seus amigos te encontrem. Você provavelmente tem uma conta no Facebook. Você quer uma confirmação das suas ações antes que elas sejam efetivadas.

Você deseja produtos personalizados que sejam únicos e relevantes para você além de uma experiência inovadora, relevante, consistente e segura.

Um usuário que declara ser maior de 13 anos e que nunca foi condenado por crimes sexuais, que deseja um conteúdo altamente personalizado e fortalecer seus relacionamentos com as pessoas e as coisas que você adora ao criar, encontrar, compartilhar, se comunicar e descobrir conteúdos do seu interesse em um ambiente seguro, inclusivo e positivo mas que não está disposto a pagar por isso .

Este é o sistema que fiz para você:

Seus amigos podem encontrar você através de seu nome e identificar pela sua foto. Já você pode encontrar seus amigos através do Facebook e da sua agenda telefônica, caso deseje. Outras pessoas podem te seguir, curtir e comentar suas publicações e você pode escolher ser notificado quando isso acontecer.

O sistema coleta o conteúdo, comunicações e outras informações que você ou que outras pessoas fornecem (compartilhamentos, comentários, mensagens etc) quando usam nossos Produtos, seja para para personalizar recursos e conteúdos, fazer sugestões a você e promover a segurança dentro e fora do Instagram. Quando você compartilha e se comunica usando o Instagram, você escolhe o público para aquilo que compartilha. Compartilhamos informações globalmente, tanto internamente nas Empresas do Facebook, quanto externamente com nossos parceiros e com aqueles com quem você se conecta, mas impomos fortes restrições sobre como nossos parceiros podem usar e divulgar os dados que fornecemos.

Um sistema gratuito que destaca conteúdos, recursos e contas que possam ser de seu interesse, além de oferecer formas de você experimentá-la.

Como funciona e como deve usá-lo:

Você pode se cadastrar utilizando telefone ou e-mail. Você deve inserir seu nome, sua data de nascimento e escolher um nome de usuário. Você pode inserir uma foto de perfil, seja da sua galeria, do seu Facebook ou tirá-la na hora. Caso permita acesso a sua agenda telefônica ela será sincronizada periodicamente e a permissão pode ser revogada a qualquer momento nas suas configurações.

Nossos sistemas processam automaticamente o conteúdo e as comunicações que você e outras pessoas fornecem a fim de analisar o contexto e o conteúdo. Você pode acessar e excluir as informações que coletamos. Dentre as informações coletadas sobre você estão informações sobre as pessoas, Páginas, contas, hashtags e grupos com que você se conecta e sobre como você interage com eles; o tipo de conteúdo que você visualiza ou com o qual se envolve; os recursos que você usa; as ações que você realiza; o tempo, frequência e duração das suas atividades e informações de e sobre dispositivos conectados à Web que você usa e que se integram aos nossos Produtos, e combinamos essas informações para, por exemplo, personalizar melhor o conteúdo (inclusive anúncios) ou os recursos que você observa quando usa nossos Produtos. Os anunciantes, desenvolvedores de aplicativos e *publishers* podem nos enviar por meio das Ferramentas do Facebook para Empresas informações sobre suas atividades fora do Facebook. Exigimos que cada um desses parceiros tenha autorização legal para coletar, usar e compartilhar seus dados antes de fornecê-los para nós. Combinamos as informações que temos sobre você para personalizar e aprimorar nossos Produtos e selecionar e personalizar anúncios, ofertas e outros conteúdos patrocinados que exibimos para você e para verificar contas e atividades, combater condutas danosas, detectar e prevenir spam e outras experiências negativas. O serviço é financiado através do trabalho com parceiros externos que nos ajudam a fornecer e a aprimorar nossos Produtos ou que usam as Ferramentas do Facebook para Empresas para ampliar os negócios. Não vendemos nenhuma de suas informações para ninguém e jamais o faremos. Concedemos a você a capacidade de acessar, retificar, portar e apagar seus dados. Em determinadas circunstâncias, você também tem o direito de contestar e restringir o tratamento de seus dados pessoais ou de revogar seu consentimento quando tratamos de dados fornecidos por você.

Sua experiência com o sistema é personalizada com base no que você e outras pessoas fazem dentro e fora do Instagram. Essas informações (dados pessoais, atividades e interesses) também são utilizadas por todos os Produtos das Empresas do Facebook (inclusive o Instagram) para fornecer serviços que sejam melhores e mais seguros e destacar anúncios e ofertas relevantes através dos quais o sistema é financiado.

Você não deve se passar por outras pessoas ou fornecer informações imprecisas; cometer ato ilícito, enganoso, fraudulento ou com finalidade ilegal durante o uso; vender, licenciar ou comprar contas; ou publicar informações privadas ou confidenciais de terceiros sem permissão nem fazer qualquer coisa que viole os direitos de outra pessoa, incluindo direito propriedade intelectual.

Continuando pelos signos estáticos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você busca uma interface minimalista e provavelmente gostaria de se conectar com seus amigos e saber quando interagirem com a sua conta. Você também quer que outras pessoas te identifiquem. Você provavelmente possui conta no Facebook. Você não se preocupa com seus dados e com os termos de uso (figura 6).

Este é o sistema que fiz para você.

Um sistema com interface simples em que você pode se conectar com seus amigos. Você também pode adicionar uma foto de perfil. Você pode escolher ser notificado quando interagirem com sua conta.

Como funciona e como deve usá-lo?

Você precisa inserir sua data de aniversário e você pode se conectar com outras pessoas através do Facebook e da sua agenda de contatos.

E por fim, a reconstrução da metamsagem dos signos dinâmicos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você deseja se conectar com outras pessoas, inclusive pessoas públicas. Você gosta de realizar tarefas em etapas.

Este é o sistema que fiz para você.

Um sistema em que você pode seguir e deixar de seguir pessoas. Ao se cadastrar você pode focar em uma etapa por vez.

Como funciona e como deve usá-lo?

Você tem duas formas de se cadastrar, precisa escolher um nome de usuário disponível e deve inserir sua data de nascimento para comprovar que tem idade para usar a rede. Ao se cadastrar, algumas sugestões de pessoas públicas para você seguir serão feitas .

4.2.1.2. Análise e Identificação de Estratégias de Design do Cenário 1

O usuário representado nesse cenário (a Luiza), pode ter interpretações errôneas na tela de inserir data de nascimento. Ao preenchê-la é informado ao usuário qual a sua idade, para título de conferência. Caso a idade seja menor que 6 anos ela aparece destacada em vermelho e a mensagem “Você precisa inserir sua data de nascimento” aparece abaixo do campo de preenchimento, diferentemente de para idade a partir dos 6 anos. Isso pode levar o usuário a acreditar que a idade mínima para o cadastro são 6 anos, quando na verdade a idade mínima é 13 anos. Uma solução para este problema seria mudar o destaque em vermelho para qualquer idade abaixo de 13 anos, ou desabilitar o botão de “avançar” caso a idade não seja válida. Exceto essa situação, os signos são consistentes com a intenção do design.

Existe uma redundância entre as metamensagens ao afirmarem que o Instagram é um sistema para conectar pessoas. Isso se justifica por ser uma rede social. Durante a execução da tarefa os signos estáticos e dinâmicos funcionam como um reforço ao que era comunicado pelos signos metalinguísticos. Por exemplo, na etapa “inserir a data de nascimento”, acima do título (signo metalinguístico) encontra-se a figura de um bolo de aniversário (signo estático) e no campo de preenchimento é possível visualizar a idade de acordo com a data preenchida (signo dinâmico). Contudo, não foram identificadas contradições entre as metamensagens.

Quanto ao uso de *Dark Patterns*, na etapa de confirmar cadastro (figura 6) pode ser notada a presença do *Dark Pattern Misdirection*. Os links para “Termos de uso”, “Política de Dados” e “Política de Cookies” ficam na parte inferior da página em letras menores e sem nenhum destaque, em oposição ao botão de “Cadastre-se” no topo da página em cor vibrante e chamando mais atenção em relação aos demais elementos.

4.2.2. Controle Sobre o Uso de Dados

Para este princípio foi elaborado o seguinte cenário: “Depois de alguns dias utilizando o Instagram, Luiza leu uma matéria sobre a coleta de dados feita pelas redes sociais. Ao descobrir que tem direito de acessar esses dados coletados, além de retificá-los e excluí-los, Luiza decide acessá-los, baixá-los e verificar se tem algo que deseja apagar.”

Neste cenário serão inspecionadas três tarefas: acessar dados, baixar dados e apagar dados. Antes de iniciar a inspeção foi necessário utilizar algumas funcionalidades do Instagram, como seguir outras contas, curtir e comentar publicações e reagir à *stories*. Essa necessidade surgiu para que houvesse dados a serem mostrados, baixados ou apagados durante a inspeção das tarefas.

Para realizar as tarefas através do aplicativo para sistemas IOS, inicialmente deve-se ir em configurações e depois em segurança. Desta forma a seguinte tela é mostrada.

Figura 15-Configurações de Segurança do Instagram



Fonte: Instagram.com

Para cumprir a primeira e a última tarefas seleciona-se a aba “Acessar dados” na seção “Dados e Histórico”, sendo necessário confirmar o login como mostra a figura 16. As figuras 17-21 mostram algumas telas da execução da tarefa.

Figura 16-Login para acessar dados



The image shows the Instagram login interface. At the top, there is a language selector set to 'Português (Brasil)'. The Instagram logo is prominently displayed in the center. Below the logo, there is a blue button with the Facebook icon and the text 'Continuar com o Facebook'. Underneath this, the word 'OU' is centered between two horizontal lines. This is followed by two input fields: the first is labeled 'Telefone, nome de usuário ou email' and the second is labeled 'Senha'. To the right of the password field is a link that says 'Esqueceu a senha?'. Below the input fields is a light blue button labeled 'Entrar'. At the bottom, there is a link that says 'Não tem uma conta? Cadastre-se'.

Português (Brasil) ▾

Instagram

 Continuar com o Facebook

OU

Telefone, nome de usuário ou email

Senha

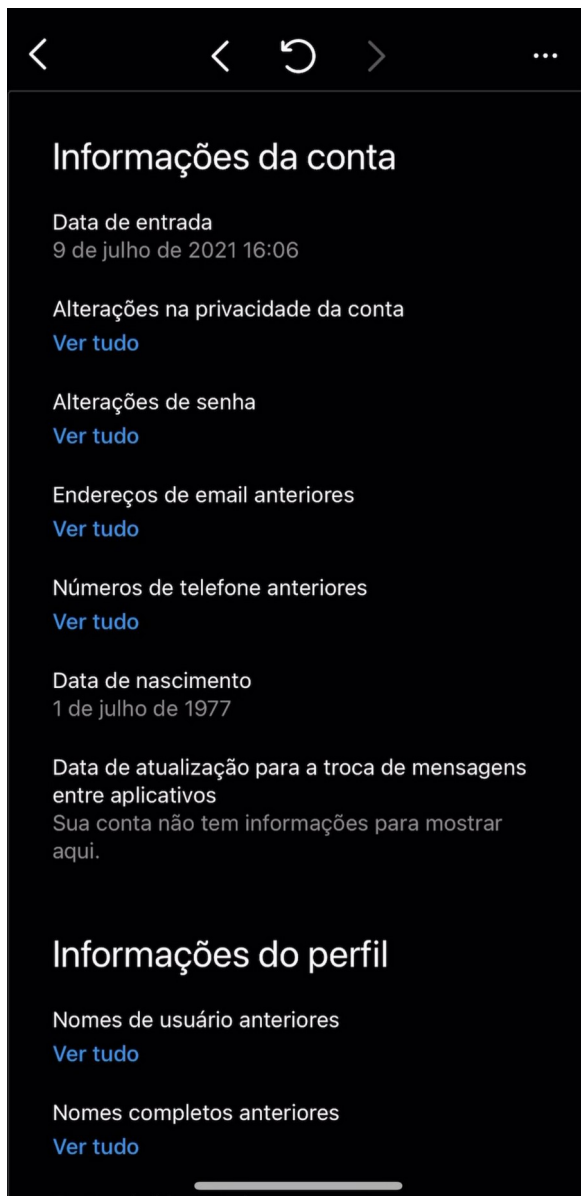
[Esqueceu a senha?](#)

Entrar

Não tem uma conta? [Cadastre-se](#)

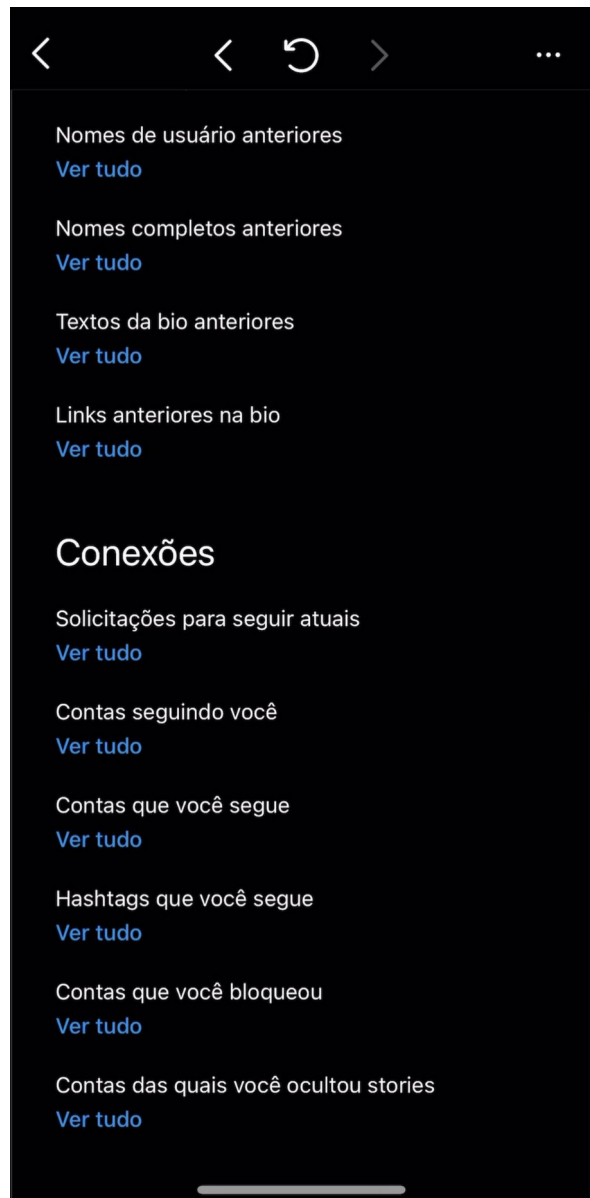
Fonte: Instagram.com

Figura 17-Primeira parte de acessar dados



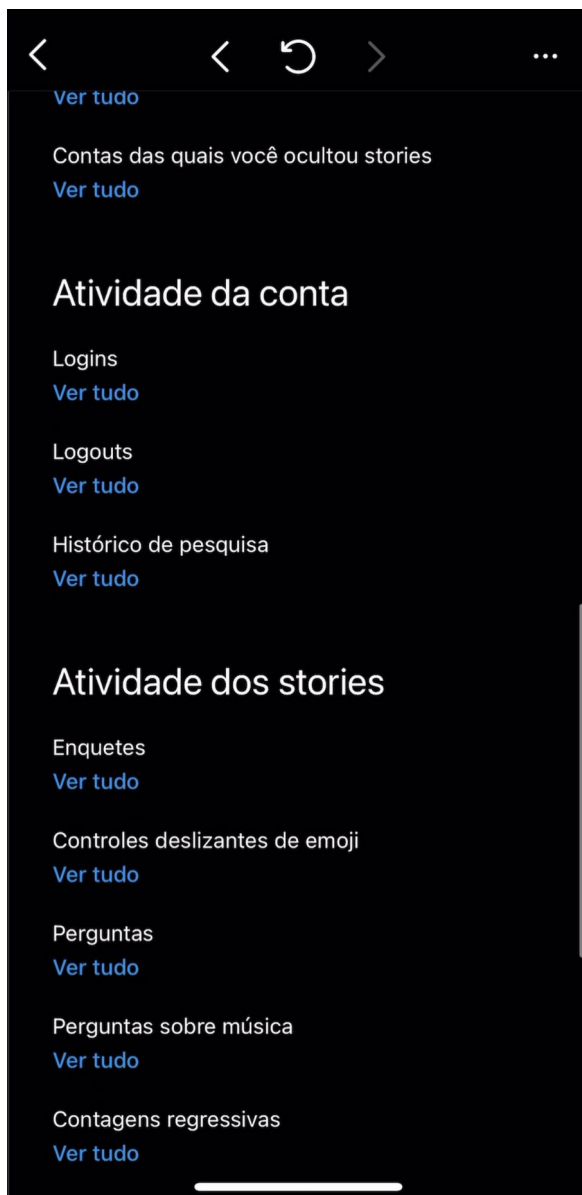
Fonte: Instagram.com

Figura 18-Segunda parte de acessar dados



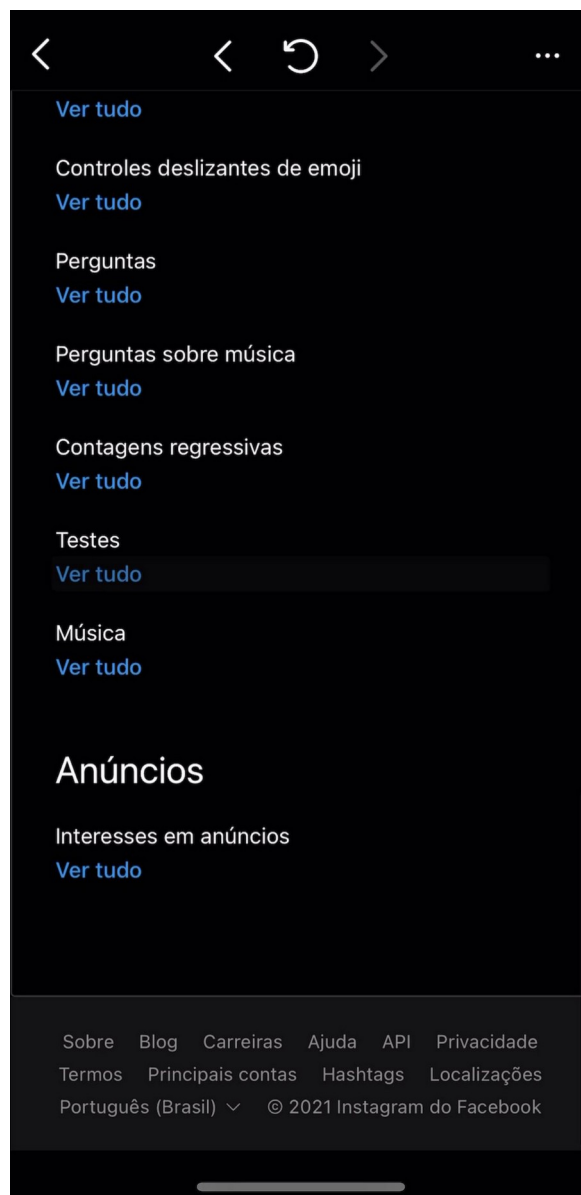
Fonte: Instagram.com

Figura 19-Terceira parte de acessar dados



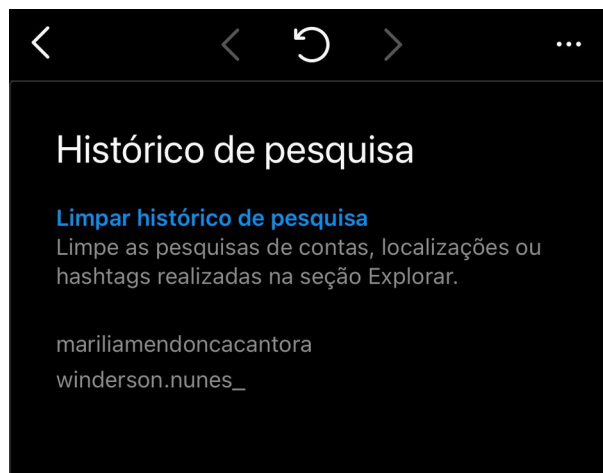
Fonte: Instagram.com

Figura 20-Quarta parte de acessar dados



Fonte: Instagram.com

Figura 21-Acesso aos dados de histórico de pesquisa



Fonte: Instagram.com

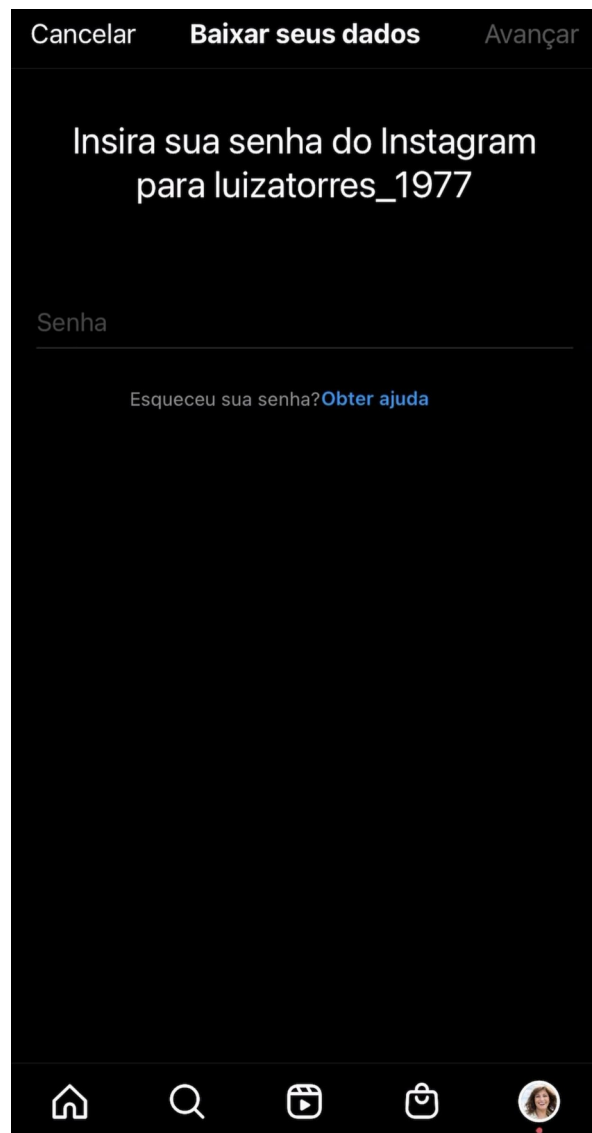
Para a segunda tarefa seleciona-se “Baixar dados”, na mesma sessão (figura 15). As figuras 22-24 representam as etapas dessa tarefa.

Figura 22-Solicitar download de dados



Fonte: Instagram.com

Figura 23-Inserir senha para download



Fonte: Instagram.com

Figura 24-Confirmação de solicitação de download



Fonte: Instagram.com

4.2.2.1. Reconstrução da Metacomunicação no Cenário 2

A seguir a reconstrução da metamensagem, começando pelos signos metalinguísticos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você é um usuário que se preocupa com os dados coletados sobre você e a segurança deles (figura 16, figura 23) além de querer acessá-los e controlá-los a qualquer momento. Você é prático e quer agilidade ao realizar tarefas.

Este é o sistema que fiz para você.

Um sistema em que você pode se conectar e/ou interagir com hashtags, outras contas e anúncios. Nele você pode baixar os seus dados e também visualizar alguns deles online.

Como funciona e como deve usá-lo?

Para visualizar o que você compartilhou no sistema, você deve inserir sua senha e esperar até 48 horas para que um link de download seja enviado para o seu e-mail. Alguns dados como atividade da conta e dos stories, conexões e informações da conta e do perfil você consegue visualizar fazendo login, sem precisar solicitar download. Você pode escolher salvar suas informações de login para não inseri-las novamente.

Em seguida a inspeção dos signos estáticos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você é um usuário que provavelmente possui conta no Facebook e se preocupa com a segurança de seus dados. Você gosta de ver informações organizadas em tópicos.

Este é o sistema que fiz para você.

Um sistema em que você pode acessar e fazer download de seus dados.

Como funciona e como deve usá-lo?

Para baixar seus dados é necessário inserir o e-mail para onde eles serão enviados e a senha de sua conta. Você pode excluir seu histórico de pesquisa, mas não os demais dados (figura 21).

E por fim a inspeção dos signos dinâmicos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você é uma pessoa que gosta de realizar tarefas em etapas e ver informações em listas.

Este é o sistema que fiz para você.

Um sistema que lhe fornece informações sobre você listadas e atualizadas com o tempo.

Como funciona e como deve usá-lo?

De acordo com a utilização do sistema as informações vão sendo alteradas ou acrescentadas nas listas.

4.2.2.2. Análise e Identificação de Estratégias de Design do Cenário 2

Há uma predominância dos signos metalinguísticos que são explicativos, fazendo com que não haja abertura para interpretações diferentes das idealizadas pelo design. Comparando as metamensagens nota-se uma leve redundância sobre a preocupação do usuário em relação à segurança dos dados coletados sobre si, o que é visto de forma positiva dentro do ponto de vista deste trabalho. Contudo, existe uma contradição dado que os signos metalinguísticos comunicam que o usuário quer controlar os seus dados, mas os estáticos afirmam que apenas os dados de histórico podem ser apagados.

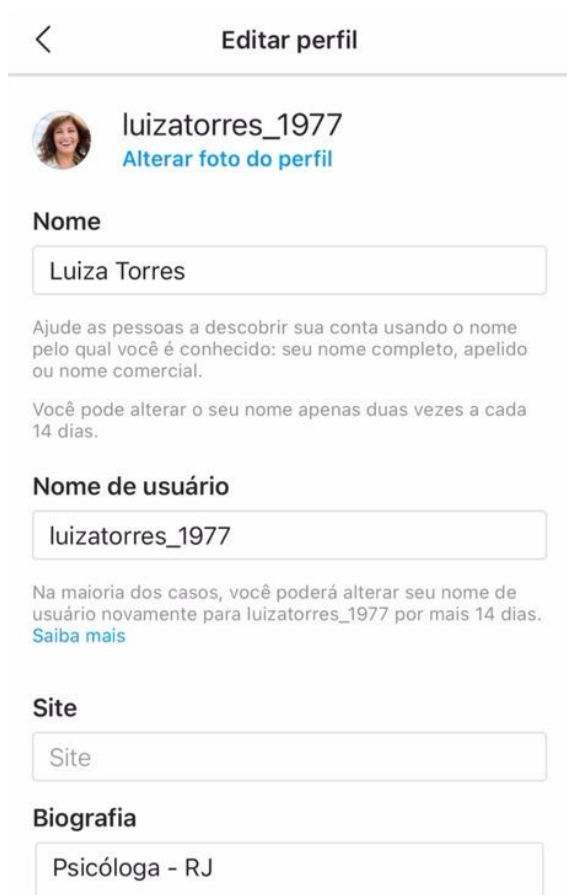
Essa contradição se relaciona com o Dark Pattern *Roach Motel*, visto que embora seja bastante fácil fornecer informações pessoais ao Instagram, o que é visível pela quantidade de dados disponíveis na sessão de “Acessar dados”, não é possível dizer o mesmo sobre desfazer essa ação e apagar os dados. Durante a execução da tarefa os únicos dados com a possibilidade de serem excluídos são os de histórico de pesquisa (figura 21). Ao buscar por “excluir” na seção de ajuda do Instagram, nenhum resultado diretamente relacionado a exclusão de dados é retornado. Fica subentendido que o usuário pode excluir seus dados ao apagar publicações e ao desfazer interações e que algumas informações como histórico de login e histórico de bio só seriam apagados com a exclusão da conta. Contudo, apenas 30 dias após a exclusão da conta que os dados começam a serem apagados.

4.2.3. Direito a Restringir Processamento de Dados

Para este princípio foi elaborado o seguinte cenário: “Na próxima semana, Luiza precisará realizar um concurso público para o CAPS de sua cidade. Para conseguir se concentrar melhor nos seus estudos decidiu dar uma pausa na utilização do Instagram. Para isso, ela gostaria de inativar a sua conta. “

Neste cenário existe apenas uma tarefa a ser inspecionada: inativar a conta. Para iniciar a tarefa, primeiro deve-se, através de um navegador, ir em editar perfil. Por fim, é preciso rolar até o final da página onde apresenta-se o link “Desativar minha conta temporariamente” (Figura 25,26).

Figura 25-Primeira parte de “Editar perfil”



Fonte: Instagram.com

Figura 26-Segunda parte de “Editar perfil”



Fonte: Instagram.com

Figura 27-Desativar conta

Desativar sua conta temporariamente

Olá, **luizatorres_1977**.

Você pode desativar sua conta em vez de excluí-la. Isso significa que sua conta ficará oculta até você reativá-la fazendo login novamente.

Só é possível desativar sua conta uma vez por semana.

Por que você está desativando sua conta?

Selecionar

Para continuar, insira a sua senha novamente

[Esqueceu a senha?](#)

Fonte: Instagram.com

Figura 28-Desativar conta porque segunda conta foi criada

Por que você está desativando sua conta?

Uma segunda conta foi criada

Verifique se você está conectado a essa segunda conta accidental para evitar a exclusão de sua conta principal. Você está conectado como **luizatorres_1977**. Se isso estiver incorreto, [primeiro saia](#) e entre com a conta correta.

Para continuar, insira a sua senha novamente

[Esqueceu a senha?](#)

Fonte: Instagram.com

Figura 29-Desativar conta por causa de anúncios em excesso

Por que você está desativando sua conta?

Anúncios em excesso

Mais sobre a publicidade no Instagram:

- Você é o proprietário de suas fotos e vídeos, ponto final. A publicidade não altera isso.
- Queremos mostrar a você anúncios de negócios que lhe sejam interessantes e relevantes. Saiba mais sobre como [O Instagram decide quais anúncios mostrar a você](#).

Para continuar, insira a sua senha novamente

[Esqueceu a senha?](#)

Fonte: Instagram.com

Figura 30-Desativar conta por outro motivo

Por que você está desativando sua conta?

Outro motivo

Para continuar, insira a sua senha novamente

[Esqueceu a senha?](#)

Fonte: Instagram.com

Figura 31-Desativar conta por precisar de um tempo

Por que você está desativando sua conta?

Preciso apenas dar um tempo

Para continuar, insira a sua senha novamente

[Esqueceu a senha?](#)

Fonte: Instagram.com

Figura 32-Desativar conta porque não consegue achar pessoas para seguir

Por que você está desativando sua conta?

Não consigo achar pessoas para seguir

Antes de desativar sua conta temporariamente, convém dar uma olhada nesses artigos na nossa Central de Ajuda.

- [Link para redes sociais](#)
- [Como usar hashtags](#)
- [Encontrar contas interessantes para seguir](#)

Fonte: Instagram.com

Figura 33-Desativar conta por questões de privacidade

Por que você está desativando sua conta?

Questões de privacidade

Antes de desativar sua conta temporariamente, convém dar uma olhada nesses artigos na nossa Central de Ajuda.

- [Quero bloquear um usuário](#)
- [Quero ter uma conta privada](#)
- [Desejo parar de seguir um usuário](#)
- [Minha conta foi invadida](#)

Fonte: Instagram.com

Figura 34-Desativar conta por problemas para começar

Por que você está desativando sua conta?

Problemas para começar

Antes de desativar sua conta temporariamente, convém dar uma olhada nesses artigos na nossa Central de Ajuda.

- [Dicas para começar](#)

Para continuar, insira a sua senha novamente

Fonte: Instagram.com

Figura 35-Desativar conta porque quer remover algo

Por que você está desativando sua conta?

Quero remover algo

Antes de desativar sua conta temporariamente, convém dar uma olhada nesses artigos na nossa Central de Ajuda.

- [Quero excluir um comentário que deixei](#)
- [Desejo parar de seguir um usuário](#)
- [Eu não quero que um usuário me siga](#)
- [Quero excluir uma foto que carreguei](#)
- [Desejo alterar meu nome de usuário ou informação da conta](#)

Fonte: Instagram.com

Figura 36-Desativar conta porque ocupa muito tempo

Por que você está desativando sua conta?

Ocupa muito do meu tempo/desvia muito a mi

Compreendemos que talvez você esteja muito ocupado para usar o Instagram e sugerimos que você remova o aplicativo do seu telefone seguindo essas etapas:

1. Encontre o aplicativo do Instagram.
2. Toque no ícone de aplicativo e mantenha pressionado por alguns segundos.
3. A tela vai começar a "agitar-se" e, depois, um "X" será exibido no ícone do aplicativo.
4. Toque no "X" e, na pergunta se deseja prosseguir, selecione "Excluir".

A remoção do aplicativo deverá dar a você a pausa que você procura. Todas as suas fotos e dados do perfil ainda serão salvos, mas você não receberá mais notificações push e poderá voltar a acessar sua conta quando quiser, reinstalando o Instagram.

Fonte: Instagram.com

Figura 37-Inserir senha para desativar prosseguir, selecione "Excluir".

A remoção do aplicativo deverá dar a você a pausa que você procura. Todas as suas fotos e dados do perfil ainda serão salvos, mas você não receberá mais notificações push e poderá voltar a acessar sua conta quando quiser, reinstalando o Instagram.

Para continuar, insira a sua senha novamente

[Esqueceu a senha?](#)

Quando você pressionar o botão abaixo, suas fotos, comentários e curtidas estarão ocultos até você reativar sua conta fazendo o login novamente.

Desativar conta temporariamente

Fonte: Instagram.com

Figura 38-Confirmar que quer desativar a conta

Para continuar, insira a sua senha novamente

••••••••••

Você está prestes a desativar sua conta temporariamente. Prosseguir?

Sim Não

Desativar conta temporariamente

Assim, suas fotos, vídeos e comentários ficarão ocultos até que você faça login novamente.

Fonte: Instagram.com

4.2.3.1. Reconstrução da Metacomunicação no Cenário 3

A seguir a reconstrução da metamensagem, começando pelos signos metalinguísticos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você é um usuário do sistema que gostaria de manter sua conta oculta temporariamente, mas apenas como última opção (Figuras 28,29,32-36). Você não deseja fazer isso com frequência (Figura 27). Você quer facilidade para voltar a utilizar o sistema.

Este é o sistema que fiz para você.

Um sistema em que você pode desativar temporariamente sua conta depois de ser informado de outras soluções.

Como funciona e como deve usá-lo?

Você só pode desativar sua conta uma vez por semana e para ativá-la novamente basta fazer login. Ao desativá-la suas fotos, comentários e curtidas ficarão ocultos até a reativação.

Em seguida, a reconstrução da metamensagem gerada pelos signos estáticos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você é um usuário que deseja manter sua conta oculta temporariamente (Figura 27) e se preocupa com a segurança ao fazê-lo (Figuras 37,38). Você não deseja fazer isso com frequência.

Este é o sistema que fiz para você.

Um sistema em que você pode desativar sua conta.

Como funciona e como deve usá-lo?

Você deve escolher um motivo e clicar em “desativar conta temporariamente”.

E por último, a reconstrução da metamsagem gerada pelos signos dinâmicos:

Quem você é, o que deseja/precisa fazer, de que formas preferenciais e por quê.

Você é uma pessoa que por diferentes motivos deseja como última opção ocultar sua conta. Você pode ter dúvidas sobre desejar ocultar sua conta. (Figuras 28,29,32-36)

Este é o sistema que fiz para você.

Um sistema que te informa opções à ocultação da conta de acordo com a sua motivação.

Como funciona e como deve usá-lo?

Você deve selecionar uma das opções de motivação para ver diferentes soluções antes de decidir pela desativação. Você precisa confirmar que deseja ocultar sua conta antes de desativá-la.

4.2.3.2. Análise e Identificação de Estratégias de Design do Cenário 3

Embora não tenham sido identificados signos que possam levar o usuário a interpretar erroneamente a mensagem do design, analisando as metamsagens nota-se que são contraditórias, visto que enquanto os signos estáticos apontam que o usuário deseja ocultar sua conta, os signos metalinguísticos e os signos dinâmicos apontam sistematicamente que ele só deseja isso como última opção

(principalmente ao selecionar o motivo para a desativação). Isso pode levar o usuário a se confundir durante a execução da tarefa, reconsiderando suas próprias intenções e inclusive desistindo de realizá-la.

Um ponto crítico no resultado da reconstrução das metamensagens é a afirmação “Você só pode desativar sua conta uma vez por semana e para ativá-la novamente basta fazer login”. Neste ponto está sendo comunicada a estratégia *Roach Motel*, tipo de *Dark Patterns*, já que, como a própria metamensagem afirma, é bem simples reativar a conta, basta fazer login. Contudo, é impossível desfazer a ação (desativar a conta) dentro de uma semana.

Outro fato a ser notado é que esta tarefa não pode ser realizada através do aplicativo, mas apenas de um navegador, mesmo que parte importante das funcionalidades do Instagram, como publicar um story, só possam ser utilizadas pelo aplicativo. Uma observação importante é que esta é a única funcionalidade presente em “Editar Perfil” do navegador que não está presente no aplicativo. Isso também pode se caracterizar como utilização da estratégia *Roach Motel*, já que a forma de desativar a conta é mais restrita (pode ser realizada apenas através de um navegador) em relação à forma de ativá-la.

4.3. DISCUSSÃO

Nesta seção retoma-se a pergunta problema apresentada no capítulo de Introdução: “O Instagram proporciona um relacionamento negativo com seus usuários pela falta de aplicação de princípios de privacidade? De que forma?”

Dado que o Instagram utilizou a estratégia *Misdirection* na tela de cadastro, o princípio de consentimento foi quebrado. Como dito no capítulo anterior, os links para “Termos de uso”, “Política de Dados” e “Política de Cookies” ficam no rodapé da página em posição oposta ao botão para se cadastrar. A própria mensagem responsável por informar ao usuário que ao continuar ele concorda com os termos de uso e com a política dados não está em destaque. Além do uso de *Misdirection*, não é necessária nenhuma ação para confirmar o consentimento, como selecionar

um checkbox ou responder um pop-up de confirmação, além de continuar com o cadastro. O usuário também deveria ter o direito de remover o consentimento a qualquer momento.

Pensando em consentimento informado, embora o Instagram tenha uma extensa política de dados, esta não informa exatamente quais são os dados coletados, apenas exemplificando alguns de forma vaga. Embora seja afirmado que o usuário tem possibilidade de apagar e retificar seus dados, não é informado evidentemente como isso pode ser feito. Ao longo de todo o documento não foram identificadas informações sobre os riscos dessa coleta de dados ou alternativas. Por fim, a política de dados do Instagram é extensa, o que é um problema, já que políticas de privacidade menores aumentam as chances de que os usuários a leiam e se informem (Meier, Schäwel & Krämer, 2020).

Com a utilização da estratégia *Roach Motel*, o princípio de controle sobre os próprios dados foi prejudicado, visto que ao acessar os próprios dados o usuário tem a possibilidade de apagar seu histórico de pesquisa, mas não os demais dados visualizados. Na política de dados do Instagram é informado que é concedido ao usuário “a capacidade de acessar, retificar, portar e apagar seus dados”. Porém, como dito anteriormente, ao buscar por “excluir” na seção de ajuda do Instagram, nenhum resultado diretamente relacionado a exclusão de dados é retornado. Fica subentendido que o usuário pode excluir seus dados com a exclusão de sua conta, contudo mesmo nesse caso, o processo de exclusão demora 30 dias para ser iniciado e poder levar até 90 dias. Buscando na sessão de ajuda por “retificar” nenhum resultado é retornado.

E por fim, com a utilização da estratégia *Roach Motel* novamente o princípio de direito de restringir processamento foi quebrado. Inicialmente, porque existe uma limitação de desativar a conta apenas uma vez por semana, ou seja, se o usuário tiver desativado e reativado sua conta dentro desse período ele não consegue mais exercer o seu direito de restringir o processamento de seus dados. Ademais, além da desativação da conta ser dificultada por ser realizada apenas através de um navegador, o usuário é constantemente desencorajado a realizar a tarefa, o que é uma quebra clara do princípio de direito a restringir o processamento de dados. Outras opções para restringir acesso aos dados poderiam ser dadas, como escolher

ver as postagens de contas que o usuário segue por ordem de publicação não utilizando assim a IA. Dessa forma poderia ser assegurada uma opção de restringir o processamento de dados sem ficar impossibilitado de utilizar o sistema.

5. CONCLUSÃO

Neste trabalho realizou-se uma avaliação na aplicação mobile para sistemas IOS da rede social Instagram com os objetivos de: a) identificar problemas de comunicabilidade do Instagram relacionados aos princípios éticos de privacidade; b) avaliar se o Instagram falha em promover um relacionamento ético com seus usuários; c) identificar rastros de *Dark Patterns* nas estratégias de comunicação dos princípios éticos.

Na primeira etapa do nosso estudo foi realizada uma inspeção preliminar na própria aplicação do Instagram em busca de pontos de encontro entre tarefas da aplicação e princípios éticos de privacidade. Foram encontrados pontos de encontro com os seguintes princípios éticos: consentimento, controle sobre o uso dos dados e direito a restringir processamento.

Na segunda etapa do estudo foi aplicado o Método de Inspeção Semiótica (de SOUZA et al., 2006) e identificados *Dark Patterns* com o objetivo de avaliar se os princípios éticos foram empregados e avaliar as estratégias de comunicação do Instagram. Foram encontrados problemas relacionados aos três princípios além de outros problemas de comunicabilidade no Instagram.

Finalmente, retomamos a pergunta problema apresentada no capítulo de introdução: “De que forma o Instagram proporciona um relacionamento negativo com seus usuários pela falta de aplicação de princípios de privacidade?” Os três princípios analisados neste trabalho foram quebrados, o que nos leva a concluir que sim, o Instagram proporciona um relacionamento negativo com seus usuários.

Resumidamente, as formas como o Instagram proporciona esse relacionamento negativo são (1) não garantindo o consentimento informado, visto que não fornece informações e condições suficientes para que o usuário tome uma decisão com ciência de todos os seus impactos e riscos; (2) dando a ilusão ao usuário de controle sobre os seus dados quando na realidade esse controle é bem restrito; e (3) não permitindo a livre decisão de não ter seus dados processados.

5.1. LIMITAÇÕES

Uma das limitações deste trabalho é a inexistência de estudos com a participação de usuários. Devido ao período em que o presente trabalho foi desenvolvido, durante a pandemia do COVID-19, a realização de estudos envolvendo outras pessoas foi dificultada.

Além disso, já que não existe a possibilidade de acesso aos algoritmos do Instagram, o estudo ficou limitado a explorar a comunicabilidade dos princípios éticos de privacidade através da interface.

Por fim estudar um sistema em constante mudança faz com que as conclusões formadas no presente trabalho não sejam definitivas, visto que os problemas apresentados podem ser solucionados e novos problemas podem surgir de acordo com as atualizações do sistema.

5.2. TRABALHOS FUTUROS

Um possível trabalho futuro seria aplicação do Método de Avaliação da Comunicabilidade (MAC) para que também seja analisada a recepção da mensagem, e não apenas a emissão, a fim de comparação com o presente trabalho. Dessa forma também seria possível ampliar o conhecimento sobre como os usuários interpretam a comunicação do Instagram em relação aos princípios éticos de privacidade.

Outro possível trabalho futuro seria repetir este estudo em outras redes sociais buscando violações a este ou outros princípios éticos, a fim de comparação com os resultados obtidos com o Instagram.

E por fim, um *survey* pode ser aplicado com usuários do Instagram para identificar as suas percepções sobre questões éticas e privacidade na rede social.

6. REFERÊNCIAS BIBLIOGRÁFICAS

AEPD. Agencia Espanola Proteccion Datos. **A Guide to Privacy by Design**, 2019.

AHLGREN, Matt. 40+ Instagram Statistics & Facts. WebsiteHostingRating. com, 2021. Disponível em: <https://www.websitehostingrating.com/research/instagram-statistics/>. Acesso em: 28 out. 2021.

AI, HLEG. High-level expert group on artificial intelligence. **Ethics guidelines for trustworthy AI**, 2019.<<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>>

BARBOSA, Simone; SILVA, Bruno. **Interação humano-computador**. Elsevier Brasil, 2010.

BRASIL. **Constituição** (1988). **Constituição** da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BINDU, T. Hima. Deducing Private Information from Social Network Using Unified Classification. **Journal of Science and Technology (JST)**, v. 2, n. 3, p. 41-46, 2017.

BOSTROM, Nick; YUDKOWSKY, Eliezer. The ethics of artificial intelligence. **The Cambridge handbook of artificial intelligence**, v. 1, p. 316-334, 2014.

CAVOUKIAN, Ann. Privacy by design. 2009.

CAVUSOGLU, Huseyin et al. Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. **Information Systems Research**, v. 27, n. 4, p. 848-879, 2016.

CHEN, Jilin et al. Understanding individuals' personal values from social media word use. In: **Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing**. 2014. p. 405-414.

BIER, Christoph; KÜHNE, Kay; BEYERER, Jürgen. PrivacyInsight: the next generation privacy dashboard. In: **Annual Privacy Forum**. Springer, Cham, 2016. p. 135-152.

DE CARVALHO, Juliano Varella et al. Inspeção semiótica e avaliação de comunicabilidade: identificando falhas de comunicabilidade sobre as configurações de privacidade do Facebook. **Anais Estendidos do XI Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais**, 2012, Brasil., 2012.

DE REZENDE XAVIER, Simone Isabela. Privacidade em redes sociais: uma análise da experiência dos usuários. 2014.

DOS SANTOS, Geanderson E.; BARBOSA, Marcelo W.; BARBOSA, Glívia AR. Caracterização das Estratégias de Privacidade do Instagram. In: **Anais do XIII Simpósio Brasileiro de Sistemas Colaborativos**. SBC, 2016. p. 31-45.

DE SOUZA, Clarisse Sieckenius. **The semiotic engineering of human-computer interaction**. MIT press, 2005.

DE SOUZA, C. et al. The Semiotic Inspection Method. In: **BRAZILIAN SYMPOSIUM ON HUMAN FACTORS IN COMPUTING SYSTEMS**, 7, 2006, Natal. New York: Association for Computing Machinery, p. 148-157, 2006.

DE SOUZA, Clarisse Sieckenius; LEITÃO, Carla Faria. Semiotic engineering methods for scientific research in HCI. **Synthesis Lectures on Human-Centered Informatics**, v. 2, n. 1, p. 1-122, 2009.

DWIVEDI, Yogesh K. et al. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. **International Journal of Information Management**, p. 101994, 2019.

FJELD, Jessica et al. Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. **Berkman Klein Center Research Publication**, n. 2020-1, 2020.

GRAY, Colin M. et al. The dark (patterns) side of UX design. In: **Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems**. 2018. p. 1-14.

Harry Brignull. 2010. Dark Patterns. Retrieved Sep 2, 2021 from <https://www.darkpatterns.org/>

KEMP, Simon. DIGITAL 2020: 3.8 billions people use social media. [S. l.], 30 jan. 2020. Disponível em: <https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media>. Acesso em: 10 de Dez. de 2020

KEMP, Simon. SOCIAL media users pass the 4 billions mark as global adoption soars.. [S. l.], 20 out. 2020. Disponível em: <https://wearesocial.com/blog/2020/10/social-media-users-pass-the-4-billion-mark-as-global-adoption-soars>. Acesso em: 10 de Dez. de 2020.

KIZZA, Joseph Migga et al. Ethical and social issues in the information age. London: Springer, 2007.

KOHN, Karen; MORAES, CH de. O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital. In: **XXX Congresso Brasileiro de Ciências da Comunicação**. 2007. p. 1-13.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. **Proceedings of the national academy of sciences**, v. 110, n. 15, p. 5802-5805, 2013.

LEWIS, Sarah. Qualitative inquiry and research design: Choosing among five approaches. **Health promotion practice**, v. 16, n. 4, p. 473-475, 2015.

LINDAMOOD, Jack et al. Inferring private information using social network data. In: **Proceedings of the 18th international conference on World wide web**. 2009. p. 1145-1146.

MAJEDI, Maryam; BARKER, Ken. The Privacy Policy Permission Model: A Unified View of Privacy Policies. **Trans. Data Priv.**, v. 14, n. 1, p. 1-36, 2021.

MEIER, Yannic; SCHÄWEL, Johanna; KRÄMER, Nicole C. The shorter the better? Effects of privacy policy length on online privacy decision-making. **Media and Communication**, v. 8, n. 2, p. 291-301, 2020.

MOONEY SJ, Pejaver v. Big data in public health: terminology, machine learning, and privacy. *Annu Rev Public Health* 2018; 39:95-112.

MOOR, James H. What is computer ethics?. **Metaphilosophy**, v. 16, n. 4, p. 266-275, 1985.

MORTIER, Richard et al. Human-data interaction: The human face of the data-driven society. **Available at SSRN 2508051**, 2014.

OHM, Paul. Broken promises of privacy: Responding to the surprising failure of anonymization. **Ucla L. Rev.**, v. 57, p. 1701, 2009.

ONU: Declaração Universal dos Direitos Humanos.
<https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>

RECUERO, Raquel. Considerações sobre a difusão de informações em redes sociais na internet. **Intercom Sul**, 2007.

RUSSELL, Stuart J.; NORVIG, Peter. Artificial Intelligence (A Modern Approach). 2010.

RYAN, Mark; STAHL, Bernd Carsten. Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. **Journal of Information, Communication and Ethics in Society**, 2020.

SANTORO, Flávia Maria; DA COSTA, Rosa Maria E. Moreira. Towards Ethics in Information Systems. **Journal on Interactive Systems**, v. 12, n. 1, p. 69-82, 2021.

TERTO, Ana et al. Imagem e privacidade: contradições no Facebook. In: **Relatórios da Competição de Avaliação do XI Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais**. 2012. p. 24.

THOMAS, Erl. Big data fundamentals: concepts, drivers & techniques. 2016.

UNESCO. As pedras angulares para a promoção de sociedades do conhecimento inclusivas: acesso à informação e ao conhecimento, liberdade de expressão, privacidade e ética na internet global. Paris, França: UNESCO, 2017.
(<https://unesdoc.unesco.org/ark:/48223/pf0000260742>)

VIANNA, Tulio. Transparência pública, opacidade privada. **Rio de Janeiro: Revan**, 2007.

WANG, Yilun; KOSINSKI, Michal. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. **Journal of personality and social psychology**, v. 114, n. 2, p. 246, 2018.

ZHELEVA, Elena; GETOOR, Lise. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In: **Proceedings of the 18th international conference on World wide web**. 2009. p. 531-540.