Estratégias de comunicação do Consentimento Informado e rastros de Padrões Obscuros no Instagram

Patrícia Raposo Santana Lima[1], **Luciana Cardoso de Castro Salgado**[1]

[1]Instituto de Computação – Universidade Federal Fluminense (UFF)
Niterói, Rio de Janeiro, Brasil

patriciaraposo@id.uff.br, luciana@ic.uff.br

Abstract. *Research has warned about the risks of new technologies with enormous computational and processing power if combined with the large volume of data arising from the increasing use of social networks. One of the risks is about the privacy and the ownership of personal data. This study investigated the Instagram social network communicability regarding the informed consent process. We applied the Semiotic Inspection Method to seek strategies to communicate this ethical principle of privacy. Results indicate the presence of Dark Patterns and violations of the ethical privacy principle related to consent.*

Resumo. *Pesquisas têm alertado sobre riscos de novas tecnologias com enorme poder computacional e de processamento se aliadas ao grande volume de dados advindos da crescente utilização de redes sociais. Um dos riscos está relacionado a privacidade e a propriedade dos dados pessoais. Este trabalho investigou a comunicabilidade do Instagram com o objetivo de identificar as estratégias de comunicação desta rede social sobre o consentimento informado. Para isso, aplicamos o Método de Inspeção Semiótica, um método com foco na avaliação da comunicabilidade de sistemas interativos. Os resultados indicam violações do princípio ético de privacidade relacionado ao consentimento e a presença de Padrões Obscuros nas estratégias de comunicação do Instagram.*

1. Introdução

De acordo com Recuero (2007) uma rede social é definida como o conjunto de atores da rede (pessoas, instituições ou grupos) e suas conexões por meio da Internet intermediadas por dispositivos e computadores. Segundo levantamento realizado pela WeAreSocial[1], uma agência de marketing digital especializada em mídias sociais, em parceria com GlobalWebIndex[2] e App Annie[3], em 2022, 58.4% da população mundial relatou utilizar redes sociais. O gasto médio de acessos diários é de 3 horas e 31 minutos [Kemp 2022]. Se em 2019 o número de usuários de redes sociais era de 3.8 bilhões, em outubro de 2020 era de 4.14 bilhões de usuários [Kemp 2020] e em janeiro de 2022 alcançamos a marca de 4.62 bilhoes de usuários ativos [Kemp 2022]. O Instagram[4], por exemplo, identificado como favorito por 14.8% dos usuários globais da internet [Kemp 2022], possui mais de 1 bilhão de usuários ativos mensalmente e 500 milhões de usuários ativos diariamente. Com isso,

[1]https://wearesocial.com/
[2]https://www.gwi.com/
[3]https://www.appannie.com/en
[4]https://www.instagram.com

são mais de 4.2 bilhões de *"likes"*, 100 milhões de uploads de fotos e 400 milhões de "stories" por dia. [Ahlgren, 2021]

Lançado em outubro de 2010 e pertencente a Meta Inc.[5], 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 destes 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 conversar de forma privada e enviar fotos e vídeos que ficam indisponíveis após uma ou duas visualizações, de acordo conforme 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.

Pesquisas têm alertado que a aplicação de relacionamentos entre dados, incluindo os oriundos da utilização de redes sociais, pode acarretar inferência ou descoberta de informações privadas [Rocasolano 2022]. Mesmo dados anônimos podem ser re-identificados e atribuídos a indivíduos específicos [Ohm 2009]. Além disso, através de diferentes tipos de dados como textos [Chen et al. 2014], imagens [Wang and Kosinski 2018], e inclusive *"likes"* [Kosinski et al. 2013], informações como gênero, sexualidade, dentre outras, podem ser deduzidas por meio de técnicas de Inteligência Artificial (IA) [Bindu 2017]. Apesar de existirem políticas de privacidade e termos de uso com as quais os usuários precisam consentir antes de utilizar um determinado sistema, 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 and Barker 2021][de Almeida and de Castro Salgado 2019].

Essa problemática se relaciona a uma potencial violação dos princípios éticos de privacidade [Fjeld et al. 2020], visto que, através de um consentimento prejudicado por falta de informação disponível aos usuários, há uma maior produção e disponibilidade de dados que podem ser utilizados por esses sistemas. Este trabalho tem como objetivo avaliar a comunicabilidade do Instagram sobre um princípio de privacidade relacionado ao consentimento informado e identificar se há rastros do uso de Padrões Obscuros em alguma das estratégias de comunicação de princípios éticos no Instagram.

O princípio de privacidade relacionado ao consentimento informado foi escolhido por conveniência, visto que se encaixa em cenários de uso do Instagram que podem ser verificados por meio da utilização da aplicação, sem acesso a seus algoritmos. A coleta de dados foi feita por meio de pesquisa qualitativa preditiva [Lewis 2015] com a aplicação do Método de Inspeção Semiótica (MIS) [de Souza and Leitão 2009], dado que o critério para a análise dos resultados não é numérico e depende de interpretação crítica e subjetiva das pesquisadoras.

Este trabalho está organizado da seguinte forma: detalhamos a fundamentação teórica na Seção 2. A Seção 3 discute os trabalhos relacionados. Na Seção 4, apresentam-se e discutem-se os resultados do MIS. Na Seção 5, as conclusões e trabalhos futuros.

[5]https://about.facebook.com/meta/

2. Fundamentação Teórica

2.1. Conceituação

A privacidade é um direito fundamental garantido pela Declaração Universal dos Direitos Humanos [ONU 1948], 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.5°, 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".

O direito à privacidade reveste-se de interesse não apenas individual, mas também e principalmente de interesse público [Vianna 2007]. 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 por exmeplo: o Regulamento Geral sobre a Proteção de Dados (GDPR) (UE)2016/679, em proteção a todos os indivíduos na União Europeia; 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.

A privacidade 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 [Kizza 2003]. Considerando esses três pontos (identidade pessoal, autonomia e relações sociais) como seus atributos, Kizza (2003) classifica a privacidade em três diferentes tipos: privacidade pessoal, que envolve nada nem ninguém se envolver ou se intrometer no espaço pessoal alheio; privacidade institucional, que envolve a proteção de dados privados de instituições e organizações; e privacidade da informação, a mais relacionada ao presente trabalho, que envolve a proteção de quaisquer informações relacionadas a algum indivíduo, seja ela pessoal, financeira, médica, digital, dentre outros.

Dentre as violações da privacidade levantadas por Kizza (2003) estão a intrusão (como quando *hackers* invadem um sistema); o mal uso da informação (coleta de informações para uso não autorizado); a intercepção 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).

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 [Fjeld et al. 2020]. A questão da privacidade, contudo, não aparece apenas em relação à utilização desses sistemas, mas também durante o seu desenvolvimento e treinamento dos modelos de IA [Fjeld et al. 2020]. A GDPR determina [European Union 2016], Art. 25, que o *Privacy by Design (PbD)* é obrigatório. Com a adoção do *PbD* 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 da tecnologia, 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 seus impactos antes mesmo que eles ocorram; (2) "Privacidade como Configuração padrão", ou seja, a garantia de que dados pessoais são automaticamente protegidos o máximo possível em qualquer sistema, sem a necessidade de que o individuo tome ação para isso; (3) "Privacidade incorporada ao design", o que implica que a privacidade é considerada um requisito não-funcional; (4) "Funcionalidade total", ou seja, a privacidade deve ser incorporada de forma que não comprometa a plena funcionalidade do sistema, não competindo com outros interesses legítimos; (5)"Segurança de ponta a ponta"; ou seja, o PbD se aplica a todo ciclo de vida dos dados envolvidos; (6) "Visibilidade e Transparência", o sistema deve poder ser sujeito a verificações; e (7)"Respeito pela privacidade do usuário", que pressupõe o máximo prezo pelos interesses do usuário. [Cavoukian 2009]

A Comissão Europeia de Peritos de Alto Nível sobre a IA (HLEGAI) conceitua sistemas de IA como sistemas de software (e eventualmente de hardware) que atuam percepcionando 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 [HLEGAI 2019]. Princípios Éticos de IA são diretrizes criadas para fixar regras e recomendações com o objetivo de promover que sistemas que utilizam 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 foi explorado no Instagram o princípio de consentimento, contido no princípio ético de privacidade [Fjeld et al. 2020].

Ética em computação envolve a análise da natureza e do impacto social das tecnologias computacionais e a formulação de políticas pessoais e sociais para o uso ético dessas tecnologias [Moor 1985]. Existe uma lacuna política sobre 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. [Moor 1985]

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 da 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 ao 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]

Segundo Brignull (2010), Padrões Obscuros são truques usados em sites e aplicativos que levam o usuário a fazer coisas que ele não pretendia realmente. Ou seja, Padrões Obscuros 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]. Eles são importantes 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.

Dentre os tipos de Padrões Obscuros definidos por Brignull está o *Misdirection* , 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].

2.2. Método de Inspeção Semiótica

Fundamentado na Engenharia Semiótica [de Souza 2005], o MIS avalia a comunicabilidade de um sistema interativo por meio da inspeção [de Souza et al. 2010] da metacomunicação do designer codificada na interface [Barbosa and Silva 2010]. A engenharia semiótica vê a interação humano-computador como um caso particular de metacomunicação designer-usuário. [de Souza and Leitão 2009] e considera a interface como representante de seus projetistas. Por meio do MIS é identificar quem é o usuário pretendido pelos projetistas, o que eles querem fazer, de que formas e porquê, 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."

Antes da inspeção o avaliador identifica quais são os perfis de usuários da aplicação e seus objetivos nela, para a partir disso definir o foco da avaliação, o escopo da inspeção e os cenários de interação [de Souza 2005].

O método consiste em reconstruir a metamensagem emitida pelo *design* através da inspeção de signos metalinguísticos, estáticos e dinâmicos, um tipo por vez. Signos estáticos são aqueles que expressam um estado do sistema e não dependem de relações causais ou temporais, como imagens e ícones, podendo ser capturados por fotografias ou screenshots, por exemplo. Já os signos dinâmicos expressam e significam o comportamento do sistema e são melhor capturados através de gravações e da interação continua com o sistema, como uma barra de progresso ou as cores de um menu que mudam de acordo com a aba selecionada. E por sua vez, signos metalinguísticos são os que explicam os outros signos do sistema, seja através de legendas, mensagens de erros, documentos, sessão de ajuda, entre outros. [de Souza et al. 2006]

Depois de reconstruir as três metamensagens, o avaliador deve contrastá-las e compará-las a fim de avaliar incoerências entre os diversos tipos de signos ou entre o *design* da aplicação e a proposta de seus desenvolvedores; a 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 ou se há pontos em que esta comunicação pode se interromper. Se houver, explica o problema e elabora recomendações de como corrigi-lo [de Souza et al. 2006].

3. Trabalhos Relacionados

Encontramos em uma revisão bibliográfica alguns trabalhos que exploraram a perspectiva de Design e utilizaram o MIS no processo de avaliação. No estudo de Coopamootoo e Ashenden (2011) os princípios de gerenciamento de privacidade de comunicação (CPM) são usados dentro da inspeção semiótica para examinar os mecanismos de privacidade online. Eles descobriram que a privacidade como um processo de comunicação viola muitos dos princípios do CPM. Concluiram, portanto, que isso pode explicar por que os usuários finais não interagem eficazmente com os mecanismos de privacidade online.

Já o trabalho de De Rezende Xavier (2014) aponta diversas questões em que as redes sociais online não atendem as necessidades de seus usuários e que estratégias eles têm utilizado para contornar essas situações. Para isso, foram realizadas entrevistas e questionários para identificar as principais questões a partir da experiência do usuário. Depois foi feita uma inspeção no Facebook e as decisões de interação que contribuem para os problemas foram discutidas.

O estudo de Dos Santos et al. (2016) buscou avaliar a interface do Instagram para identificar e caracterizar a proposta de privacidade do sistema. Utilizando o MIS, tentaram 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 os usuários nem sempre percebem ou utilizam os recursos disponíveis por meio das configurações oferecidas.

O estudo de Brito do Rêgo e Sampaio (2017), realizado no Facebook, buscou entender como está sendo assegurada a privacidade dos dados dos usuários, já que um dos propósitos do Facebook é, na verdade, a exposição dos dados dos usuários. Para analisar esta questão, foram utilizados dois métodos de avaliação: Método de Inspeção Semiótica (SIM) e Método de Avaliação da Comunicabilidade (CEM). Concluiram que o Facebook tem uma preocupação real com as informações de seus usuários, porém, em alguns casos, eles não estão recebendo essa mensagem de acordo. Como resultado, embora os usuários entendam os riscos da falta de privacidade, eles geralmente não sabiam como usar as ferramentas do Facebook para garantir sua privacidade.

Por último, a pesquisa de Barreto e colegas aplicou o MIS e identificou estratégias de comunicação que habilitam ou restringem a tomada de decisões das pessoas em sistemas que promovem a transparência no uso de dados pessoais. Algumas das estratégias envolvem a emissão de alertas para as ações dos usuários e a disponibilização de meios para os usuarios reportarem problemas.[Barreto et al. 2018a] [Barreto et al. 2018b]

O principal diferencial do presente trabalho em relação aos demais é que estes citam e analisam os mecanismos de controle de privacidade disponíveis, enquanto o pre-

sente trabalho buscou avaliar a privacidade de um usuário em relação ao próprio sistema e a adoção do princípio de consentimento.

4. Inspeção Semiótica do Instagram

Na etapa de preparação foi realizada uma inspeção preliminar no aplicativo para identificar partes da aplicação aderentes aos princípio ético de privacidade para o consentimento. Foram definidos uma persona e um cenário de interação para uma tarefa. A persona definida é a Luiza Torres, mulher de 43 anos, formada em Psicologia. Ela tem certa familiaridade com tecnologia, ama filmes de comédia e gosta de ouvir música. Ela não possui redes sociais e nunca utilizou o Instagram. o cenário de interação é: "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. Após 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."

A inspeção foi realizada entre março e julho de 2021 autoras do trabalho, em conjunto, sendo uma avaliadora de nível júnior e a outra uma avaliadora de nível especialista. O estudo foi realizado quando o Instagram pertencia ao Facebook Inc., antigo nome da Meta Inc. No contexto da tarefa de criar uma conta no Instagram, ao entrar pela primeira vez no aplicativo é oferecida a opção de criar uma nova conta junto com a opção de fazer login com uma conta existente. O usuário deve clicar em "criar nova conta" para iniciar a tarefa.

Durante a inspeção, 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.

4.1. Reconstrução da metacomunicação no cenário

Esta seção apresenta as metamensagens resultantes da etapa de análise segmentada dos signos estáticos, dinâmicos e metalinguísticos.

Metacomunicação com signos metalinguísticos:

Eis quem os projetistas do Instagram pensam que o usuário é, o que deseja/precisa fazer, de que formas preferenciais e porquê: *Um usuário 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. Você quer criar um*

cadastro para você, sua empresa ou seu animal de estimação 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. Você não gostaria que suas informações fossem coletadas, usadas ou compartilhadas sem autorização, ou vendidas para alguém. Você gostaria de ter controle sobre os seus dados.

Este é o sistema que fiz para você: *Um sistema gratuito que destaca conteúdos, recursos e contas que possam ser de seu interesse, além de oferecer formas de você experimentá-la, a partir de informações coletadas por ele ou por terceiros sobre você. Seus amigos podem te encontrar através de seu nome e te 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. 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. Você pode acessar e excluir as informações que coletamos. 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.*

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. Quando você compartilha e se comunica usando o Instagram, você escolhe o público para aquilo que compartilha. Nossos sistemas processam automaticamente o conteúdo e as comunicações que você e outras pessoas fornecem a fim de analisar o contexto e o conteúdo. Ele coleta o conteúdo, comunicações e outras informações que você ou que outras pessoas fornecem (compartilhamentos, comentários, mensagens etc) quando usam nossos Produtos para personalizar recursos e conteúdos, fazer sugestões a você e promover a segurança dentro e fora do Instagram. 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 vê 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. 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. Exigimos que cada um desses parceiros tenha autorização legal para coletar, usar e compartilhar seus dados antes de fornecê-los para nós.Combinamos as informa-*

ções que temos sobre você para personalizar e aprimorar nossos Produtos e selecionar e personalizar 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. 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 a propriedade intelectual.

Metacomunicação com signos estáticos:

Eis quem os projetistas do Instagram pensam que o usuário é, o que deseja/precisa fazer, de que formas preferenciais e porquê: *Uma pessoa com pelo menos 6 anos que 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. A forma como são utilizados os seus dados e os termos de uso do sistema não são de grande importância para você.*

Este é o sistema que fiz para você: *Um sistema com interface simples para você 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 deve inserir sua data de aniversário e pode usar o Facebook e sua agenda de contatos pata se conectar com outras pessoas.*

Metacomunicação com signos dinâmicos:

Eis quem os projetistas do Instagram pensam que o usuário é, o que deseja/precisa fazer, de que formas preferenciais e porquê: *Uma pessoa com pelo menos 6 anos que gosta de realizar tarefas em etapas e deseja se conectar com outras pessoas, inclusive pessoas públicas.*

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

4.2. Análise e identificação das estratégias de comunicação

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 em geral funcionam como um reforço ao que é 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 conforme a data preenchida (signo dinâmico). Há uma contradição direta entre as metamensagens em relação à idade mínima para utilização do sistema. Enquanto os signos metalinguísticos comunicam que a idade mínima para utilizar o Instagram é treze anos, as metamensagens dos signos estáticos e dinâmicos comunicam que a idade mínima é seis anos.(Figura 1)

Além disso, foi identificada uma contradição indireta entre as metamensagens reconstruídas a partir dos signos estáticos e metalinguísticos. Enquanto os signos estáticos comunicam "A forma como são utilizados os seus dados e os termos de uso do sistema não são de grande importância para você"os signos metalinguísticos os contradizem, comentando durante boa extensão da metamensagem reconstruída sobre coleta e uso de dados, com destaque para o trecho "Você não gostaria que suas informações fossem coletadas, usadas ou compartilhadas sem autorização ou vendidas para alguém. Você gostaria de ter controle sobre os seus dados.".

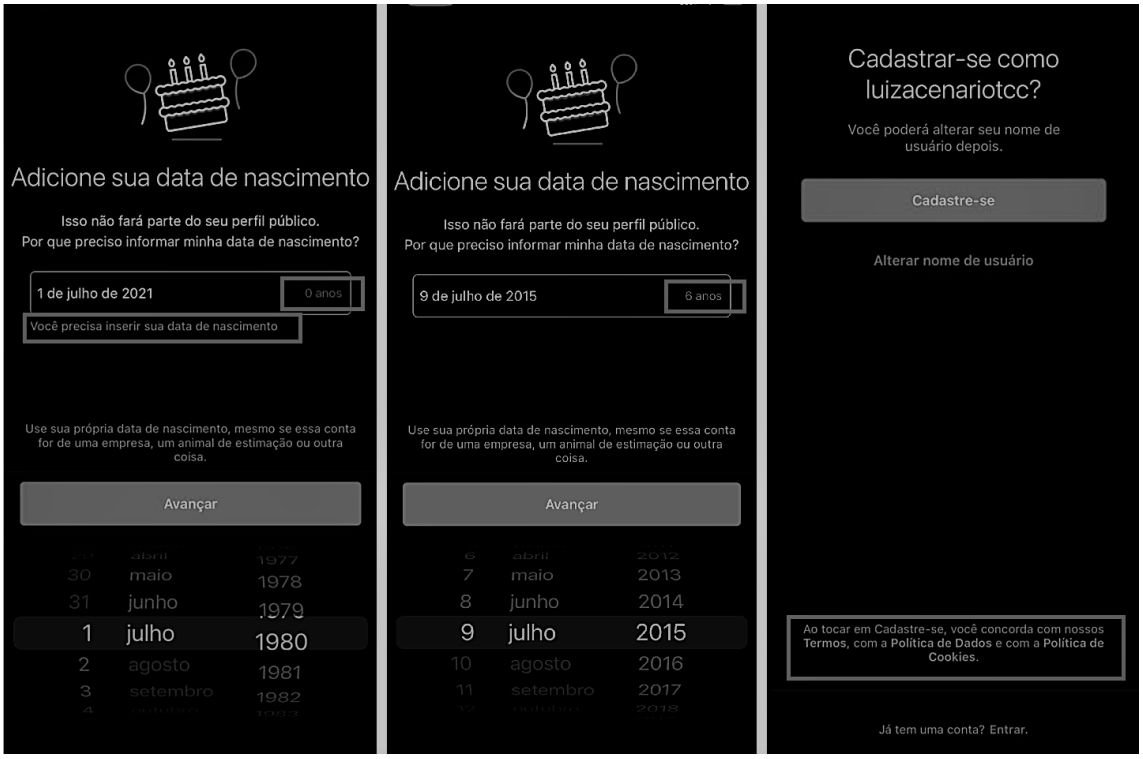

Figura 1. Inserir data de nascimento e confirmar o cadastro

Através de uma análise da interface foi identificado o uso de *Misdirection* exatamente na parte correspondente a contradição citada anteriormente. Os *links* para “Termos de uso”, “Política de Dados” e “Política de Cookies” ficam na parte inferior da página em letras menores e em cores que os camuflam, em oposição ao botão de “Cadastre-se” no topo da página em cor vibrante e chamando mais atenção em relação aos demais elementos (Figura 1). Como consequência do uso desse Padrão Obscuro, não há garantia de que

o usuário tenha o conhecimento de que seus dados serão utilizados, atributo do princípio ético de consentimento [Fjeld et al. 2020].

Existe uma predominância dos signos metalinguísticos em relação aos demais, demonstrado pela desproporção no tamanho entre as metamensagens reconstruídas. Isso é resultado da política de dados do Instagram que é extensa, mesmo que políticas de privacidade maiores diminuam as chances de que os usuários as leiam e se informem [Meier et al. 2020]. Ainda sobre os signos metalinguísticos, há uma falha na comunicabilidade quando se fala sobre os dados do usuário. Embora seja comunicada uma necessidade do usuário ("Você gostaria de ter controle sobre os seus dados.") e a solução do sistema para isso ("Concedemos a você a capacidade de acessar, retificar, portar e apagar seus dados. Você pode acessar e excluir as informações que coletamos. 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.") não é comunicado ao usuário como utilizar a solução em "Como funciona e como deve usá-lo".

Ou seja, a revogação do consentimento e a possibilidade de apagar e retificar dados são comentadas na metamensagem reconstruída a partir dos signos metalinguísticos, mas não é explicitada a forma como isto poderia ser feito pelo usuário. Isso compromete o direito do usuário de remover o consentimento sobre uso e coleta de seus dados a qualquer momento [European Union 2016]. Pensando em consentimento informado, mesmo que parte da metamensagem cite quais dados são coletados e para que são usados, eles não são informados com exatidão, sendo utilizados diversas vezes termos vagos como "e outras informações", "Dentre as informações coletadas sobre você"e "e outras experiências negativas". Isso entra em contradição com o trecho "Você gostaria de ter controle sobre os seus dados."além de comprometer o direito do usuário de ter ciência dos riscos, benefícios e alternativas em relação uso de seus dados [Fjeld et al. 2020].

5. Considerações Finais e Conclusões

O estudo realizado indicou pontos de potenciais rupturas na comunicabilidade do princípio ético relacionado ao consentimento. O usuário representado no cenário de interação usado no MIS (a Luiza), pode ter interpretações errôneas na tela de inserir data de nascimento. Uma solução para este problema seria mudar o destaque em vermelho para qualquer idade abaixo de treze anos, ou desabilitar o botão de “avançar” caso a idade não seja inválida.

Dado que o Instagram utilizou a estratégia *Misdirection* na tela de cadastro, consideramos que o princípio de consentimento foi mal adotado. Como dito na seção 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 (Figura 1). 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. Uma forma de solucionar o uso de *Misdirection* seria acrescentar alguma ação obrigatória para utilização do sistema, visando confirmar o consentimento, como selecionar um *checkbox* ou responder um *pop-up*. Desta forma garante-se que o usuário pelo menos está ciente que existem políticas com as quais está consentindo.

Por fim, a política de dados do Instagram é extensa, o que é um problema, porque

como já citado, políticas de privacidade maiores diminuem as chances de que os usuários a leiam e se informem [Meier et al. 2020]. Ao longo de todo o documento também não foram identificadas informações sobre os riscos ou alternativas da coleta de dados do usuário, o que é necesário para o consentimento informado [Fjeld et al. 2020]. Portanto, consideramos também que este principio foi mal adotado, visto que o Instagram não fornece informações e condições suficientes para que o usuário decida com ciência de todos os seus impactos e riscos. Uma forma de solucionar ambos os problemas seria a adoção de uma política de dados mais curta e direta, que liste com exatidão os tipos de dados coletados, a partir de quais fontes e com quem podem ser compartilhados, além de explicitar como acessá-los, retificá-los, apagá-los e retirar o consentimento do seu uso. Reconhecer e antecipar políticas de privacidade ruins e suas consequências é fundamental e um dos princípios de *PbD* [Cavoukian 2009].

Sem a determinação clara, objetiva e exata dos tipos de dados que estão sendo coletados, por quem e para qual finalidade, como definido pela LGPD (2018), a privacidade dos usuários pode estar sendo violada por mal uso (dado que os usuários não sabem exatamente todas as finalidades do uso de seus dados), por intercepção (dado que os usuários não sabem quem são os terceiros com quem o Instagram compartilha informações) e por combinação de informações (dado que o Instagram também combina as informações coletadas por ele com as provenientes de terceiros não explicitados) [Kizza 2003]. Sobre a última violação, embora o Instagram não cite diretamente o uso de Inteligência Artificial nos trechos de interface analisados, o uso fica subentendido em "Nossos sistemas processam automaticamente o conteúdo e as comunicações que você e outras pessoas fornecem [...] Combinamos as informações que temos sobre você para personalizar e aprimorar nossos Produtos [...]", o que coincide com a definição de IA da HLEGAI (2019). Portanto, os dados do usuário podem ou não estar sendo utilizados para inferência de informações [Rocasolano 2022] que ele não consentiria se tivesse conhecimento. Por sua vez, o direto do usuário de não ser monitoriado, fundamental para o Estado Democrático de Direito [Vianna 2007], pode ser violado. Reiteramos que a privacidade do usuário na era da informação é fundamental para proteger sua autonomia [Kizza 2003].

Esta pesquisa traz duas contribuições principais com a aplicação do MIS: investigação da comunicabilidade de princípios éticos com a identificação de oportunidades concretas para melhorar a comunicabilidade do princípio ético do consentimento; e a caracterização do padrão obscuro misdirection no contexto do Instagram.

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 algorítimos do Instagram, o estudo ficou limitado a explorar a comunicabilidade dos princípios éticos de privacidade através da interface. Em trabalhos futuros estudaremos em outras redes sociais buscando violações a este ou outros princípios éticos, a fim de comparação com os resultados obtidos com o Instagram.

6. Agradecimentos

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

Referências

AEPD (2019). A guide to privacy by design.

Ahlgren, M. (2021). 40+ instagram statistics & facts. https://www.websitehostingrating.com/research/instagram-statistics/. Acesso em: 28 out. 2021.

Barbosa, S. and Silva, B. (2010). *Interação humano-computador*. Elsevier Brasil.

Barreto, P., Salgado, L., and Viterbo, J. (2018a). Assessing the communicability of human- data interaction mechanisms in transparency enhancing tools. In *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pages 897–906.

Barreto, P., Salgado, L., and Viterbo, J. (2018b). Transparency communication strategies in human-data interaction. New York, NY, USA. Association for Computing Machinery.

Bindu, T. H. (2017). Deducing private information from social network using unified classification. *Journal of Science and Technology (JST)*, 2(3):41–46.

BRASIL (1988). Constituição da república federativa do brasil de 1988.

Brignull, H. (2010). Dark patterns. https://www.darkpatterns.org/. Acesso em: 2 sep. 2021.

Brito do Rêgo, B., Monteiro, I. T., and Sampaio, A. L. (2017). Communicability evaluation of privacy settings on facebook for android. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 623–639. Springer.

Cavoukian, A. (2009). *Privacy by design*.

Chen, J., Hsieh, G., Mahmud, J. U., and Nichols, J. (2014). Understanding individuals' personal values from social media word use. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, pages 405–414.

Coopamootoo, P. L. and Ashenden, D. (2011). A systematic evaluation of the communicability of online privacy mechanisms with respect to communication privacy management. In *International Conference of Design, User Experience, and Usability*, pages 384–393. Springer.

de Almeida, M. C. G. and de Castro Salgado, L. C. (2019). Investigating google dashboard's explainability to support individual privacy decision making. In *Proceedings of the 18th Brazilian Symposium on Human Factors in Computing Systems*, IHC '19, New York, NY, USA. Association for Computing Machinery.

de Rezende Xavier, S. I. (2014). Privacidade em redes sociais: uma análise da experiência dos usuários. Master's thesis, Universidade Federal de Minas Gerais.

de Souza, C. S. (2005). *The semiotic engineering of human-computer interaction*. MIT press.

de Souza, C. S. and Leitão, C. F. (2009). Semiotic engineering methods for scientific research in hci. *Synthesis Lectures on Human-Centered Informatics*, 2(1):1–122.

de Souza, C. S., Leitão, C. F., Prates, R. O., and Da Silva, E. J. (2006). The semiotic inspection method. In *Proceedings of VII Brazilian symposium on Human factors in computing systems*, pages 148–157.

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

dos Santos, G. E., Barbosa, M. W., and Barbosa, G. A. (2016). Caracterização das estratégias de privacidade do instagram. In *Anais do XIII Simpósio Brasileiro de Sistemas Colaborativos*, pages 1275–1289. SBC.

European Union (2016). General data protection regulation. *Official Journal of the European Union*, page 48.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., and Srikumar, M. (2020). Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for ai. *Berkman Klein Center Research Publication*, (1).

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A. L. (2018). The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pages 1–14.

HLEGAI (2019). High-level expert group on artificial intelligence. ethics guidelines for trustworthy ai. https://ec.europa.eu/digital-single-market/en/news/ethics guidelines-trustworthy-ai.

Kemp, S. (2020). Social media users pass the 4 billions mark as global adoptionsoars.. [s. l.], 20 out. 2020. https://wearesocial.com/blog/2020/10/social-media-users-pass-the-4-billion-mark-as-global-adoption-soars. Acesso em: 10 dez. 2010.

Kemp, S. (2022). Digital 2022: Another year of bumper growth, 26 jan. 2022. https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/. Acesso em: 7 apr. 2022.

Kizza, J. M. (2003). *Ethical and social issues in the information age*. Springer.

Kosinski, M., Stillwell, D., and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the national academy of sciences*, 110(15):5802–5805.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, 16(4):473–475.

Majedi, M. and Barker, K. (2021). The privacy policy permission model: A unified view of privacy policies. *Trans. Data Priv.*, 14(1):1–36.

Meier, Y., Schäwel, J., and Krämer, N. C. (2020). The shorter the better? effects of privacy policy length on online privacy decision-making. *Media and Communication*, 8(2):291–301.

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy*, 16(4):266–275.

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, 57:1701.

ONU (1948). Declaração universal dos direitos humanos.

PRESIDÊNCIA DA REPÚBLICA (2018). Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd).

Recuero, R. (2007). Considerações sobre a difusão de informações em redes sociais na internet. *Intercom Sul*.

Rocasolano, M. M. (2022). Human rights, big data and artificial intelligence: Elements of a complex algorithm. In *Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts*, pages 93–102. Springer.

Vianna, T. (2007). *Transparência pública, opacidade privada*. Editora Revan, 1st edition.

Wang, Y. and Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology*, 114(2):246.