ESCOLA ENSINO MÉDIO INTEGRAL
MARIA AUGUSTA SIQUEIRA PROFESSORA

OPENVOICE

REDE SOCIAL

FELIPE PEREIRA BATISTA, GUSTAVO MARINHO, GUSTAVO SILVA, LARYSSA TORRES, MARIA EDUARDA & ISMAEL AVELINO LIMA

OSASCO
2024

FELIPE PEREIRA BATISTA, GUSTAVO MARINHO, GUSTAVO SILVA, LARYSSA TORRES, MARIA EDUARDA & ISMAEL AVELINO LIMA

OPENVOICE

REDE SOCIAL

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Desenvolvedor de Sistemas pela Escola de Ensino Médio em Tempo Integral Maria Augusta Siqueira Professora.

Orientador: Prof. João Vitor Yokada

OSASCO
2024

FICHA CATALOGRÁFICA

Batista, Felipe Pereira, 2007 -
OpenVoice: Rede Social / Felipe Pereira Batista, Gustavo Marinho, Gustavo Silva, Laryssa Torres, Maria Eduarda, Ismael Avelino Lima - 2024

Orientador: Prof. João Vitor Yokada.
Trabalho de conclusão de curso (graduação) - Ensino Médio em Tempo Integral Maria Augusta Siqueira Professora, Curso Técnico de Desenvolvimento de Sistemas, 2024

OPENVOICE

REDE SOCIAL

FELIPE PEREIRA BATISTA, GUSTAVO MARINHO, GUSTAVO SILVA, LARYSSA TORRES, MARIA EDUARDA & ISMAEL AVELINO LIMA

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Desenvolvedor de Sistemas pela Escola de Ensino Médio em Tempo Integral Maria Augusta Siqueira Professora.

Aprovado em: _____/_____/_____.

BANCA EXAMINADORA

_____

Orientador

Prof. João Vitor Yokada

E.M.T.I. Maria Augusta Siqueira Professora

_____

Membro da banca (1)

Prof. Leonel de Souza

E.M.T.I. Maria Augusta Siqueira Professora

_____

Membro da banca (2)

Prof. Rogério Rocha

E.M.T.I. Maria Augusta Siqueira Professora

DEDICATÓRIA

Dedicamos este trabalho para todos que lutam pela liberdade de expressão e pelo direito de cada voz ser ouvida.

AGRADECIMENTOS

Agradecemos ao Professor David J. Malan, do curso CS50X, por proporcionar um vasto entendimento que foi fundamental para a criação deste projeto.

Agradecemos a Newman LM, por nos ajudar a enxergar o mundo de forma melhor e contribuir com as nossas ideias.

Agradecemos ao Professor Leonel, por nos ajudar muito em relação aos projetos de ambas as matérias do curso técnico.

Agradecemos a Professora Maria Cristina que sempre deu o seu melhor nos dias de aula e que infelizmente não está aqui por ter ótimas competências por estar em uma área melhor.

Agradecemos ao Professor Rogério Rocha por ser um ótimo professor e saber explicar bem e estar nos preparando para o futuro.

“Posso não concordar com nenhuma das palavras que você disser, mas defenderei até a morte o teu direito de dizê-las.”

— François-Marie Arouet (Voltaire)

RESUMO

Conforme a progressão das redes sociais, essas plataformas se tornaram espaços onde as pessoas podem se informar do que está acontecendo e se expressarem. No entanto, o uso dos algoritmos constantemente limita a liberdade de expressão, polariza o conteúdo exibido e explora a privacidade dos usuários. O projeto OpenVoice visa corrigir esses problemas. O OpenVoice se diferencia por ser uma rede social sem anúncios, coletando o mínimo de dados pessoais e respeitando a privacidade dos usuários. Além disso, promove a liberdade de expressão, sem a interferência de algoritmos que possam restringir a experiência dos usuários.

Palavras-chave: privacidade, algoritmos, liberdade de expressão, dados.

ABSTRACT

As social media has evolved, these platforms have become spaces where people can learn about what's happening and express themselves. However, the use of algorithms constantly limits freedom of expression, polarizes the content displayed, and exploits users' privacy. The OpenVoice project aims to address these issues. OpenVoice stands out by being an ad-free social network, collecting minimal personal data and respecting users' privacy. In addition, it promotes freedom of expression, without the interference of algorithms that could restrict users' experience.

Keywords: privacy, algorithm, freedom of expression, data.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

EMTI – Ensino Médio em Tempo Integral

PbD - Privacy by Design

ISO - International Organization for Standardization

LGPD - Lei Geral de Proteção de Dados

GDPR - Regulamento Geral de Proteção de Dados

SGSI - Sistema de Gestão de Segurança da Informação

AIP - Avaliações de Impacto à Privacidade

HTML – HyperText Markup Language

CSS – Cascading Style Sheets

AWS S3 – Amazon Simple Storage Service

SQLite3 - Structured Query Language Lite 3

Vue.js – Vue JavaScript

SUMÁRIO

1. INTRODUÇÃO

As redes sociais se tornaram um espaço onde as pessoas podem se informar sobre o que está acontecendo no presente e se expressarem. Contudo, as redes sociais fazem o uso de algoritmos que constantemente limitam a liberdade de expressão, polarizam o conteúdo exibido e explora a privacidade dos usuários, coletando o máximo de informações possíveis para poder vendê-las ou utilizá-las em estratégias de marketing mais bem direcionadas.

Entretanto, esse cenário levanta preocupações sobre o impacto dessas práticas na sociedade. O uso intensivo de algoritmos, por exemplo, embora tenha como objetivo personalizar o conteúdo e melhorar a experiência do usuário, acaba criando bolhas de informações e favorecendo a polarização. Ao apresentar apenas o que o algoritmo considera relevante para cada usuário, muitas vezes baseado em interações passadas, esses sistemas limitam o acesso a uma diversidade de perspectivas e podem intensificar divisões ideológicas.

Além disso, o comércio de dados pessoais se tornou uma prática comum entre as grandes plataformas. As redes sociais tradicionais coletam informações detalhadas sobre os usuários, desde hábitos de navegação até interações e preferências pessoais, que muitas vezes é feita sem o pleno conhecimento dos próprios usuários. Essas informações são frequentemente utilizadas para direcionar anúncios de forma cada vez mais precisa, levantando questões éticas sobre privacidade e manipulação de dados.

1.1. QUESTÃO DE PESQUISA

É neste cenário que surge o OpenVoice, uma rede social que adota uma abordagem oposta, com o objetivo de corrigir esses problemas ao priorizar a liberdade de expressão, a privacidade dos usuários e oferecer um ambiente livre de algoritmos, anúncios e a coleta de dados pessoais. Assim, a questão que orienta

este trabalho é: *Como o OpenVoice pode representar uma alternativa mais ética e segura em comparação às redes sociais tradicionais?*

1.2. OBJETIVOS DA PESQUISA

O objetivo geral deste trabalho é analisar como o OpenVoice pode ser uma alternativa segura e transparente em meio às redes sociais tradicionais. Especificamente, busca-se:

- Investigar como a ausência de algoritmos impacta a liberdade de expressão e a diversidade de opiniões na plataforma.
- Avaliar como a privacidade dos usuários é preservada em um ambiente sem coleta de dados.
- Explorar o impacto da ausência de anúncios na experiência do usuário.

1.3. JUSTIFICATIVA

A crescente preocupação com a privacidade e o impacto dos algoritmos nas redes sociais tradicionais torna necessária a busca por alternativas mais éticas e transparentes. O OpenVoice oferece uma nova abordagem ao criar um espaço digital que devolve o controle ao usuário, eliminando interferências automatizadas e interesses comerciais. Este trabalho visa contribuir para o debate sobre a ética nas plataformas digitais, explorando os potenciais benefícios de um modelo que prioriza a liberdade de expressão e a privacidade.

2. REVISÃO DE LITERATURA

Para compreender a proposta do OpenVoice e seu contraste com as redes sociais tradicionais, é essencial analisar as principais questões envolvidas ao uso de

algoritmos, à coleta de dados e à liberdade de expressão nas plataformas digitais. Esta seção apresenta uma revisão da literatura que aborda os seguintes aspectos:

- O impacto dos algoritmos na personalização do conteúdo e na formação de bolhas informacionais.
- A coleta e o uso de dados pessoais nas redes sociais, bem como suas implicações éticas.
- Alternativas propostas para redes sociais mais transparentes e voltadas à privacidade, com foco em plataformas que promovem a liberdade de expressão sem interferências comerciais.

Além disso, serão analisados estudos e normativas como *Privacy by Design* (PbD), a Lei Geral de Proteção de Dados (LGPD) bem como os padrões ISO (International Organization for Standardization) 27.001:2022, ISO 27002:2022 e ISO 29134, que estabelecem diretrizes para a implementação de controles de segurança da informação e para a avaliação de impacto à privacidade. Esses marcos fornecem o embasamento necessário para compreender o contexto no qual o OpenVoice se insere, destacando sua abordagem ética e voltada à privacidade.

2.1. PRIVACY BY DESIGN (PBD)

O Privacy by Design (PbD) é uma abordagem de projeto que tem o objetivo de incorporar a privacidade e a proteção de dados pessoais em todas as fases de desenvolvimento de produtos, serviços e sistemas. Essa abordagem foi criada por Ann Cavoukian em 1995 (Cavoukian, 1995) e se tornou uma das principais estratégias para garantir a privacidade e a segurança de dados na era digital. Essa abordagem foi incorporada ao Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UNIÃO EUROPEIA, 2016). O artigo 25 do GDPR estabelece que os controladores de dados devem implementar medidas técnicas e organizacionais apropriadas desde o início do processo de tratamento de dados, para garantir qie os princípios de proteção de dados sejam atendidos. Isso inclui a implementação do PbD, que visa garantir que a proteção de dados seja considerada desde a concepção do sistema. O desenvolvimento de software com PbD envolve uma série de práticas e processos que visam garantir a privacidade e a segurança

de dados pessoais dos usuários. Algumas práticas utilizadas são a minimização de dados, onde se é coletado apenas os dados necessários para o funcionamento da aplicação, anonimizar os dados, ou seja, remover ou substituir informações que possam identificar diretamente os usuários e exigir o consentimento explícito quando for necessário coletar algum tipo de dado, mostrando para qual finalidade está sendo exigido. Essas práticas nos ajudam além de garantir a conformidade com as legislações e regulamentações de privacidade, também ajuda a proteger a confiança e a fidelidade dos usuários.

Por exemplo uma rede social, ela pode inicialmente coletar apenas os dados essenciais para o funcionamento básico do sistema como nome, email e data de nascimento e por padrão deixar desabilitado a opção de compartilhar esses dados com terceiros.

2.2. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A LGPD, ou Lei Geral de Proteção de Dados (Lei 13.709/2018), tem como objetivo proteger a privacidade e os dados pessoais dos cidadãos brasileiros (BRASIL, 2018). Esta lei estabelece regras e diretrizes para o tratamento dos dados por empresas e outras organizações.

A LGPD foi inspirada em legislações semelhantes em vigor em outros países, tal como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UNIÃO EUROPEIA, 2016). A lei é importante porque garante que os dados pessoais dos cidadãos brasileiros sejam tratados de forma responsável e ética.

Desta forma, a lei nos protege de abusos e violações como ocorreu em 2018 com usuários da rede social *Facebook*, na época foram acessados sem autorização os dados de mais de 87 milhões de pessoas pelo mundo e de mais de 443 mil brasileiros pela consultoria Cambridge Analytica. (VEJA, 2018).

A lei estabelece uma série de direitos para os titulares de dados, como o direito de acesso, retificação, exclusão e portabilidade dos seus dados pessoais. Também define as obrigações das empresas e organizações que tratam esses dados, exigindo que elas implementem medidas de segurança e privacidade

adequadas para protegê-los. Em relação ao desenvolvimento de software, a LGPD pode impactar essas empresas e organizações a realizar ajustes em suas políticas de privacidade, pedindo autorização dos seus usuários para o armazenamento e utilização dos dados sensíveis.

Também é necessário melhorar a segurança no armazenamento dos dados seja com uso de criptografia, realizando o controle de acesso ou monitorando e detectando ameaças para evitar vazamentos e demais transtornos.

A conscientização e treinamento dos funcionários é fundamental. É necessário que todos entendam suas obrigações legais e sigam a política interna da empresa. Além disso, as empresas precisam estar preparadas para se apresentar aos órgãos reguladores que estão em conformidade com as medidas e que estão protegendo a privacidade dos titulares de dados. Nesse sentido, é imprescindível realizar o mapeamento de todos os dados pessoais que a organização coleta, processa e armazena. Isso permite ter uma visão mais clara sobre os tipos de dados envolvidos, a finalidade da coleta, as bases legais e possíveis transferências para terceiros. O uso de um relatório de impacto é importante já que ele é um documento que descreve os possíveis impactos que determinadas mudanças ou decisões têm em um projeto em relação a sua privacidade e proteção de dados.

Para garantir que a privacidade e a proteção de dados pessoais sejam incorporadas em todas as fases de desenvolvimento de produtos e serviços, a LGPD prevê a adoção de princípios que propõem que a privacidade e a proteção de dados pessoais devem ser tratadas desde o início do desenvolvimento de um software, isso é, que as medidas de segurança devem ser adotadas desde a concepção do projeto em vez de ser tratada posteriormente, esse princípio é conhecido como *Privacy by Design*.

2.3. ISO/IEC 27001:2022

A norma ISO/IEC 27001:2022 específica os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Essa norma é amplamente utilizada por

organizações de todos os setores para proteger suas informações de maneira sistemática e proativa.

O foco principal está portanto em uma abordagem de gestão de riscos, onde a organização deve identificar e avaliar as ameaças e vulnerabilidades associadas aos ativos de informação. Ela estabelece um processo contínuo de identificação, avaliação e tratamento dos riscos à segurança da informação.

Os principais componentes dessa norma incluem:

- **Contexto da organização**: Identificação das necessidades e expectativas de partes interessadas, como clientes, fornecedores e reguladores, no que se refere à segurança da informação.
- **Avaliação de Riscos**: Identificação de ameaças e vulnerabilidades aos ativos de informação, análise de riscos e priorização de controles para mitigação.
- **Controles e medidas de segurança**: Implementação de medidas de segurança adequadas aos riscos identificados, incluindo processos, tecnologias e políticas.
- **Monitoramento e melhoria contínua**: Avaliação constante da eficácia das medidas de segurança e ajustes conforme necessário.

A implementação da ISO/IEC 27001:2022 permite que as organizações demonstrem conformidade com padrões internacionais de segurança, o que é crucial para manter a confiança de clientes e parceiros, além de atender a regulamentações de proteção de dados, como a LGPD e o GDPR.

2.4. ISO/IEC 27002:2022

A norma ISO/IEC 27002:2022 complementa a ISO/IEC 27001:2022 ao fornecer um conjunto detalhado de controles se segurança da informação que podem ser aplicados no contexto do SGSI. Esses controles cobrem diversas áreas

de segurança e são adaptáveis conforme as necessidades específicas de cada organização.

A norma ISO 27002 atua como um guia prático, fornecendo recomendações sobre a seleção, implementação e gestão de controles de segurança da informação. Ela abrange aspectos como:

- **Políticas de segurança**: Definição de políticas claras que orientam o uso e proteção de informações.
- **Controles de acesso**: Medidas para restringir o acesso a informações com base na necessidade de conhecimento.
- **Proteção contra malware**: Implementação de defesas contra vírus, ransomware e outros malwares que possam comprometer a segurança das informações
- **Gestão de incidentes**: Procedimentos para lidar com violações de segurança, incluindo detecção, resposta e recuperação de incidentes.
- **Gestão de continuidade**: Planos para garantir que os serviços essenciais permaneçam disponíveis em caso de falhas ou incidentes de segurança.

Uma das principais atualizações na versão 2022 da ISO 27002 foi a reorganização e consolidação dos controles de segurança, que foram reduzidos e agrupados em categorias mais intuitivas, tomando a norma mais acessível e prática para implementação.

2.5. ISO/IEC 29134:2023

A norma ISO/IEC 29134:2023 é um guia que estabelece diretrizes e princípios para a realização de Avaliações de Impacto à Privacidade (AIP). As AIPs são ferramentas que ajudam as organizações a identificar e a avaliar os riscos à privacidade associados às suas atividades de tratamento de dados pessoais.

As AIPs são muito importantes em contextos nos quais os dados pessoais são coletados e tratados em grande escala, ou quando envolvem informações sensíveis ou de alto risco. As AIPs permitem que as organizações identifiquem os riscos à privacidade associados a essas atividades e ajudem a avaliar sua gravidade e implementem medidas para mitigar esses riscos.

As principais etapas das AIPs incluem a identificação de dados pessoais que serão coletados ou processados, a identificação de riscos e ameaças à privacidade, a avaliação da gravidade desses riscos, a identificação de medidas para mitigá-los e a documentação de todo o processo.

Ela fornece diretrizes e orientações que são fundamentais para as empresas que desejam avaliar a conformidade com a privacidade e proteção de dados pessoais em seus sistemas. Para isso, é necessário adotar uma abordagem baseada em riscos, que permita avaliar os potenciais riscos e ameaças à privacidade dos dados coletados pelo software.

Algumas dessas diretrizes são: Realizar uma nova AIP ou atualizar para minimizar esses riscos e garantir a proteção dos dados pessoais. A aplicação dessas diretrizes e orientações pode contribuir significativamente para a criação de sistemas de software seguros e confiáveis, que respeitam a privacidade dos usuários e atendem às exigências das regulamentações de proteção de dados. Ela descreve um processo de avaliação em três fases: planejamento, execução e relatório.

O processo envolve a identificação dos processos e sistemas que lidam com dados pessoais, a avaliação dos riscos à privacidade e a identificação das medidas de mitigação apropriadas.

Essa norma também fornece orientações para a definição de critérios de avaliação e para a seleção de avaliadores qualificados. Ela incentiva a participação de partes interessadas e o envolvimento de especialistas em privacidade e proteção de dados pessoais para garantir a qualidade da avaliação.

3. OBJETIVOS DO ESTUDO

3.1. OBJETIVO GERAL

Analisar como a plataforma OpenVoice pode servir como uma alternativa mais ética e segura em relação às redes sociais tradicionais.

3.2. OBJETIVOS ESPECÍFICOS

1. Investigar os impactos da ausência de algoritmos na liberdade de expressão.
2. Examinar as percepções dos usuários sobre a privacidade e segurança de seus dados.
3. Avaliar a experiência do usuário sem a presença de anúncios direcionados.

4. PROCEDIMENTOS METODOLÓGICOS

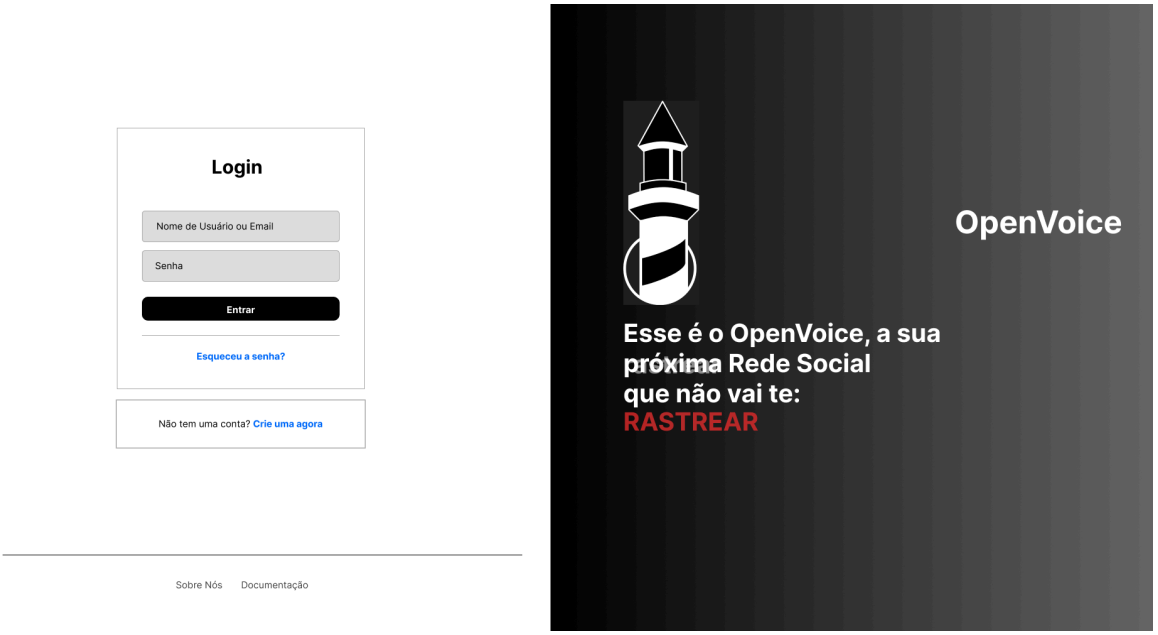
A abordagem metodológica adotada visa explorar como a plataforma pode oferecer uma alternativa mais ética e segura em comparação às redes sociais tradicionais, utilizando uma análise detalhada dos elementos de privacidade e segurança, utilizando como base a LGPD (Lei Geral de Proteção de Dados), Privacy by Design (Design por Privacidade) e as normas ISO 27001, ISO 27002 e ISO 29134.

4.1. DESIGN DA PLATAFORMA

O desenvolvimento da plataforma foi realizado utilizando HTML5, CSS3, JavaScript e Vue.js para o Front-End e PHP, Laravel MySQL e Web Socket para o Back-End. Inicialmente, ferramentas de prototipagem foram utilizadas para criar

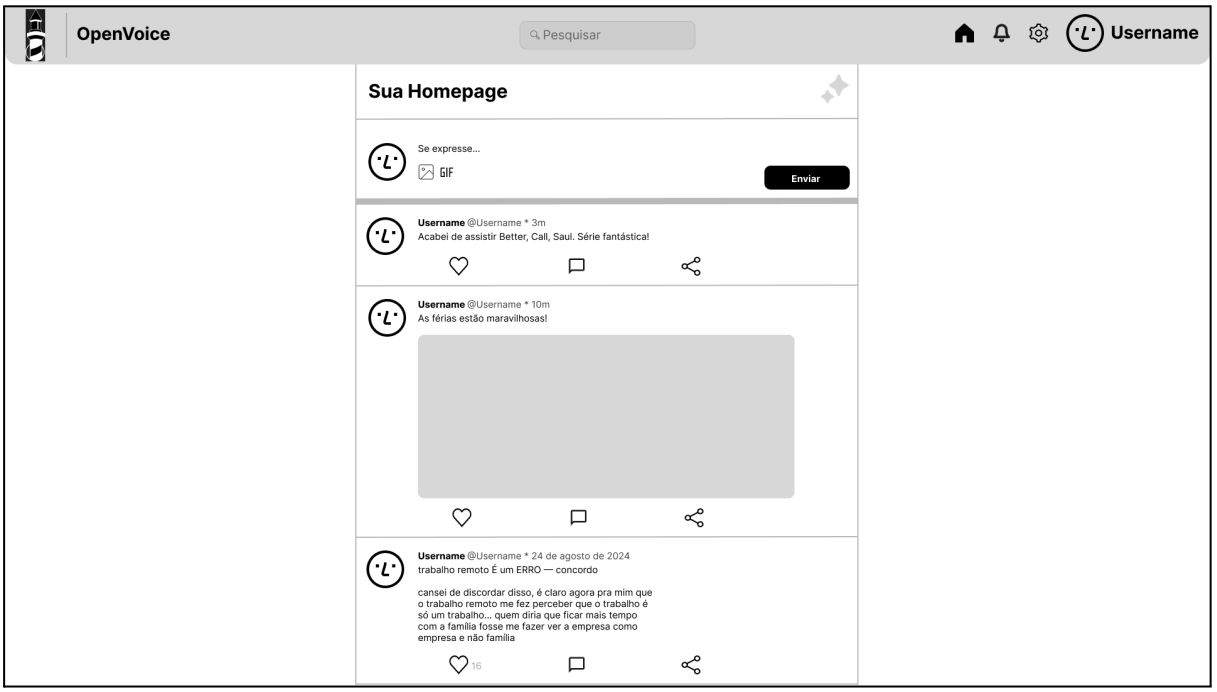
wireframes e fluxos de usuário, com o intuito de proporcionar uma experiência amigável e intuitiva.

- **FIGURA 4.1.1 - ONBOARDING DESKTOP**

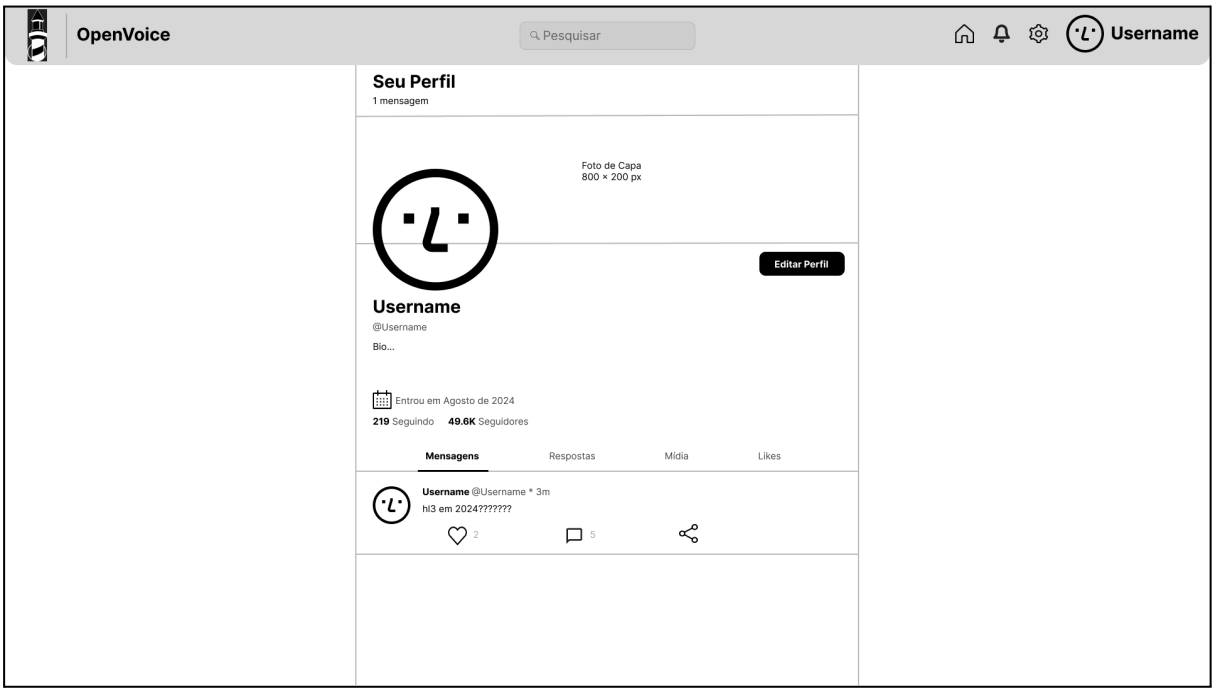


- **FIGURA 4.1.2 - ONBOARDING SMARTPHONE**

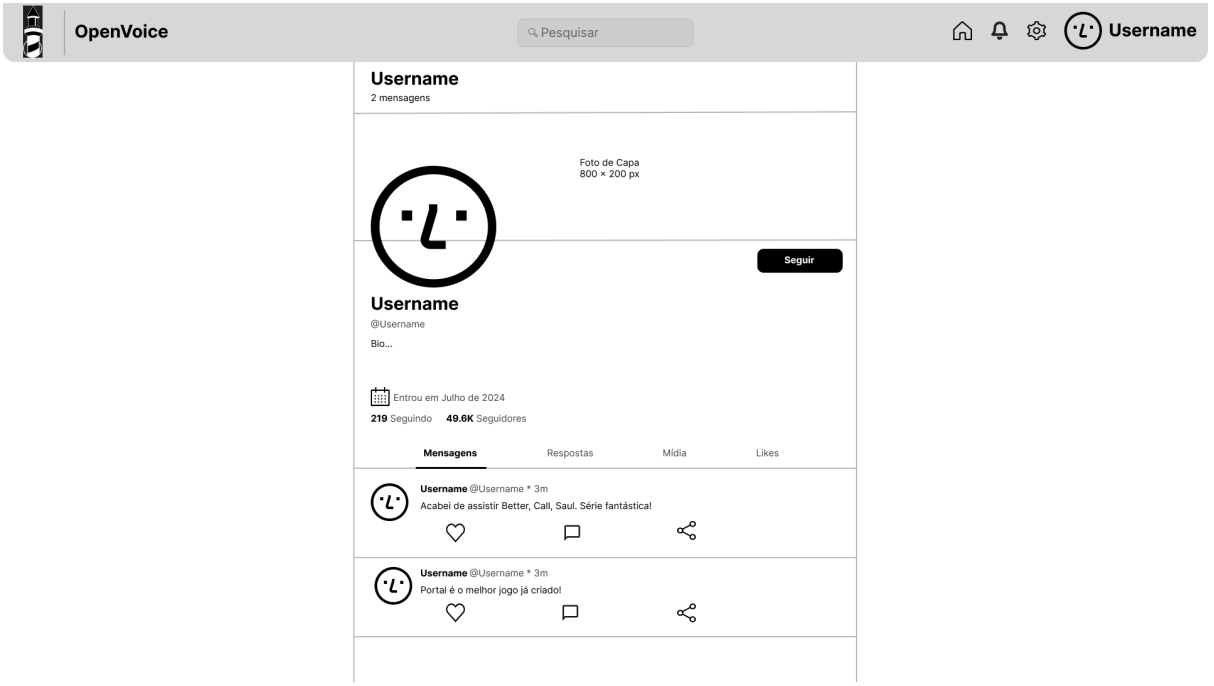
- **FIGURA 4.1.3 - HOMEPAGE**



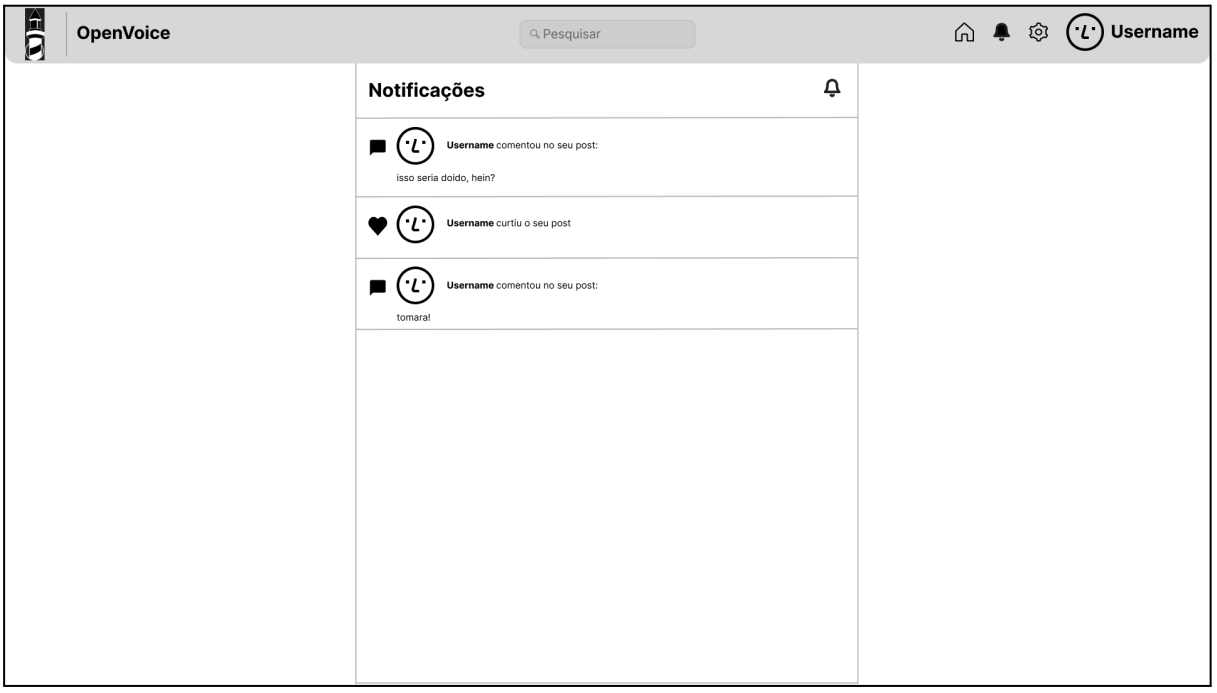
- **FIGURA 4.1.4 - MEU PERFIL**



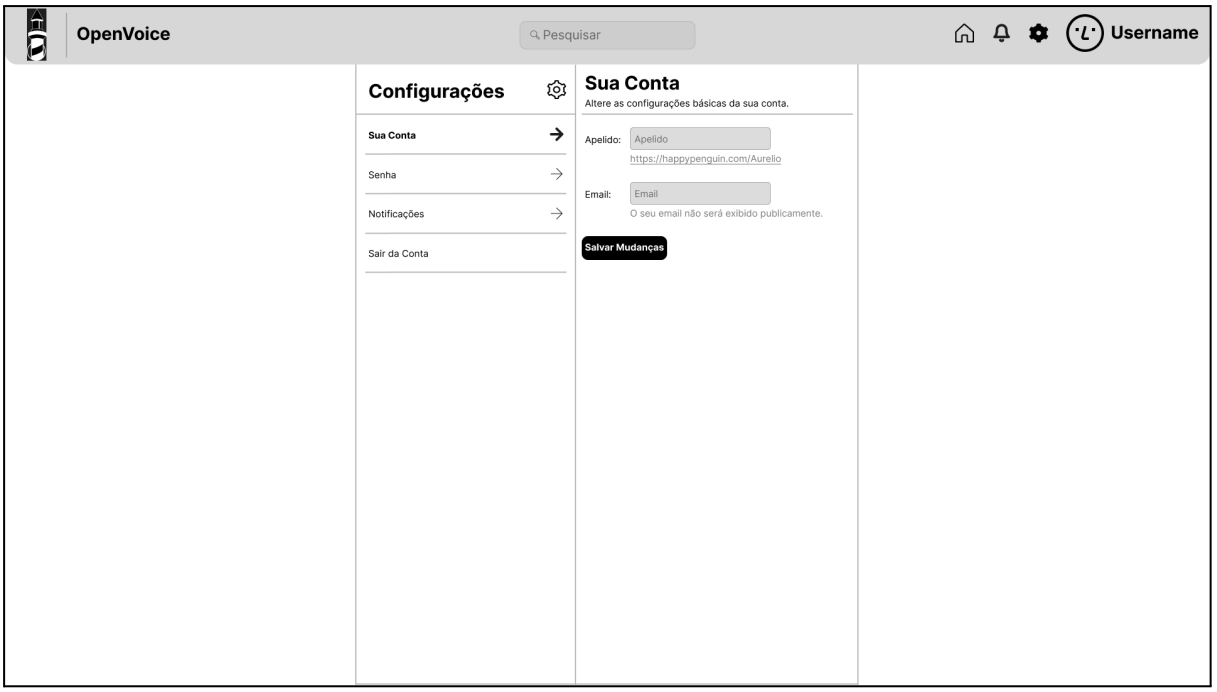
- **FIGURA 4.1.5 - OUTRO PERFIL**



- **FIGURA 4.1.6 - NOTIFICAÇÕES**



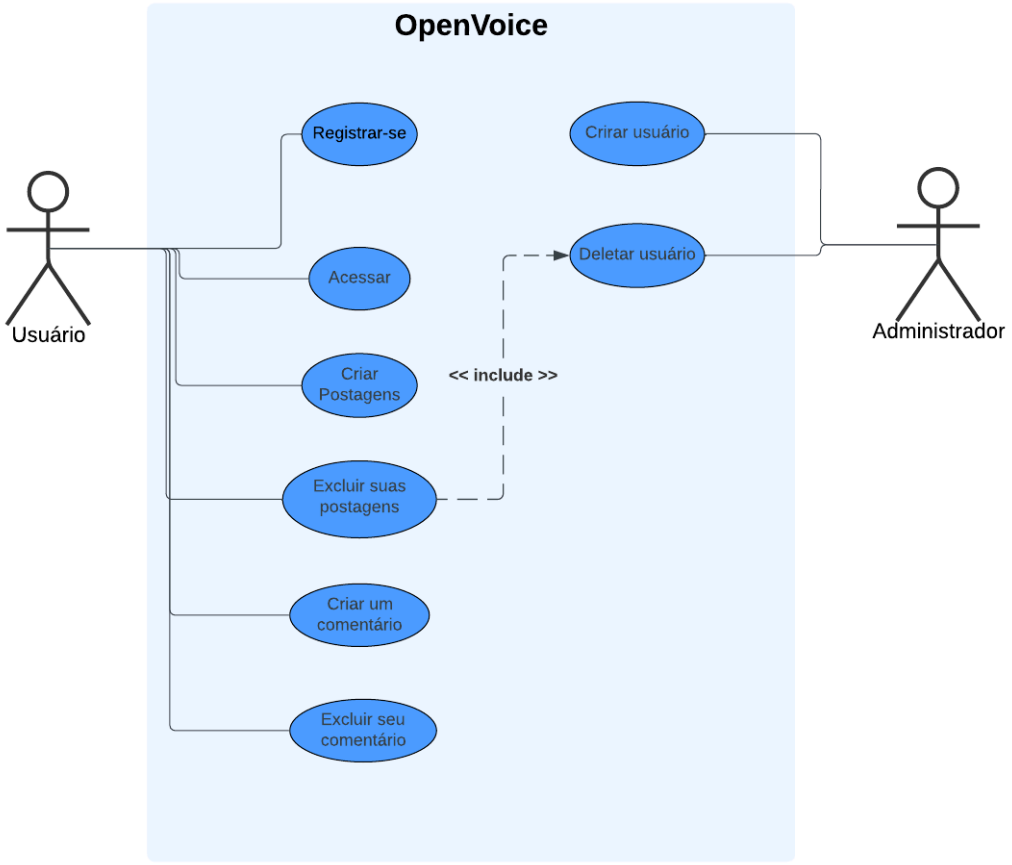
- **FIGURA 4.1.7 - CONFIGURAÇÕES**



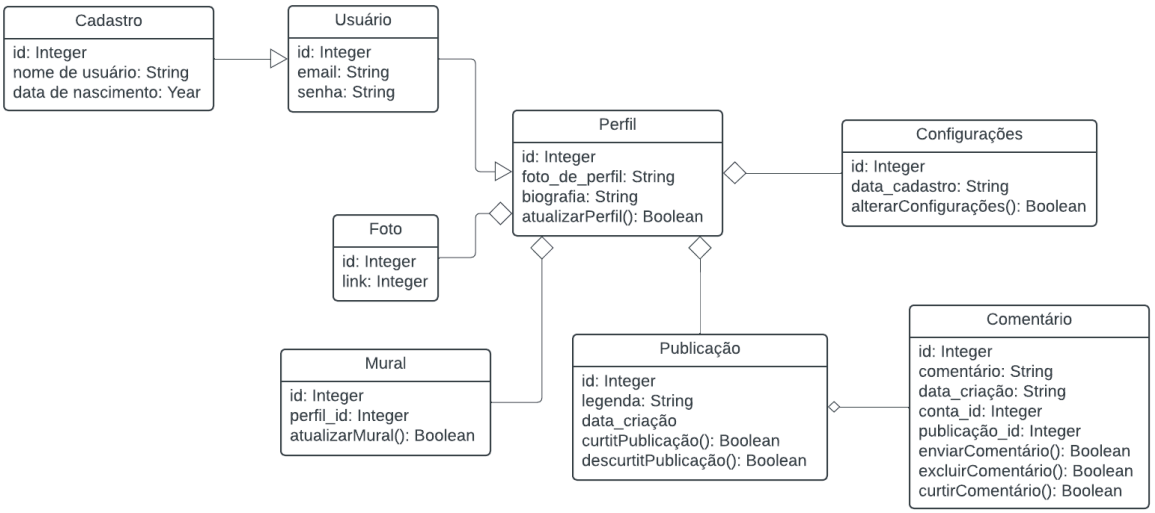
4.2. DIAGRAMAS DE MODELAGEM

Para complementar o entendimento sobre a estrutura do sistema, foram elaborados diagramas de casos de uso, classes e sequenciais. Esses diagramas são essenciais para visualizar a interação entre os usuários e a plataforma, além de esclarecer as funcionalidades do sistema.

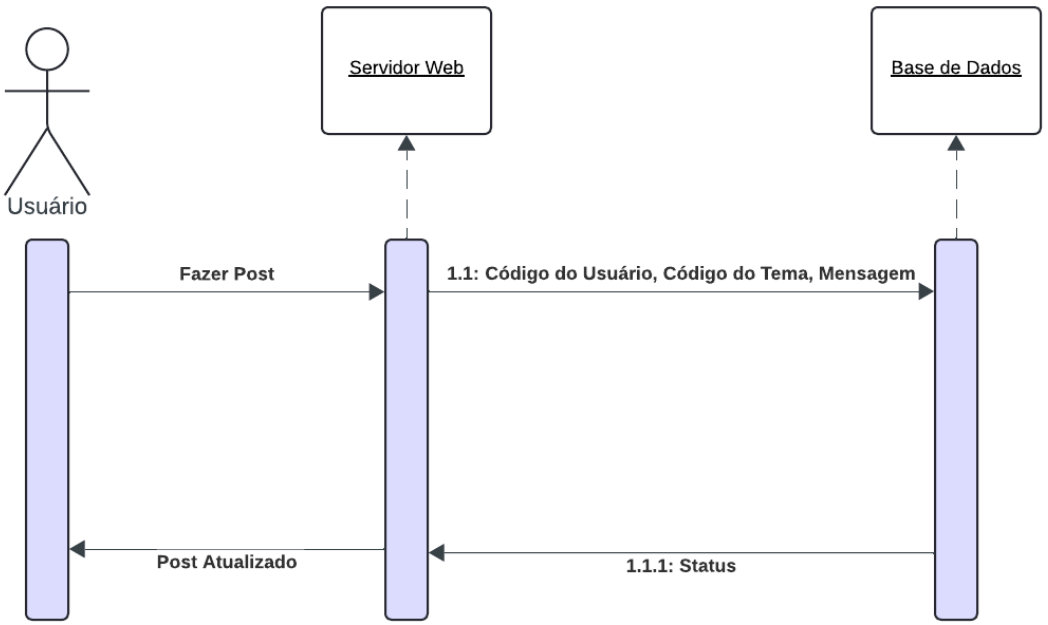
- **FIGURA 4.2.1 - DIAGRAMA DE CASOS DE USO**



- **FIGURA 4.2.2 - DIAGRAMA DE CLASSE**



- **FIGURA 4.2.3 - DIAGRAMA DE SEQUÊNCIA**



5. CONCLUSÃO

Este trabalhou buscou desenvolver uma rede social com o propósito de não explorar os dados e a privacidade dos usuários, utilizando conceitos que priorizam a privacidade de dados dos usuários.

Os desafios e dificuldades enfrentadas estão relacionados ao aperfeiçoamento dos conhecimentos nas tecnologias utilizadas para o desenvolvimento do site. Também se tratando da aplicação, houve desafios no volume de dados que são necessários coletar e o armazenamento correto deles.

5.1. LIÇÕES APRENDIDAS

Ao final do estudo, podemos destacar algumas lições como a importância de se ter uma abordagem proativa em relação a segurança e privacidade do usuário, buscando minimizar os riscos desde o início do desenvolvimento do projeto.

5.2. TRABALHOS FUTUROS

Durante o desenvolvimento deste projeto, foi possível identificar pontos que podem ser abordados para implementá-lo em futuras versões como desenvolver versões da aplicação que sejam compatíveis nativamente com dispositivos móveis como na plataforma Android e adaptação a futuras mudanças nas legislações e regulamentações vigentes.

6. REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 set. 2024.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho,de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de Dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Mais de 443 mil brasileiros foram vítimas de vazamentos do Facebook, Veja, 2018.

Disponível em: https://veja.abril.com.br/economia/mais-de-443-mil-brasileiros-foram-afetados-no-escandalo

-do-facebook> Acesso em: 10 set. 2024.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles.

Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 29134:2023 - Tecnologia da informação - Técnicas de segurança - Diretrizes para a privacidade no projeto de sistemas. Rio de Janeiro, 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2022 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2022

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. Rio de Janeiro, 2022