PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

RECOMENDAÇÕES PARA A IMPLEMENTAÇÃO DE PRIVACIDADE EM INTERFACES DE SOFTWARE

JOÃO VICTOR CUPERTINO SANCHES

GOIÂNIA
2023

JOÃO VICTOR CUPERTINO SANCHES

RECOMENDAÇÕES PARA A IMPLEMENTAÇÃO DE PRIVACIDADE EM INTERFACES DE SOFTWARE

Monografia apresentada ao curso de Engenharia de Computação da PUC Goiás, como parte dos registros para a obtenção do título de Bacharel em Engenharia da computação.

Orientadora: Profa. Ma. Adriana Silveira de Souza

GOIÂNIA
2023

JOÃO VICTOR CUPERTINO SANCHES

RECOMENDAÇÕES PARA A IMPLEMENTAÇÃO DE PRIVACIDADE EM INTERFACES DE SOFTWARE

Este Trabalho de Conclusão de Curso julgado adequado para obtenção do título de Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola de Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás em _____/_____/_____.

_____

Profª. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Banca Examinadora:

_____

Orientadora: Profª. Ma. Adriana Silveira de Souza

_____

Prof. Esp. André Luiz Alves

_____

Prof. Dr. Juliano Lopes de Oliveira

GOIÂNIA
2023

RESUMO

Este trabalho de conclusão de curso tem com finalidade levantar requisitos de privacidade que podem ser tratados em interfaces gráfica de usuários para software. A metodologia de pesquisa adotada é qualitativa, com o objetivo de compreender e estudar normas e padrões que apoiem a definição de privacidade interfaces gráficas. Para isso, estudou-se técnicas de *Privacy by Design*, a norma ISO/IEC 29184, a norma ISO/IEC 29134 e Lei Geral de Proteção de Dados. Os dados para o estudo foram coletados através de uma revisão de literatura e análise de interfaces de sistemas existentes. O trabalho também destaca a importância da Avaliação de Impacto na Privacidade (AIP) antes do lançamento de novas funcionalidades que coletam dados adicionais do usuário. A AIP é um processo que ajuda as organizações a identificar e reduzir os riscos de privacidade associados a um projeto de dados.

Palavras-chave: Privacy by Design, ISO/IEC 29184, ISO/IEC 29134, LGPD, Avaliação de Impacto na Privacidade (AIP), Interfaces Gráficas de Usuários (GUI).

ABSTRACT

This work aims to raise privacy requirements that can be addressed in graphical user interfaces for software. The research methodology adopted is qualitative, with the objective of understanding and studying norms and standards supporting privacy in graphical interfaces. This work approached several subjects, for example, Privacy by Design techniques, the ISO/IEC 29184 standard, the ISO/IEC 29134 standard, and the General Data Protection Law. Literature review and analysis of existing system interfaces service of the base to collect data. The work also highlights the importance of the Privacy Impact Assessment (PIA) before launching new features that collect additional user data. The AIP is a process that helps organizations identify and mitigate the privacy risks associated with a data project.

Keywords: Privacy by Design, ISO/IEC 29184, ISO/IEC 29134, LGPD, Privacy Impact Assessment (PIA), Graphic User Interfaces (GUI).

LISTA DE ABREVIATURAS

AIP – Avaliação de Impacto na Privacidade

ISO – International Organization for Standardization (Organização Internacional de Normalização)

IEC – International Electrotechnical Commission (Comissão Eletrotécnica Internacional)

LGPD – Lei Geral de Proteção de Dados

GUI – Graphical User Interface (Interface Gráfica do Usuário)

GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados).

LLC - Limited Liability Company

SUMÁRIO

1. INTRODUÇÃO

A proteção da privacidade e dos dados pessoais tem sido um tema cada vez mais relevante e discutido no contexto atual (Castells, 2010), especialmente com o advento de novas tecnologias e a ampliação da coleta de dados pessoais por empresas e organizações, como redes sociais e aplicativos de localização (Zuboff, 2019). Nesse sentido, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018), entrou em vigor no Brasil em 2020, estabelecendo normas para o tratamento de dados pessoais por empresas e organizações.

A motivação da LGPD baseia-se na necessidade de proteger os direitos fundamentais de liberdade e privacidade dos cidadãos, bem como garantir o desenvolvimento econômico e tecnológico do país (Cavalcante, 2021). A lei visa tratar questões como consentimento, transparência, segurança, anonimização e responsabilização das empresas e organizações que coletam, processam e armazenam dados pessoais (Brasil, 2018).

Além da LGPD, a norma *Information technology - Security techniques - Guidelines for privacyimpact* ISO/IEC 29134:2017 estabelece um *framework* para a realização de análises de risco relacionadas à privacidade de dados pessoais (DPs). Essa norma define diretrizes gerais para avaliar os riscos associados à coleta, uso, retenção e exclusão DPs (ISO/IEC 29134:2017, 2017). Já o conceito de "*privacy by design*" (privacidade desde o início do design) tem sido amplamente discutido na literatura como uma abordagem para garantir a privacidade dos dados pessoais desde o início do processo de design de produtos e serviços (Cavoukian, 2011).

A conexão entre a LGPD, a norma ISO/IEC 29134:2017 e o conceito de "*privacy by design*" reside na sua finalidade comum de proteger a privacidade e os dados pessoais. A LGPD estabelece os requisitos legais para o tratamento de dados pessoais no Brasil, a norma ISO/IEC 29134:2017 fornece um *framework* para avaliar os riscos à privacidade dos dados pessoais, e o conceito de "*privacy by design*" propõe uma abordagem proativa para garantir a privacidade desde o início do processo de design de produtos e serviços. Juntos, eles formam um conjunto robusto de diretrizes e práticas para a proteção da privacidade e dos dados pessoais.

A aplicação desses conceitos em interfaces visuais de *software* é um tema importante, uma vez que pode ajudar a garantir a privacidade e a segurança dos dados pessoais dos usuários. Outros modelos, como o Regulamento Geral de Proteção de

Dados (GDPR) da União Europeia, também fornecem diretrizes para a proteção de dados pessoais, incluindo em interfaces de usuário (GDPR, 2016). Sim, essas diretrizes são fundamentais no meu trabalho, pois elas orientam o design e a implementação de interfaces seguras e centradas no usuário (GDPR, 2016).

Por exemplo, um site de comércio eletrônico pode utilizar essas práticas para garantir que as informações de pagamento e envio de produtos não sejam compartilhadas com terceiros não autorizados. Além disso, um aplicativo de saúde pode utilizar o *privacy by design* para garantir que as informações dos pacientes sejam armazenadas de forma segura e confidencial.

O objetivo deste trabalho é identificar as melhores práticas e recomendações para a aplicação do privacy by design em conformidade com a LGPD, a norma ISO/IEC 29134:2017 e o GDPR. Para isso, são analisadas referências relevantes sobre o assunto, como as publicações de Cavoukian (2011) e ISO/IEC 29134:2017 (2017), bem como estudos recentes na área (Cavoukian, 2011; ISO/IEC 29134:2017, 2017).

É relevante estudar este tema porque a proteção de dados pessoais é um direito fundamental e sua violação pode acarretar sérias consequências para os indivíduos e para as empresas (Warren& Brandeis, 1890). Por exemplo, violações de privacidade podem resultar em danos financeiros significativos, como evidenciado pelo caso do Facebook em 2018, onde a empresa foi multada em $5 bilhões pela Federal Trade Commission (FTC) por violações de privacidade (BBC News, 2019). Além disso, a violação de dados pode levar a danos reputacionais, perda de confiança dos clientes e possíveis ações legais (Reuters, 2021).

Além disso, a aplicação do *privacy by design* em interfaces visuais de software pode contribuir para a construção de um ambiente digital mais seguro e confiável, aumentando a confiança dos usuários e beneficiando a sociedade como um todo (Cavoukian, 2011).

Diante do contexto exposto, a questão de pesquisa que norteia este trabalho é: Como aplicar oconceito de *privacy by design* e da norma ISSO/IEC 29134:2017 para implementar conformidade com a LGPD em interfaces visuais de software?

Interfaces são partes de um programa que realizam a comunicação com o mundo exterior, permitindo a interação entre o usuário e o sistema ou entre sistemas (Dix et al., 2004). Um exemplo de interface é a tela inicial de um aplicativo, onde o usuário pode clicar em botões e acessar diferentes funcionalidades.

O design de uma interface é o que define como um usuário irá interagir com um *software*. Uma boa interface deve ser intuitiva e fácil de usar, além de proporcionar uma experiência agradável ao usuário. Segundo Nielsen (1994), algumas das características fundamentais de uma boa interface incluem a visibilidade do sistema, a correspondência entre o sistema e o mundo real, o controle e a liberdade do usuário, a prevenção de erros, a eficiência e a consistência.

A visibilidade do sistema significa que o usuário deve ser capaz de entender o estado atual dosistema e as possíveis ações disponíveis. A correspondência entre o sistema e o mundo real serefere à utilização de conceitos e linguagem familiares aos usuários, facilitando a compreensãoe a interação. O controle e a liberdade do usuário estão relacionados à capacidade do usuário de navegar e realizar ações no sistema sem restrições desnecessárias.

Problemas em interfaces visuais podem ocorrer quando o design não leva em consideração a privacidade e a segurança dos dados pessoais dos usuários. Por exemplo, uma interface mal projetada pode expor informações sensíveis a terceiros não autorizados ou permitir a coleta dedados sem o consentimento do usuário.

Portanto, é uma boa prática sempre informar claramente aos usuários porque você está coletando dados, como você vai usá-los e por quantotempo você vai mantê-los. Isso pode ser feito por meio de uma declaração de privacidade clara e compreensível, que é apresentada ao usuário no momento da coleta de dados (Nielsen, 1994).

Os atributos que podem influenciar na confiança, segurança e usabilidade da interface incluemclareza, simplicidade, *feedback* adequado, flexibilidade e eficiência (Nielsen, 1994). Boas práticas em interfaces envolvem a aplicação desses atributos, garantindo que a interface seja fácil de usar e que os dados pessoais dos usuários sejam protegidos.

Para traduzir esses atributos em uma interface, é importante considerar os seguintes pontos:

- Clareza: A interface deve ser clara e fácil de entender. Isso pode ser alcançado através do uso de linguagem simples e direta, bem como de ícones e imagens que são facilmentereconhecíveis.
- Simplicidade: A interface deve ser simples e intuitiva. Isso pode ser alcançado atravésdo uso de um layout limpo e organizado, com um número mínimo

de opções e botões.

- *Feedback* adequado: A interface deve fornecer *feedback* adequado ao usuário. Isso pode ser alcançado através do uso de mensagens de erro claras e úteis, bem como de indicadores de progresso e confirmação.
- Flexibilidade: A interface deve ser flexível e adaptável às necessidades do usuário. Isso pode ser alcançado através do uso de opções de personalização e configurações ajustáveis.
- Eficiência: A interface deve ser eficiente e rápida de usar. Isso pode ser alcançado através do uso de atalhos e opções de automação, bem como de um design responsivo que se adapta a diferentes tamanhos de tela e dispositivos.

Para operacionalizar a aplicação do *privacy by design* em interfaces visuais de software, é importante seguir os requisitos estabelecidos pela LGPD, ISO/IEC 29134:2017 e GDPR, além de considerar os princípios de usabilidade e as boas práticas de design de interfaces.

Para abordar a aplicação do *privacy by design* em interfaces visuais de software, é fundamental analisar exemplos e estudos de caso que demonstrem como incorporar efetivamente esses princípios em projetos de interface. Algumas estratégias para aplicar o *privacy by design* em interfaces incluem:

- Transparência e controle do usuário: Informar claramente aos usuários sobre a coleta, uso e armazenamento de dados pessoais, fornecendo opções para gerenciar e controlar essas informações (Cavoukian, 2011).
- Minimização de dados: Coletar apenas os dados estritamente necessários para o funcionamento do sistema e armazená-los pelo tempo mínimo necessário (ISO/IEC 29134:2017).

Esta monografia está organizada em quatro capítulos.

CAPÍTULO 2 - introduz o tema da monografia, estabelecendo o contexto e a importância do estudo. Este capítulo apresenta a problemática, os objetivos da pesquisa e a justificativa do estudo. Aborda a revisão da literatura e a teoria relacionada ao tema da monografia. Este capítulo discute os conceitos de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD, bem como sua aplicação em interfaces gráficas.

CAPÍTULO 3 - descreve a metodologia adotada neste trabalho para investigar aimplementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfacesgráficas. A metodologia de pesquisa é fundamental para qualquer estudo acadêmico, pois fornece o quadro dentro do qual a pesquisa é conduzida e os dados são coletados, analisados einterpretados.

CAPÍTULO 4 – se trata de um capítulo foca em recomendações e boas práticas para interfacescom o foco para que se adequem da melhor forma a LGPD. Nesse capítulo é descrito as principais técnicas, os itens essenciais para gerar a conformidade, exemplos retirados de interfaces reais e famosas no mercado tecnológico.

CAPÍTULO 5 – realiza as conclusões finais sobre o trabalho, confirmando os beneficios e eficacias dos métodos pesquisados que podem ser implementados em interfaces gráficas de software. Tambem é apresentado a contribuição para trabalhos futuros, que podem partir do conteudo pesquisado por este.

2. O REFERENCIAL TEÓRICO

Nesta seção, exploram-se os principais conceitos e teorias que fundamentam este trabalho. O estudo concentra-se em cinco áreas principais: interfaces (com ênfase especial nas interfaces gráficas), *Privacy by Design*, a Lei Geral de Proteção de Dados (LGPD), *Information technology - Security techniques - Guidelines for privacy impact* ISO/IEC 29134:2017 e *Information technology - Online privacy notices and consent* ISO/IEC 29184:2021.

As interfaces, especialmente as interfaces gráficas, servem como a ponte entre os usuários e ossistemas digitais, desempenhando um papel crucial na determinação da eficácia e eficiência com que os usuários interagem com esses sistemas. São examinadas as melhores práticas e princípios de design que contribuem para a criação de interfaces gráficas intuitivas e eficientes.

Em seguida, aborda-se o conceito de *Privacy by Design*, uma abordagem que enfatiza a incorporação de considerações de privacidade desde as primeiras etapas do design de um sistema. Esta abordagem é especialmente relevante no contexto atual, onde a privacidade dos dados se tornou uma preocupação primordial.

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que estabelece diretrizes claras sobre a coleta, armazenamento e processamento de dados pessoais. São discutidas as principais disposições desta lei e suas implicações para o design de sistemas.

Por fim, examinam-se as normas ISO/IEC 29134:2017 e ISO/IEC 29184:2021. A primeira fornece diretrizes para a realização de avaliações de impacto na privacidade, um componente essencial do *Privacy by Design*. A segunda estabelece requisitos e recomendações para a informação de privacidade online fornecida por organizações para as pessoas naturais.

Cada um desses tópicos contribui para a compreensão de como criar sistemas que não apenas atendem às necessidades dos usuários, mas também respeitam seus direitos de privacidade e proteção de dados.

2.1. LGPD

A Lei Geral de Proteção de Dados (LGPD), oficialmente Lei nº 13.709, de 14 de agosto de 2018 [27], é a principal regulamentação brasileira relacionada à proteção de dados pessoais e privacidade, sendo aplicável a todas as organizações que

realizam o tratamento de dados pessoais de usuários no Brasil (Brasil, 2018). No contexto do desenvolvimento de interfaces seguras e a otimização da experiência de uso, a LGPD possui implicações significativas. Entre elas, destacam-se a necessidade de transparência no tratamento de dados, a minimização da coleta de dados, a limitação do uso dos dados para os fins especificados e a garantia de segurança dos dados coletados [28].

A LGPD estabelece princípios e diretrizes que devem ser seguidos no desenvolvimento de interfaces, como transparência, minimização de dados, limitação de propósito e segurança (Brasil, 2018). Por exemplo, a transparência pode ser alcançada ao informar claramente ao usuário como seus dados serão utilizados, por meio de notificações claras e consentimento explícito. A minimização de dados pode ser implementada ao solicitar apenas as informações estritamente necessárias para o serviço ou produto oferecido [29].

Ao adotar esses princípios, projetistas de interface podem criar interfaces que garantam a segurança e a privacidade dos dados pessoais dos usuários, mitigando riscos e evitando violações de privacidade.

A conformidade com a LGPD também pode melhorar a experiência de uso das interfaces, poispromove a transparência e o controle do usuário sobre seus dados pessoais, aumentando a confiança dos usuários na solução e, consequentemente, melhorando a usabilidade e a satisfação com a interface (Nielsen, 1994).

Para desenvolver interfaces gráficas em conformidade com a LGPD, é fundamental levar em consideração a privacidade do usuário e o tratamento de seus dados pessoais. Aqui estão algumas recomendações baseadas na LGPD e em práticas recomendadas de design de interface:

- Transparência: A LGPD enfatiza a importância da transparência no tratamento de dados pessoais. Portanto, é essencial que as interfaces gráficas sejam projetadas de forma a informar claramente aos usuários como seus dados estão sendo coletados, usados e armazenados. Isso pode ser alcançado através de notificações claras e consentimento explícito do usuário (Brasil, 2018). Um exemplo disso seria a inclusão de um *pop-up* ou banner informativo no início da interação do usuário com a interface, explicando como os dados serão usados e solicitando o consentimento do usuário [30].
- Minimização de Dados: A LGPD também destaca a minimização de dados, o que significaque apenas os dados necessários para a finalidade pretendida

devem ser coletados. As interfaces gráficas devem ser projetadas de forma a solicitar apenas as informaçõesnecessárias dos usuários (Brasil, 2018). Por exemplo, se um site está vendendo um produto, ele deve solicitar apenas as informações necessárias para a transação, como nome, endereçode entrega e detalhes de pagamento, e não informações irrelevantes.

- Segurança: A segurança dos dados do usuário é um componente crítico da experiência do usuário. Pesquisas indicam que a preocupação dos usuários com a segurança e a privacidade dos seus dados pode afetar sua percepção e uso de um sistema (Bélanger & Crossler, 2011). Portanto, a implementação de medidas de segurança robustas, como a criptografia de dados, autenticação de dois fatores e firewalls, conforme recomendado pelaLGPD, pode melhorar a confiança do usuário e, consequentemente, a experiência do usuário [31].
- Conformidade com a Legislação: A conformidade com a LGPD pode melhorar a experiência de uso das interfaces, pois promove a transparência e o controle do usuário sobre seus dados pessoais, aumentando a confiança dos usuários na solução e, consequentemente, melhorando a usabilidade e a satisfação com a interface (Nielsen, 1994).

Portanto, a LGPD desempenha um papel importante no desenvolvimento de interfaces segurase na otimização da experiência de uso, contribuindo para a criação de sistemas de informaçãoe tecnologia mais confiáveis e responsáveis. Em síntese, a LGPD não apenas protege a privacidade e os dados pessoais dos usuários, mas também serve como um guia para o desenvolvimento de interfaces mais seguras, transparentes e centradas no usuário, melhorando a experiência geral do usuário e a confiança na tecnologia.

2.2. Interfaces

As interfaces são elementos cruciais na interação entre usuários e programas, permitindo a comunicação entre o sistema e o mundo exterior. Existem diversos tipos de interfaces,incluindo interfaces de texto, interfaces gráficas e interfaces de voz (Dix et al., 2004).

- Interfaces de texto: São as mais antigas e simples, onde a interação ocorre através de comandosde texto inseridos pelo usuário. Um exemplo clássico é o terminal do sistema operacional Linux, onde todas as operações são realizadas através de comandos de texto (Dix et al., 2004).

- Interfaces gráficas: Também conhecidas como GUI (*Graphical User Interface*), são interfacesonde a interação ocorre através de elementos gráficos como botões, menus e ícones. Um exemplo é o sistema operacional Windows, que permite ao usuário interagir com o sistema através de janelas, ícones e menus (Dix et al., 2004).
- Interfaces de voz: São interfaces onde a interação ocorre através de comandos de voz. Um exemplo é a assistente virtual Siri, da Apple, que permite ao usuário interagir com o sistema através de comandos de voz (Dix et al., 2004).

Entre os diversos tipos de interfaces, as interfaces visuais de software se destacam pela sua importância, uma vez que influenciam diretamente a experiência do usuário. A experiência dousuário, também conhecida pela sigla em inglês UX (*User Experience*), diz respeito à percepção global e à resposta de um usuário a um produto, sistema ou serviço. Isso engloba as emoções, crenças, preferências, percepções físicas e psicológicas, comportamentos e realizações do usuário antes, durante e após o uso (ISO 9241-210, 2010). Um exemplo de boaexperiência do usuário é quando um site é de fácil navegação, intuitivo e visualmente agradável.

Uma interface visual bem projetada tem o potencial de aumentar a eficiência, produtividade e usabilidade de um software para o usuário. A eficiência pode ser potencializada por meio de um design que reduza o tempo necessário para a realização de tarefas. Isso pode ser alcançado,por exemplo, por meio de atalhos de teclado (Shneiderman et al., 2016). A produtividade podeser aprimorada por meio de um design que permita ao usuário realizar mais tarefas em menostempo, como a inclusão de recursos de automação. A usabilidade se refere à facilidade com que um usuário pode aprender e usar o software. Um design intuitivo e consistente, com elementos familiares e *feedback* claro, pode melhorar a usabilidade (Nielsen, 1994).

Por outro lado, uma interface mal projetada pode resultar em frustração e desistência do usuário. Isso pode ocorrer quando a interface é confusa, difícil de navegar ou inconsistente. Por exemplo, se os botões não estão onde o usuário espera que estejam, ou se a interface muda drasticamente de uma página para outra, o usuário pode ficar frustrado e abandonar o software. Além disso, se a interface é lenta ou propensa a erros, isso pode levar a uma experiência de usuário negativa (Nielsen, 1994). Para compor uma interface amigável, é necessário considerar diversos conceitos, como a visibilidade do sistema, correspondência com o mundo real, controle e liberdade do usuário, prevenção de erros, eficiência e consistência (Nielsen,

1994).

Exemplos de interfaces com excelência em design incluem:

2.2.1. Apple iOS:

O sistema operacional móvel da Apple, o iOS, é amplamente reconhecido por sua interface intuitiva e esteticamente agradável. A consistência no design dos elementos e a atenção aos detalhes proporcionam uma experiência fluida e eficiente para os usuários (Apple Inc., 2021).

Por exemplo, a tela inicial do iOS apresenta uma grade de ícones de aplicativos que são facilmente reconhecíveis e acessíveis, como pode ser visto na seguinte imagem:

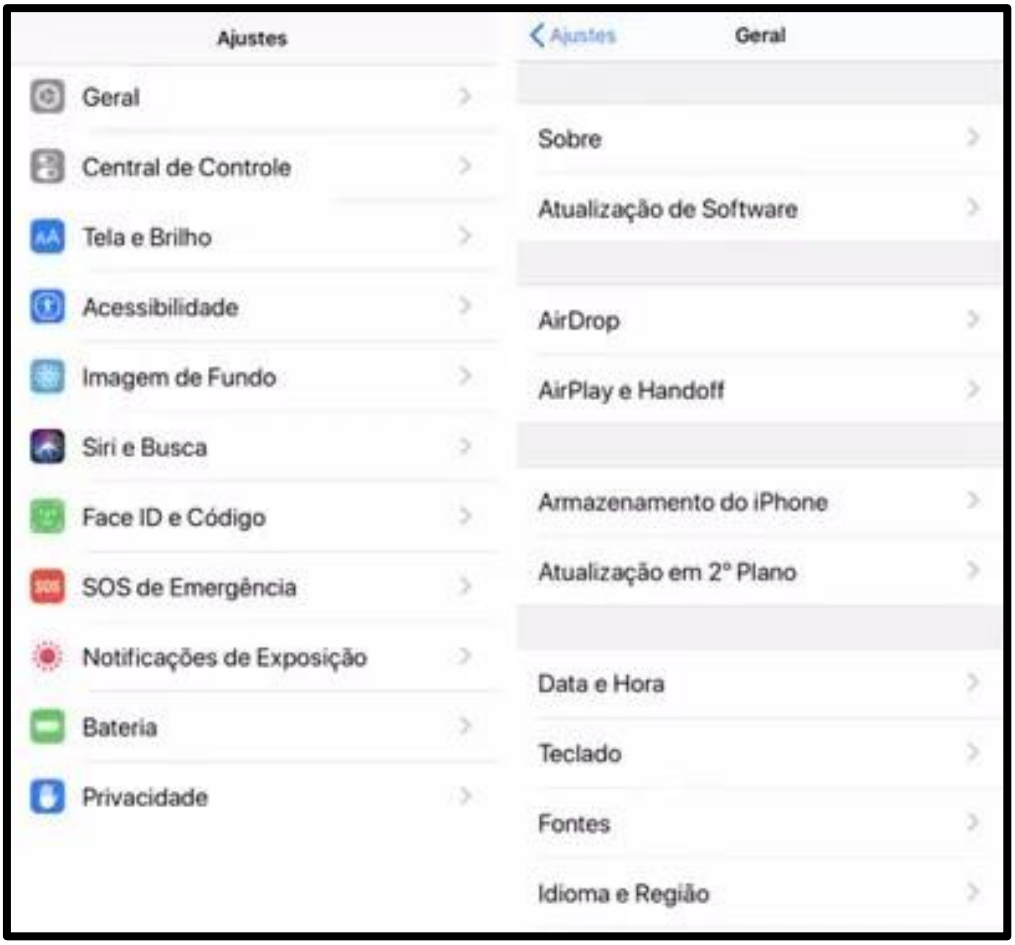
Figura 1 – Tela inicial iOS.

Fonte: https://support.apple.com/pt-br/HT207122

Um dos pontos fortes do iOS é o seu design minimalista e limpo, que facilita a localização e autilização de aplicativos e funções (Lidwell, Holden & Butler, 2010). A interface do usuário éprojetada para ser simples e direta, com ícones grandes e textos legíveis, tornando a navegaçãointuitiva mesmo para usuários novatos (Nielsen, 1994).

Por exemplo, a tela de configurações do iOS é organizada de maneira clara e concisa, com ícones e textos grandes que facilitam a localização das diferentes opções, como pode ser visto na seguinte imagem:

Figura 2 - Imagem da tela de configurações do iOS.

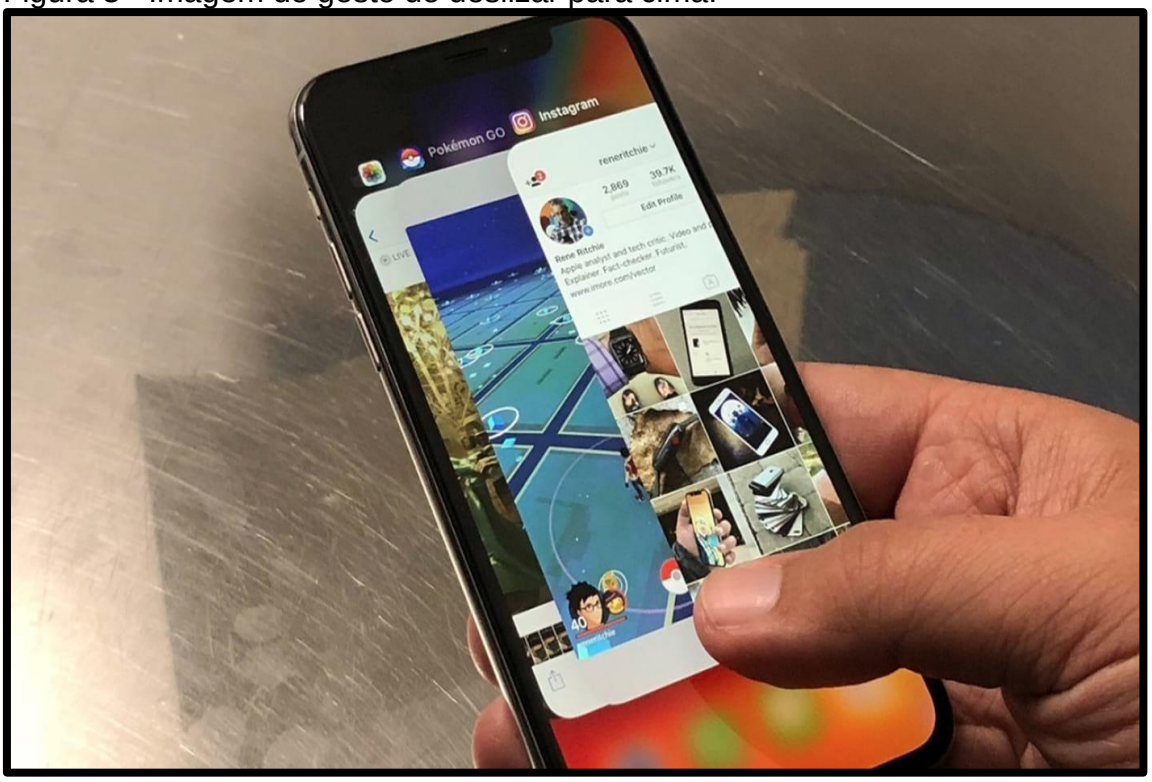


Fonte: https://br.ccm.net/faq/13225-o-aplicativo-ajustes-do-iphone

Além disso, o iOS se destaca pela sua consistência. Os elementos da interface do usuário, comobotões, ícones e gestos, mantêm-se consistentes em todo o sistema e entre diferentes versões do iOS. Isso permite que os usuários aprendam rapidamente como o sistema funciona e reduza curva de aprendizado (Shneiderman et al., 2016). Por exemplo, o gesto de deslizar para cimapara acessar o centro de

controle é consistente em todos os dispositivos iOS, como pode ser visto na seguinte imagem:

Figura 3 - Imagem do gesto de deslizar para cima.

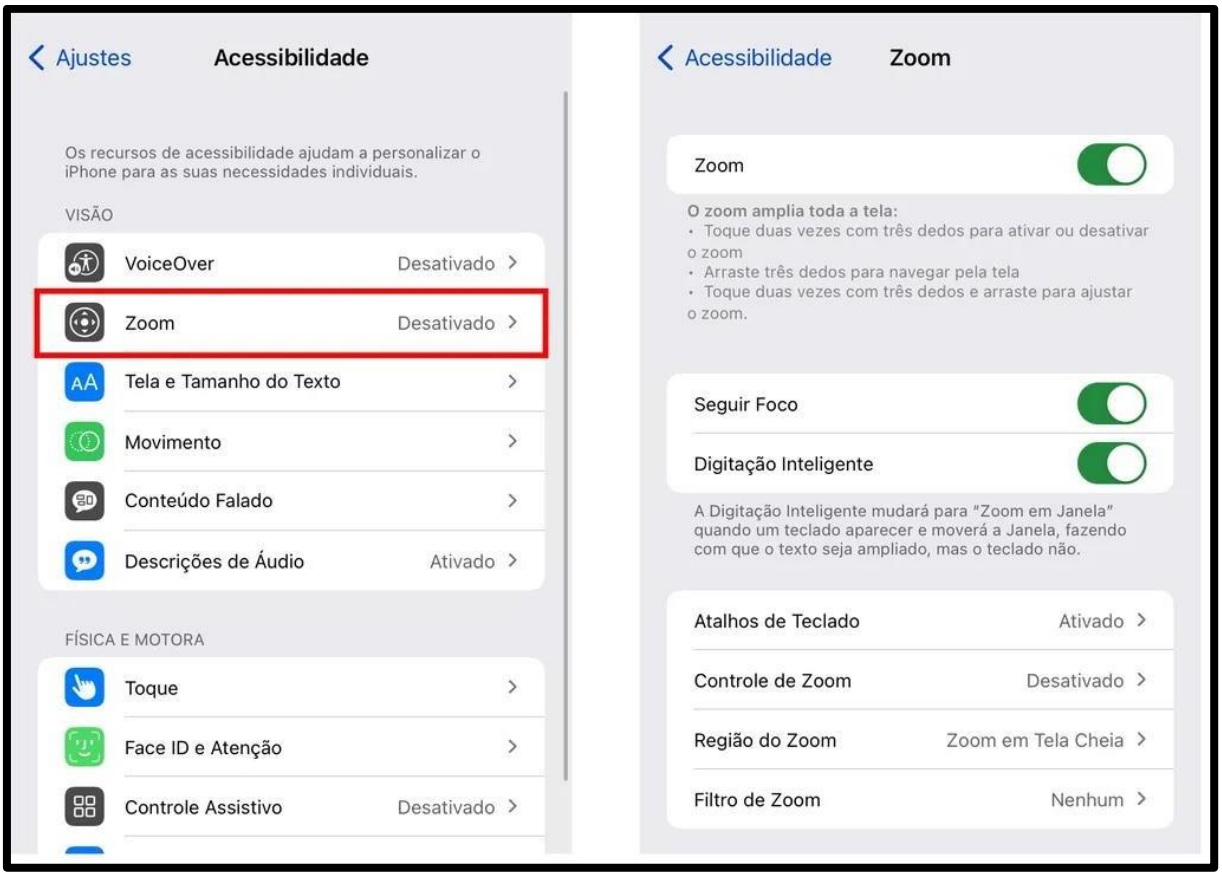


Fonte:https://www.oficinadanet.com.br/apple/29664-aplicativos-nao-abrem-ou-fecham-sozinhos-no-iphone-saiba-como-resolver-este-problema

Outro aspecto que torna o iOS uma interface de usuário superior é a sua resposta rápida e fluida. O sistema é otimizado para garantir que as ações do usuário sejam respondidas imediatamente, proporcionando uma sensação de controle e previsibilidade (Norman, 2013).

Por fim, a Apple também se destaca na implementação de recursos de acessibilidade em seu sistema operacional. O iOS inclui uma variedade de recursos que permitem que pessoas com deficiências visuais, auditivas, físicas e de aprendizagem utilizem o dispositivo de maneira eficaz (Apple Inc., 2021). Alguns exemplos desses recursos incluem o VoiceOver, que lê em voz alta o conteúdo da tela, e o Zoom, que permite ampliar a tela para facilitar a visualização. Além disso, o iOS também inclui recursos para pessoas com deficiências auditivas, como a compatibilidade com aparelhos auditivos e a transcrição de voz em texto.

Figura 4 - Imagem dos recursos de acessibilidade do iOS.



Fonte: https://canaltech.com.br/ios/melhores-recursos-de-acessibilidade-ios-iphone/

Em termos de recomendações, ao projetar uma interface de usuário, é importante considerar osprincípios de design que tornam o iOS bem-sucedido. Isso inclui a manutenção da consistência,a simplificação da interface, a garantia de uma resposta rápida e a inclusão de recursos de acessibilidade. Por exemplo, ao projetar a interface de um novo aplicativo, você pode seguir asdiretrizes de design da Apple para garantir a consistência com o restante do sistema operacional. Isso pode incluir o uso de ícones e textos semelhantes aos do iOS, a organização de elementos de maneira clara e intuitiva e a inclusão de recursos de acessibilidade, como suporte para o *VoiceOver* e o *Zoom*. Além disso, é importante garantir que o aplicativo responda rapidamente às ações do usuário para proporcionar uma sensação de controle e previsibilidade.

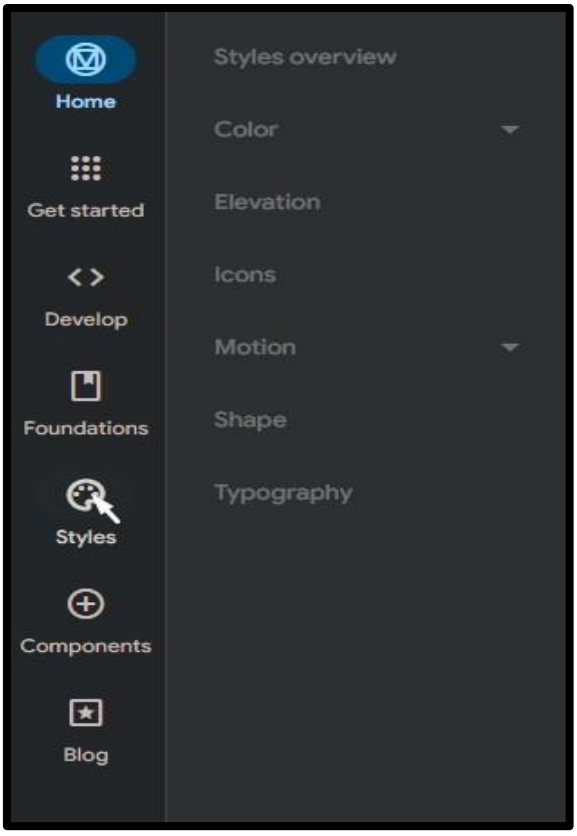
2.2.2. Google Material Design:

O Material Design é uma linguagem de design desenvolvida pelo Google, que tem como objetivo criar interfaces modernas e responsivas, reage de forma rápida e eficiente a um estímulo ou comando. A abordagem do Material Design utiliza cores,

tipografia e hierarquia visual para melhorar a experiência do usuário em diversos dispositivos e plataformas (Google Inc., 2021). A hierarquia visual é um princípio de design que é usado para indicar a importânciados elementos em uma interface. Isso é geralmente feito através do uso de tamanho, cor e posição. Por exemplo, os elementos mais importantes podem ser feitos maiores, mais coloridos ou colocados em uma posição mais proeminente na tela.

O Google Material Design se destaca por sua abordagem baseada em papel e tinta digital, que cria uma sensação de profundidade e realismo. Isso é alcançado através do uso de sombras, movimentos e transições fluidas que imitam o comportamento de objetos físicos no mundo real (Liu, 2017). Por exemplo, os botões no Material Design são projetados para se elevar quando pressionados, imitando a forma como um botão físico se comportaria. Você pode ver um exemplo disso na seguinte imagem:

Figura 5 - Imagem do Material Design.



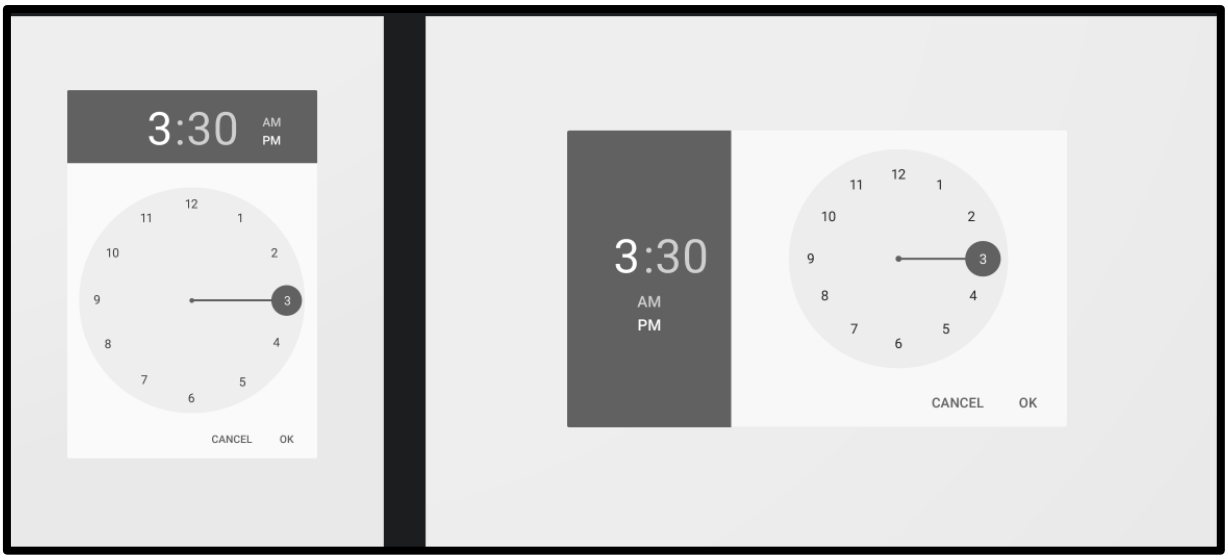
Fonte: Site do Google Material Desgin: https://m3.material.io/

Além disso, o Google Material Design utiliza uma paleta de cores vibrantes e

contrastantes para melhorar a legibilidade e a estética da interface. A tipografia é cuidadosamente selecionada para ser legível em uma variedade de tamanhos de tela e resoluções, garantindo que a interface seja acessível e agradável em todos os dispositivos (Google Inc., 2021).

O Google Material Design também se destaca pela sua flexibilidade e adaptabilidade. Ele foi projetado para ser responsivo, o que significa que a interface se ajusta automaticamente para se adequar a diferentes tamanhos de tela e orientações. Isso garante que a interface seja eficaz e fácil de usar, independentemente do dispositivo que o usuário esteja usando (Liu, 2017). Por exemplo, a seguinte imagem mostra como uma interface do Material Design se ajusta a diferentes tamanhos de tela:

Figura 6 - Imagem da interface responsiva do Google Material Design.

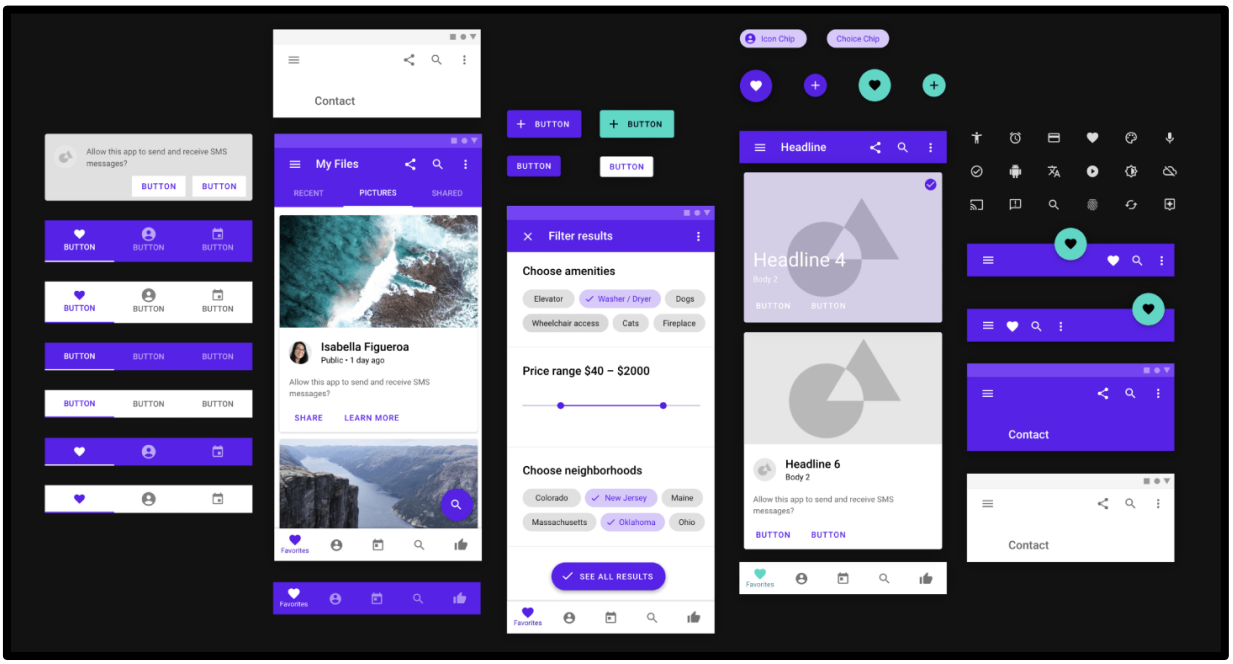


Fonte: https://m1.material.io/layout/responsive-ui.html#responsive-ui-patterns

Em termos de recomendações, ao projetar uma interface de usuário, é benéfico considerar os princípios de design que tornam o Google Material Design bem-sucedido. Isso inclui a criação de uma sensação de profundidade e realismo, o uso de cores vibrantes e contrastantes, a seleção cuidadosa da tipografia e a garantia de que a interface seja responsiva e adaptável. Por exemplo, ao projetar a interface de um novo aplicativo, você pode seguir as diretrizes do Google Material Design para criar uma interface intuitiva e agradável. Isso pode incluir o uso de sombras e movimentos para criar uma sensação de profundidade, a seleção de cores vibrantes e contrastantes

para melhorar a legibilidade, a escolha de uma tipografia que seja legível em diferentes tamanhos de tela e a garantia de que a interface se ajuste automaticamente a diferentes tamanhos de telae orientações. A seguinte imagem mostra um exemplo de como esses princípios podem ser aplicados na prática:

Figura 7 - Imagem de um exemplo de interface feita no Google Material Design.



Fonte: https://www.uxpin.com/material-design-ui-kit

2.2.3. Airbnb:

O Airbnb, Inc. se destaca por sua interface intuitiva e fácil de usar. A navegação é clara e direta, com categorias bem definidas e um sistema de busca eficiente. Por exemplo, na página inicial do Airbnb, os usuários podem facilmente selecionar o tipo de acomodação que estão procurando, inserir o destino e as datas e filtrar os resultados com base em suas preferências. Isso está alinhado com os princípios de usabilidade de Nielsen, que enfatizam a importância deuma estrutura de navegação clara para a experiência do usuário (Nielsen, 1994).

Além disso, o Airbnb utiliza imagens de alta qualidade e descrições detalhadas para apresentar as acomodações. Isso não apenas torna a interface visualmente agradável, mas também forneceaos usuários as informações necessárias para tomar uma decisão informada. Estudos mostramque a apresentação visual e a qualidade das informações são fatores críticos na decisão de reserva dos usuários (Guttentag,

2015).

No contexto da Lei Geral d Proteção de Dados (LGPD), a transparência e a clareza das informações são fundamentais. Assim, ao implementar uma interface LGPD, é importante fornecer descrições claras e detalhadas sobre como os dados do usuário serão usados e garantir que o usuário tenha controle total sobre suas informações. Isso pode ser feito através de uma tela de consentimento, onde o usuário pode optar por permitir ou negar o uso de seus dados.

O Airbnb, Inc. também implementa um sistema de avaliação transparente, permitindo que os usuários vejam as avaliações e comentários de outros hóspedes. Isso aumenta a confiança dosusuários no sistema e ajuda na tomada de decisões (Ert et al., 2016).

Em termos de recomendações, ao projetar uma interface de usuário, é benéfico considerar os princípios de design que tornam a interface do Airbnb bem-sucedida. Isso inclui a criação de uma navegação clara e intuitiva, a utilização de imagens de alta qualidade e descrições detalhadas, e a implementação de um sistema de avaliação transparente.

No contexto da LGPD, esses princípios podem ser traduzidos em uma interface que seja transparente sobre o uso dos dados do usuário, que forneça ao usuário controle total sobre suasinformações e que seja clara e fácil de usar. Por exemplo, a interface pode incluir uma tela de consentimento clara, um sistema de configurações de privacidade fácil de usar e descrições detalhadas de como os dados do usuário serão usados.

2.3. ISO/IEC 29134:2017 Information technology - Security techniques - Guidelines for privacy impact

A norma ISO/IEC 29134:2017 estabelece diretrizes para a realização de Avaliações de Impactona Privacidade (PIAs) em sistemas de informação e tecnologia (ISO/IEC, 2017). Embora a norma não se concentre especificamente em interfaces de usuário, a segurança e a privacidadedos dados do usuário são aspectos fundamentais da experiência do usuário. Portanto, a aplicação das diretrizes desta norma pode contribuir indiretamente para o desenvolvimento deinterfaces seguras e a otimização da experiência de uso.

A segurança dos dados do usuário é um componente crítico da experiência do usuário. Pesquisas indicam que a preocupação dos usuários com a segurança e a

privacidade dos seus dados pode afetar sua percepção e uso de um sistema (Bélanger & Crossler, 2011). Portanto, a implementação de medidas de segurança robustas, conforme recomendado pela ISO/IEC 29134:2017, pode melhorar a confiança do usuário e, consequentemente, a experiência do usuário.

Além disso, a conformidade com as regulamentações de privacidade, como a *General Data Protection Regulation* (GDPR) da União Europeia, é cada vez mais importante. A ISO/IEC 29134:2017 pode ajudar as organizações a cumprir essas regulamentações, realizando avaliações de impacto na privacidade para identificar e mitigar os riscos de privacidade (ISO/IEC, 2017).

Ao seguir a ISO/IEC 29134:2017 no desenvolvimento de interfaces, os projetistas podem identificar e gerenciar os riscos relacionados à privacidade dos dados pessoais dos usuários. Por exemplo, um risco potencial pode ser a coleta excessiva de dados, onde mais dados são coletados do que o necessário para a função pretendida. Isso pode ser mitigado seguindo o princípio de minimização de dados, onde apenas os dados necessários são coletados.

No entanto, mesmo com a aplicação rigorosa dessas diretrizes, ainda existem riscos potenciais que devem ser considerados.

- Violação de Dados: Mesmo com medidas de segurança robustas, sempre existe o risco de uma violação de dados, onde informações pessoais podem ser acessadas por partes não autorizadas (ISO/IEC 27001, 2013). No contexto de uma interface de usuário, uma violação de dados pode ocorrer se um invasor conseguir acessar o banco de dados que armazena as informações do usuário.
- Falhas de Segurança: Falhas no software ou hardware podem levar a brechas de segurança, permitindo o acesso não autorizado a dados pessoais (ISO/IEC 27002, 2013). No contexto de uma interface de usuário, uma falha de segurança pode ocorrer se um erro no código do software permitir que um invasor contorne as medidas de segurança.
- Erros Humanos: Erros humanos que podem resultar na exposição de dados pessoais são bastante comuns e podem ocorrer de diversas maneiras. Por exemplo, um usuário pode, sem querer, compartilhar informações pessoais demais nas redes sociais, como fotos que revelam detalhes sobre sua localização ou rotina. Outro erro comum é o envio de um e- mail pessoal pelo endereço profissional, ou vice-versa, o que pode levar à divulgação de informações sensíveis para pessoas não

autorizadas.

- Além disso, um erro comum que pode resultar na exposição de dados pessoais é a escolhade senhas fáceis de adivinhar. Senhas que incluem informações pessoais, como datas de nascimento ou nomes de animais de estimação, podem ser facilmente descobertas por invasores.
- A norma ISO/IEC 29134:2017 fornece uma série de diretrizes para a realização deAvaliações de Impacto na Privacidade (PIAs). Para exemplificar, aqui estão algumas situações:
- Identificação de Processamento de Dados Pessoais: Por exemplo, um aplicativo de saúde pode coletar e armazenar informações pessoais, como idade, peso, altura e condições de saúde do usuário. É importante que esses processos sejam claramente identificados e que os usuários sejam informados sobre eles.
- Avaliação de Riscos de Privacidade: Por exemplo, se um aplicativo de saúde armazena informações sensíveis do usuário, como registros médicos, há um risco de que essas informações possam ser acessadas por partes não autorizadas em caso de uma violação dedados. A avaliação de riscos de privacidade pode ajudar a identificar esses riscos e desenvolver estratégias para mitigá-los.
- Mitigação de Riscos: Por exemplo, para mitigar os riscos identificados, o aplicativo de saúde pode implementar medidas de segurança robustas, como criptografia de dados, e desenvolver políticas de privacidade claras que informem os usuários sobre como seus dados são coletados, usados e armazenados.
- Monitoramento e Revisão: Monitorar regularmente a eficácia das medidas de mitigação deriscos e revisar a PIA conforme necessário para garantir que ela permaneça relevante e atualizada.

A norma ISO/IEC 29134:2017 fornece diretrizes para Avaliações de Impacto na Privacidade (PIAs). Para aplicar essas diretrizes ao design e desenvolvimento de interfaces de usuário, vocêprecisaria identificar os elementos de dados que estão sendo coletados, armazenados ou processados pela interface do usuário e avaliar os riscos de privacidade associados a esses elementos de dados. Você também precisaria identificar o contexto em que a interface do usuário será usada e os impactos potenciais na privacidade. Por exemplo, você pode precisar considerar a idade, gênero, localização ou outras características pessoais dos usuários e como

essas informações serão usadas. Depois de identificar os riscos e impactos de privacidade, vocêpode então aplicar as diretrizes da ISO/IEC 29134:2017 para mitigar esses riscos e melhorar aexperiência do usuário.

Por exemplo, se você estiver projetando uma interface de usuário para um aplicativo de mídia social, você pode coletar dados como nome, localização, interesses, etc. dos usuários. Usandoa ISO/IEC 29134:2017, você pode identificar os riscos de privacidade associados à coleta desses dados, como o risco de violação de dados ou uso indevido de informações. Em seguida, você pode aplicar as diretrizes da norma para mitigar esses riscos, como implementar medidasde segurança robustas, como criptografia, e políticas de privacidade claras que informam os usuários sobre como seus dados serão usados.

Além disso, a aplicação dessas diretrizes pode melhorar a experiência de uso das interfaces, pois promove a transparência e o controle do usuário sobre seus dados pessoais. Isso pode serfeito, por exemplo, fornecendo aos usuários opções claras para gerenciar suas configurações de privacidade e consentimento, e informando-os sobre como seus dados serão usados e protegidos. Isso pode aumentar a confiança dos usuários no sistema e, consequentemente, melhorar a usabilidade e a satisfação geral com a interface (Nielsen, 1994).

Portanto, embora a norma ISO/IEC 29134:2017 seja mais diretamente aplicável à construção de sistemas de informação e tecnologia, ela também pode contribuir indiretamente para o desenvolvimento de interfaces de usuário seguras e eficazes. Ao seguir as diretrizes da norma,os designers de interface do usuário podem identificar e gerenciar os riscos de privacidade, melhorar a transparência e o controle do usuário sobre seus dados pessoais, e assim melhorara experiência geral do usuário.

Além disso, a conformidade com as regulamentações de privacidade, como a *General Data Protection Regulation* (GDPR) da União Europeia, é cada vez mais importante. A ISO/IEC 29134:2017 pode ajudar as organizações a cumprir essas regulamentações, realizando avaliações de impacto na privacidade para identificar e mitigar os riscos de privacidade. Por exemplo, a norma pode orientar as organizações a implementar medidas como a anonimizaçãode dados e a minimização de dados, que são requisitos chave do GDPR.

2.4. Privacy by Design

O conceito de "*privacy by design*" (privacidade desde o início do design),

proposto por Ann Cavoukian (2011), aborda a incorporação da privacidade e proteção de dados pessoais desde o início do processo de design de produtos e serviços. Ao aplicar o *privacy by design* no desenvolvimento de interfaces seguras, os projetistas podem garantir a otimização da experiência de uso e a conformidade com as regulamentações de privacidade.

A aplicação do *privacy by design* em interfaces visuais de software implica na implementação de práticas de privacidade e segurança em todos os aspectos do design, desde a coleta e armazenamento de dados até a apresentação de informações e funcionalidades ao usuário (Cavoukian, 2011). Essa abordagem permite que os usuários tenham maior controle e transparência sobre seus dados pessoais, o que, por sua vez, aumenta a confiança na solução e melhora a usabilidade (Nielsen, 1994).

Além disso, o *privacy by design* contribui para a criação de interfaces mais seguras ao promover a minimização de dados, a limitação de propósito e a implementação de medidas de segurança adequadas (Cavoukian, 2011). Por exemplo, a minimização de dados pode ser alcançada ao coletar apenas as informações estritamente necessárias para a funcionalidade em questão. A limitação de propósito pode ser garantida ao usar os dados coletados apenas para os fins especificados e nada mais. Medidas de segurança adequadas podem incluir a criptografia de dados, autenticação de dois fatores e firewalls.

Um estudo de 2018 publicado no *Journal of Information Systems Applied Research* (JISAR) descobriu que a aplicação do *privacy by design* em interfaces de usuário pode melhorar significativamente a confiança do usuário e a satisfação geral com a interface. O estudo analisou várias interfaces de usuário que aplicaram os princípios do *privacy by design* e descobriu que essas interfaces tinham taxas significativamente mais altas de satisfação do usuário em comparação com interfaces que não aplicaram esses princípios (JISAR, 2018).

Além disso, o *privacy by design* também pode ajudar a evitar problemas legais e de conformidade. Por exemplo, a *General Data Protection Regulation* (GDPR) da União Europeia exige que as organizações implementem medidas técnicas e organizacionais adequadas para proteger os dados pessoais dos usuários. A aplicação do *privacy by design* pode ajudar as organizações a cumprir esses requisitos e evitar penalidades potencialmente severas por não conformidade (GDPR, 2018). Isso pode ser alcançado ao incorporar práticas de privacidade e segurança desde o início do

processo de design, garantindo que a privacidade seja uma consideração fundamental em todas as etapas do desenvolvimento de produtos e serviços.

Portanto, a aplicação do *privacy by design* no desenvolvimento de interfaces de usuário pode trazer benefícios significativos, tanto em termos de melhorar a experiência do usuário quanto de garantir a segurança e a privacidade dos dados do usuário.

A aplicação dos princípios de minimização de dados, limitação de propósito e implementação de medidas de segurança adequadas pode ser traduzida em uma interface de várias maneiras:

- Minimização de Dados: Este princípio sugere que apenas os dados necessários para a finalidade específica devem ser coletados. Na interface do usuário, isso pode ser implementado solicitando apenas as informações estritamente necessárias para a funcionalidade em questão. Por exemplo, se um usuário está se inscrevendo para um newsletter, apenas o endereço de e-mail é necessário, não há necessidade de coletar informações adicionais como idade, gênero ou localização. Isso não apenas protege a privacidade do usuário, mas também simplifica a interface e melhora a experiência do usuário.
- Limitação de Propósito: Este princípio implica que os dados coletados devem ser usados apenas para o propósito declarado e nada mais. Isso pode ser comunicado ao usuário por meio de uma política de privacidade clara e compreensível, que é facilmente acessível a partir da interface do usuário. Além disso, a interface pode fornecer controles para o usuário gerenciar como seus dados são usados. Por exemplo, o usuário pode ter a opção de optar por não compartilhar seus dados para fins de marketing.
- Implementação de Medidas de Segurança Adequadas: Este princípio envolve a proteção dos dados coletados contra acesso não autorizado ou perda. Na interface do usuário, isso pode ser implementado através de recursos como autenticação de dois fatores, criptografia de dados e notificações de segurança. Por exemplo, o Google Drive implementa a autenticação de dois fatores para proteger os dados do usuário, enquanto o WhatsApp usa criptografia de ponta a ponta para garantir que apenas o remetente e o destinatário possam ler as mensagens.

Esses princípios, quando implementados corretamente, podem tornar a interface mais segura e melhorar a confiança do usuário no sistema. Além disso, eles podem ajudar a garantir a conformidade com as regulamentações de privacidade,

como a GDPR e a LGPD.

Essas práticas podem reduzir os riscos associados à privacidade e proteger os usuários contra violações de dados. Implementar o *Privacy by Design* em interfaces gráficas envolve uma série de práticas e considerações. Aqui estão algumas maneiras específicas de como isso pode ser feito:

- Transparência e Controle do Usuário: As interfaces devem ser projetadas de forma a tornar as configurações de privacidade e as opções de consentimento claramente visíveis e fáceis de usar. Isso permite que os usuários tenham controle sobre seus dados pessoais e entendam como eles estão sendo usados. Por exemplo, uma interface pode incluir uma seção claramente marcada nas configurações onde os usuários podem ver quais dados estão sendo coletados e podem optar por desativar a coleta de certos tipos de dados.
- Minimização de Dados: As interfaces devem ser projetadas para coletar apenas os dados necessários para a funcionalidade do produto ou serviço. Isso pode ser alcançado através de práticas como a solicitação de permissões em tempo de execução, onde o usuário é solicitado a fornecer acesso a determinados dados apenas quando necessário. Por exemplo, um aplicativo pode solicitar acesso à localização do usuário apenas quando o usuário está usando um recurso que requer essa informação, como um mapa ou serviço de entrega.
- Segurança Incorporada: As interfaces devem ser projetadas com segurança em mente desde o início. Isso pode envolver a implementação de criptografia de dados, autenticação de dois fatores e outras medidas de segurança para proteger os dados do usuário. Por exemplo, uma interface pode incluir uma opção para autenticação de dois fatores, que requer que o usuário forneça duas formas de identificação para acessar sua conta. Isso pode incluir algo que o usuário sabe (como uma senha), algo que o usuário tem (como um telefone celular para receber um código de verificação) e algo que o usuário é (como uma impressão digital ou reconhecimento facial).

Um exemplo real da implementação do *Privacy by Design* em interfaces gráficas pode ser visto no aplicativo de mensagens Signal. O Signal é projetado com a privacidade do usuário em mente, com recursos como criptografia de ponta a ponta e minimização de dados. As configurações de privacidade são claramente visíveis e fáceis de usar, permitindo que os usuários tenham controle sobre seus dados pessoais.

Outro exemplo é o navegador de internet Firefox, desenvolvido pela Mozilla. O Firefox é projetado com uma forte ênfase na privacidade e segurança, com recursos como bloqueio de rastreadores de terceiros, proteção contra *fingerprinting* (método usado para identificar ou rastrear dispositivos ou navegadores individuais com base em características específicas ou configurações únicas) e criptografia de dados. Além disso, o Firefox torna as configurações de privacidade facilmente acessíveis e compreensíveis para os usuários, permitindo-lhes personalizar o nível de proteção de privacidade que desejam.

Esses exemplos demonstram como o *Privacy by Design* pode ser implementado em interfacesgráficas para melhorar a privacidade e a segurança dos dados do usuário, ao mesmo tempo emque proporciona uma experiência de usuário otimizada.

O conceito de "*Privacy by Design*" (Privacidade desde o Design) é fundamental para a criaçãode interfaces gráficas que respeitam a privacidade do usuário. Aqui estão algumas recomendações e boas práticas para a implementação desse conceito:

- Transparência: Assegure-se de que os usuários entendam quais dados estão sendo coletados e por quê. Isso pode ser feito através de uma política de privacidade clara e acessível, bem como notificações na interface do usuário quando os dados estão sendocoletados. Por exemplo, uma interface pode incluir uma seção claramente marcada nasconfigurações onde os usuários podem ver quais dados estão sendo coletados e podemoptar por desativar a coleta de certos tipos de dados.
- Consentimento do Usuário: Sempre obtenha o consentimento do usuário antes de coletar ou usar seus dados. Isso pode ser feito através de caixas de seleção ou promptsna interface do usuário que permitem ao usuário optar por compartilhar seus dados. exemplo, uma interface pode incluir uma caixa de seleção que o usuário deve marcar para concordar com a coleta de dados, ou um prompt que aparece quando o usuário estáprestes a compartilhar dados sensíveis.
- Minimização de Dados: Colete apenas os dados que são absolutamente necessários paraa funcionalidade do seu produto ou serviço. Isso não apenas protege a privacidade do usuário, mas também reduz o risco de violações de dados.
- Segurança Incorporada: Implemente medidas de segurança robustas para proteger os dados do usuário. Isso pode incluir criptografia de dados, autenticação de dois fatores e outras técnicas de segurança.

- Controle do Usuário: Dê aos usuários controle sobre seus próprios dados. Isso pode incluir a capacidade de visualizar, editar e excluir seus próprios dados.
- Design Centrado no Usuário: Ao projetar sua interface, considere a perspectiva do usuário. Isso pode incluir a realização de testes de usabilidade para garantir que sua interface seja intuitiva e fácil de usar.
- Conformidade com a Regulamentação: Certifique-se de que sua interface esteja em conformidade com todas as regulamentações de privacidade relevantes, como a *General Data Protection Regulation* (GDPR) da União Europeia. Por exemplo, uma interface pode incluir uma seção claramente marcada nas configurações onde os usuários podem ver quais dados estão sendo coletados e podem optar por desativar a coleta de certos tipos de dados.

Implementar o *Privacy by Design* suas interfaces gráficas não apenas protegerá a privacidade de seus usuários, mas também poderá melhorar a confiança do usuário em seu produto ou serviço.

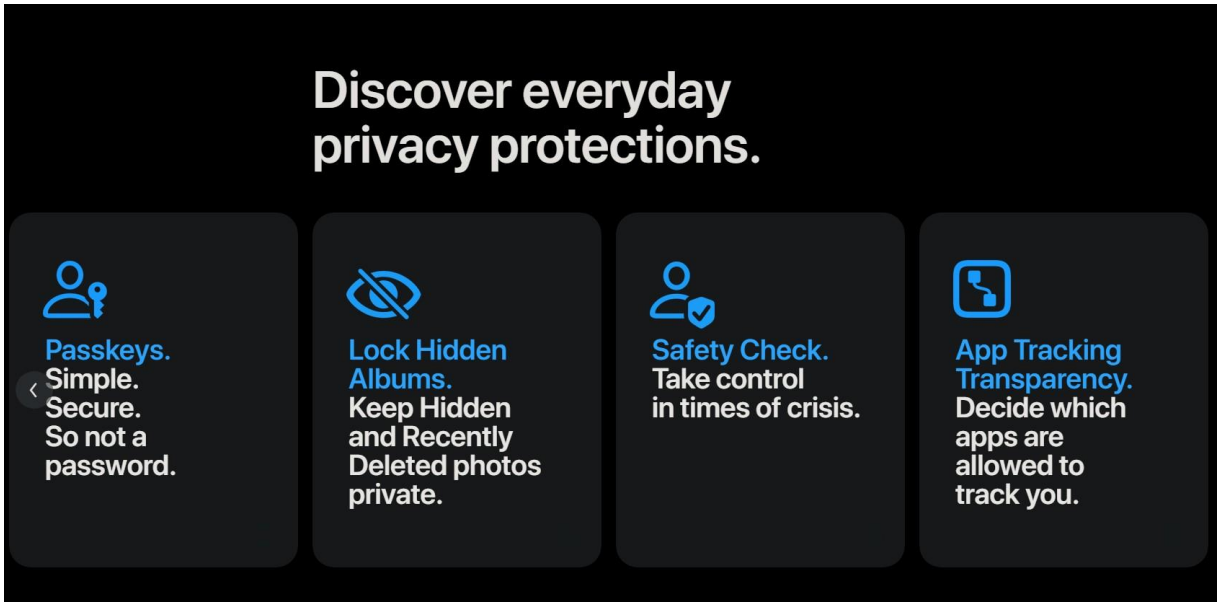
2.5. ISO/IEC 29184:2021 Information technology - Online privacy notices and consent

A ISO/IEC 29184:2021, conhecida como "Tecnologia da informação - Avisos de privacidade on-line e consentimento", é um padrão internacional que orienta as organizações sobre como comunicar suas práticas de privacidade e obter o consentimento dos usuários para o uso de suas informações pessoais (ISO, 2021). Este padrão é centrado no usuário, priorizando transparência, clareza e facilidade de compreensão das informações de privacidade. Ele orienta as organizações a fornecer detalhes claros sobre suas práticas de privacidade, incluindo o tipo de dados coletados, os propósitos da coleta, a duração da retenção de dados e com quem os dados podem ser compartilhados (ISO, 2021).

A aplicação desta norma em interfaces gráficas pode ser realizada através da implementação de avisos de privacidade claros e compreensíveis. Isso pode envolver o uso de ícones padronizados para representar diferentes tipos de dados coletados, a apresentação de informações de privacidade em linguagem simples e a inclusão de opções claras para o usuário consentir ou recusar a coleta de dados. Um exemplo disso pode ser encontrado no site da Apple, onde eles usam ícones para representar diferentes tipos de dados coletados e apresentam suas políticas de privacidade de

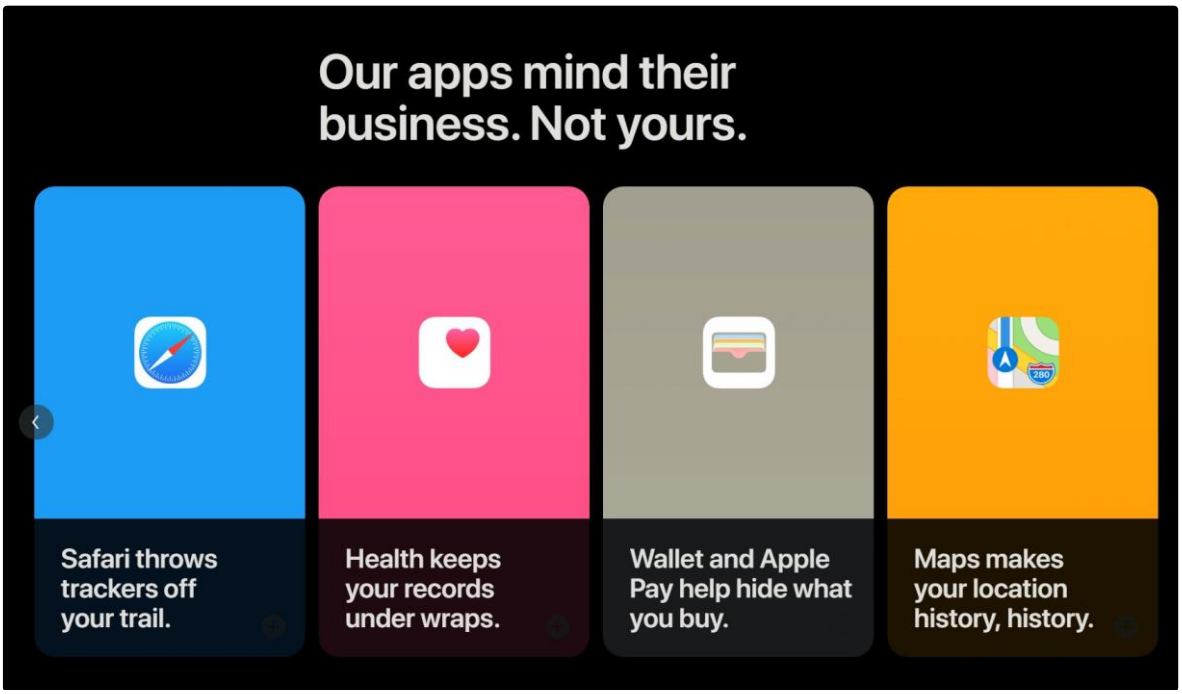
maneira clara e compreensível.

Figura 8 - Informações dos serviços de proteção a privacidade que a Apple fornece



em seu sistema.
Fonte: https://www.apple.com/privacy/

Figura 9 – Informações de segurança de privacidade presente nos próprios aplicativos da Apple.



Fonte: https://www.apple.com/privacy/

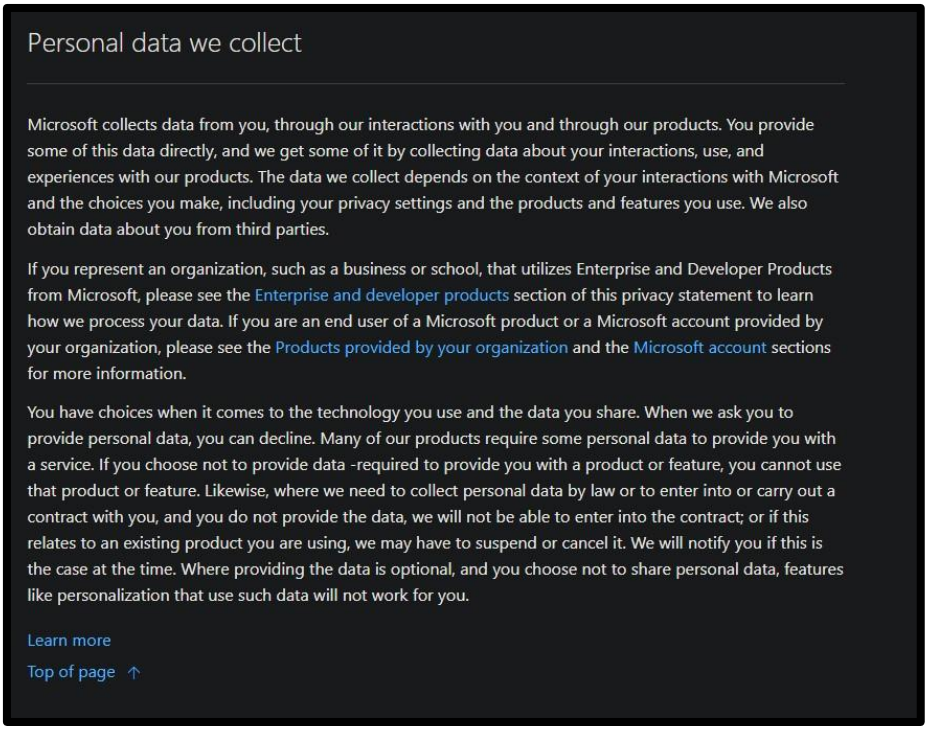
A implementação da ISO/IEC 29184:2021 pode trazer vários benefícios, como

aumentar a confiança do usuário na organização, melhorar a transparência das práticas de privacidade e facilitar a conformidade com os regulamentos de privacidade. No entanto, também pode exigiresforços significativos de design e desenvolvimento para implementar adequadamente os avisos de privacidade e as opções de consentimento. Esses esforços podem incluir a criação de ícones padronizados, a redação de avisos de privacidade em linguagem simples e a implementação de opções de consentimento claras e compreensíveis.

A norma oferece vantagens como a promoção da transparência, a melhoria da confiança do usuário e a facilitação do cumprimento de regulamentos de privacidade. Além disso, a norma pode ajudar as organizações a evitar penalidades por não conformidade, melhorar a eficiência ao reduzir a necessidade de consentimentos repetidos e melhorar a experiência do usuário ao proporcionar maior controle sobre suas informações pessoais.

Para interfaces gráficas, a norma recomenda a implementação de avisos de privacidade clarose compreensíveis, o uso de ícones padronizados para representar diferentes tipos de dados coletados, a apresentação de informações de privacidade em linguagem simples e a inclusão de opções claras para o usuário consentir ou recusar a coleta de dados. Por exemplo, o site da Microsoft implementa essas recomendações ao apresentar suas políticas de privacidade de maneira clara e compreensível, usando ícones para representar diferentes tipos de dados coletados e ornecendo opções claras para o usuário consentir ou recusar a coleta de dados.

Figura 10 – Site da Microsoft na parte de especificação de que tipo de dados eles coletam.



Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use, and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices you make, including your privacy settings and the products and features you use. We also obtain data about you from third parties.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the Enterprise and developer products section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organization, please see the Products provided by your organization and the Microsoft account sections for more information.

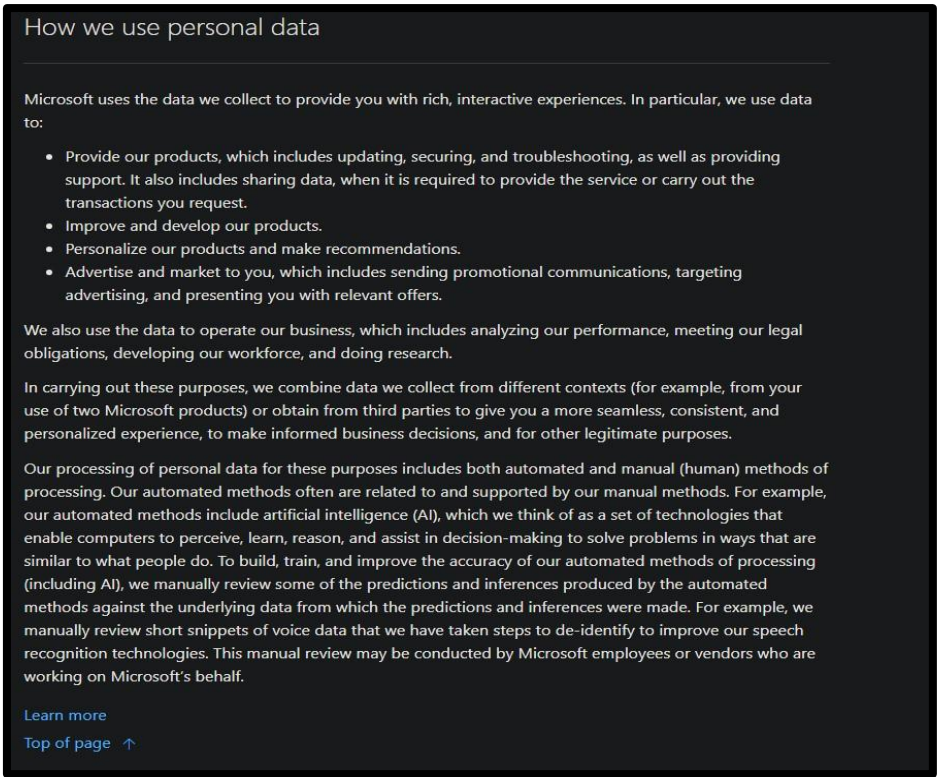
You have choices when it comes to the technology you use and the data you share. When we ask you to provide personal data, you can decline. Many of our products require some personal data to provide you with a service. If you choose not to provide data -required to provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you are using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use such data will not work for you.

Learn more

Top of page ↑

Fonte: https://privacy.microsoft.com/en-us/privacystatement

Figura 11 – Site da Microsoft onde é especificado como eles usam os dados pessoaisfornecidos.



How we use personal data

Microsoft uses the data we collect to provide you with rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you with relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

In carrying out these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products) or obtain from third parties to give you a more seamless, consistent, and personalized experience, to make informed business decisions, and for other legitimate purposes.

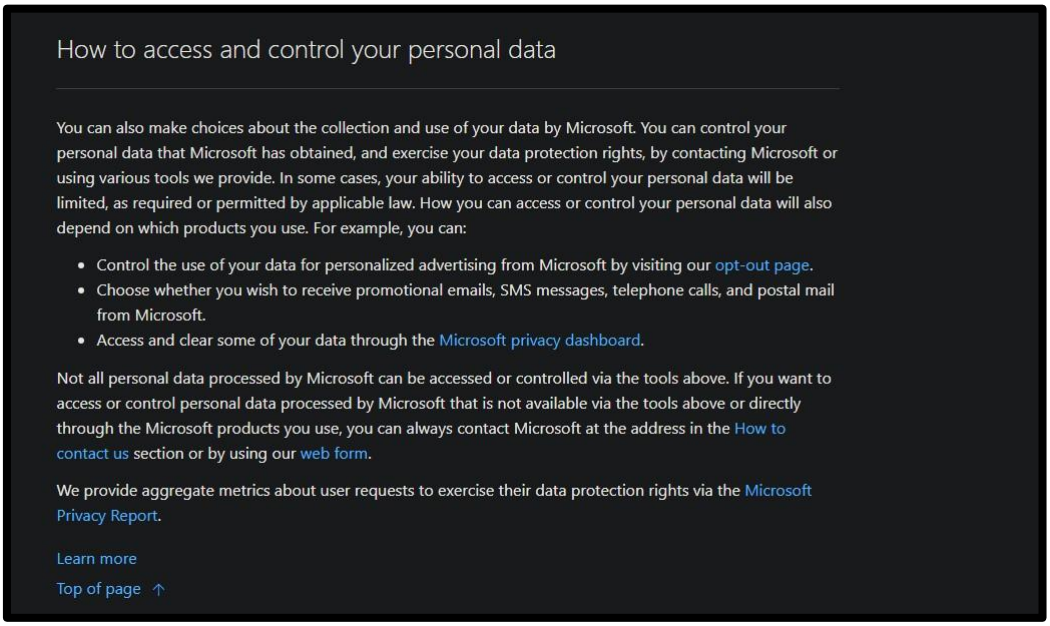
Our processing of personal data for these purposes includes both automated and manual (human) methods of processing. Our automated methods often are related to and supported by our manual methods. For example, our automated methods include artificial intelligence (AI), which we think of as a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do. To build, train, and improve the accuracy of our automated methods of processing (including AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For example, we manually review short snippets of voice data that we have taken steps to de-identify to improve our speech recognition technologies. This manual review may be conducted by Microsoft employees or vendors who are working on Microsoft's behalf.

Learn more

Top of page ↑

Fonte: https://privacy.microsoft.com/en-us/privacystatement

Figura 12 - Site da Microsoft onde é especificado onde o usuário pode acessar e controlar seusdados pessoais.



Fonte: https://privacy.microsoft.com/en-us/privacystatement

As boas práticas para a implementação da ISO/IEC 29184:2021 incluem a realização de testesde usabilidade para garantir que os avisos de privacidade sejam compreendidos pelos usuários. Um teste de usabilidade envolve a observação de usuários reais usando o sistema para entenderse a interface é fácil de usar e se os avisos de privacidade são compreendidos. Por exemplo, um teste de usabilidade pode envolver a observação de um usuário navegando pelo site e tentando entender as políticas de privacidade. Além disso, a norma recomenda a revisão regulardas práticas de privacidade para garantir a conformidade contínua. Isso pode envolver a revisãodas políticas de privacidade em um intervalo regular, como anualmente, e a atualização das políticas conforme necessário. Por fim, a norma recomenda a inclusão de opções de consentimento em pontos-chave da interação do usuário, como durante o processo de inscriçãoou nas configurações do usuário. Por exemplo, um site pode incluir uma opção para o usuárioconsentir com a coleta de dados durante o processo de inscrição.

A ISO/IEC 29184:2021 desempenha um papel essencial na implementação de interfaces gráficas, promovendo a transparência, a confiança do usuário e a

conformidade com os regulamentos de privacidade. A implementação desta norma não só aumenta a confiança do usuário, mas também melhora a reputação da organização. Embora a implementação possa exigir esforços significativos de design e desenvolvimento, os benefícios potenciais para a confiança do usuário e a reputação da organização tornam esses esforços valiosos. valiosos.

3. METODOLOGIA

Este capítulo descreve a metodologia adotada neste trabalho para investigar a implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas. A metodologia de pesquisa é fundamental para qualquer estudo acadêmico, pois fornece o quadrodentro do qual a pesquisa é conduzida e os dados são coletados, analisados e interpretados. A escolha da metodologia é influenciada pelo objetivo da pesquisa, a natureza do tema em estudoe as questões de pesquisa específicas que o estudo busca responder

No contexto deste trabalho, a metodologia foi elaborada para fornecer recomendações detalhadas e contextualizadas sobre a implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas. A metodologia adotada busca equilibrar a necessidade de uma análise aprofundada com a necessidade de uma abordagem prática e aplicável que possa ser utilizada por designers e desenvolvedores de interfaces gráficas.

A seguir, este capítulo detalha a abordagem metodológica, os métodos de coleta e análise de dados, as limitações do estudo e as considerações éticas.

3.1. Abordagem Metodológica

A metodologia deste estudo baseia-se em pesquisa qualitativa, com o objetivo de compreendere analisar a implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas. A pesquisa qualitativa foi escolhida por sua capacidade de fornecer insights detalhados e contextuais sobre o tema em estudo.

Os dados para este estudo foram coletados através de uma revisão de literatura abrangente, análise de documentos e estudos de caso. A revisão de literatura envolveu a análise de trabalhos acadêmicos, artigos de jornais, relatórios de pesquisa e documentos oficiais relacionados ao *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD. Para a busca de referências, foram utilizados motores de busca acadêmicos como Google Scholar, JSTOR e PubMed. A análise de documentos envolveu a revisão de políticas de privacidade, avisos de consentimento e outras documentações relevantes de 50 interfaces gráficas que implementaram essas normas e princípios. Os estudos de caso foram selecionados com base em sua relevância e representatividade, e foram analisados para entender como essas

normas e princípios são implementados na prática.

Os dados coletados foram analisados usando análise de conteúdo. Isso envolveu a identificação de temas e padrões emergentes relacionados à implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas. A análise de conteúdo foi realizada manualmente. Primeiramente, foi feita uma leitura dos dados e anotações sobre os temas e padrões observados. Em seguida, esses temas foram agrupados e codificados. Finalmente, esses códigos foram analisados para formar conclusões.

Este estudo reconhece várias limitações. Primeiro, a análise é limitada aos documentos e estudos de caso disponíveis e acessíveis ao pesquisador. Isso inclui políticas de privacidade, avisos de consentimento e outras documentações relevantes de interfaces gráficas que implementaram essas normas e princípios. Segundo a interpretação dos dados é subjetiva e depende do entendimento e perspectiva do pesquisador. A análise de conteúdo, embora seja uma ferramenta poderosa, é interpretativa por natureza e pode ser influenciada pelas perspectivas e preconceitos do pesquisador. Terceiro, a implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas é um campo em rápida evolução, e as práticas podem mudar rapidamente. Além disso, o estudo se limitou a analisar interfaces gráficas, o que pode não abranger todas as possíveis implementações dessas normas e princípios.

Este estudo foi conduzido de acordo com os princípios éticos da pesquisa. Todos os dados utilizados são de domínio público ou obtidos com o devido consentimento. Todas as referências, figuras e citações foram adequadamente indicadas e creditadas. Os resultados são apresentados de forma a garantir a confidencialidade e o anonimato das organizações envolvidas nos estudos de caso.

Em conclusão, esta metodologia permite uma análise aprofundada e contextual da implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas, contribuindo para a compreensão e prática neste campo emergente.

Para exemplificar a análise de conteúdo qualitativa, podemos considerar o seguinte exemplo: Suponha que um dos temas emergentes identificados na análise de documentos seja a "transparência na coleta de dados". Neste caso, o pesquisador pode codificar todas as instâncias onde a transparência na coleta de dados é mencionada ou discutida. Em seguida, esses códigos são agrupados e analisados

para formar conclusões sobre como a transparência na coleta de dados é implementada nas interfaces gráficas estudadas.

Por fim, é importante ressaltar que a análise de conteúdo qualitativa é apenas uma das muitas ferramentas disponíveis para os pesquisadores. A escolha da ferramenta de análise depende doobjetivo da pesquisa, da natureza dos dados e das preferências do pesquisador.

4. RECOMENDAÇÕES PARA CONSTRUÇÃO DE INTERFACES ADEQUADAS A LGPD

Este capítulo apresenta recomendações estratégicas para a implementação em interfaces gráficas, tendo como base os estudos realizados no capítulo 3. As recomendações são fundamentais para orientar designers, desenvolvedores e tomadores de decisão na criação de interfaces que respeitem a privacidade do usuário e estejam em conformidade com as normas e regulamentos internacionais.

A importância dessas recomendações é evidenciada por uma série de estudos e relatórios (Cisco, 2020; Forrester, 2019). De acordo com um relatório da Cisco (2020), as organizações que investem em privacidade veem benefícios significativos, incluindo uma menor probabilidade de sofrer violações de dados, menores custos de ciclo de vendas e uma maior atratividade para investidores. Além disso, a pesquisa da Forrester (2019) mostra que 79% dos consumidores tomam medidas para proteger sua privacidade online, destacando a importância de interfaces gráficas que respeitam a privacidade.

Os desenvolvedores de interface, de fato, possuem essa preocupação. A privacidade do usuário é uma questão crítica na era digital e os desenvolvedores estão cada vez mais conscientes de sua responsabilidade em proteger os dados dos usuários. Eles entendem que a implementação de práticas de privacidade eficazes não só protege os usuários, mas também aumenta a confiança do usuário e a reputação da organização.

Este capítulo apresenta como a adoção dessas recomendações pode ajudar as organizações a criar interfaces que promovam a confiança do usuário e estejam em conformidade com as normas e regulamentos internacionais.

No entanto, é importante lembrar que a implementação dessas práticas ou recomendações são um processo contínuo que requer revisão e ajuste regular para garantir a eficácia contínua. Isso significa que as políticas e práticas de privacidade devem ser revisadas regularmente para garantir que continuem a ser eficazes e relevantes para as necessidades atuais.

A privacidade do usuário é uma questão crítica na era digital, e as organizações devem fazer todos os esforços para proteger os dados pessoais dos usuários. A implementação de recomendações de boas práticas em interfaces gráficas é uma maneira eficaz de fazer isso. Embora a implementação dessas práticas possa exigir

esforços significativos, como estabelecer políticas para manuseio de dados, treinar funcionários, fornecer avisos de privacidade para clientes, limitar o acesso a informações confidenciais e implementar medidas de segurança adequadas, os benefícios potenciais para a confiança do usuário e a reputação da organização tornam esses esforços valiosos.

4.1. Recomendações para uma Interface Ideal

Com base nas análises dos capítulos anteriores, as seguintes recomendações são propostas paraa criação de uma interface gráfica que respeite a privacidade do usuário:

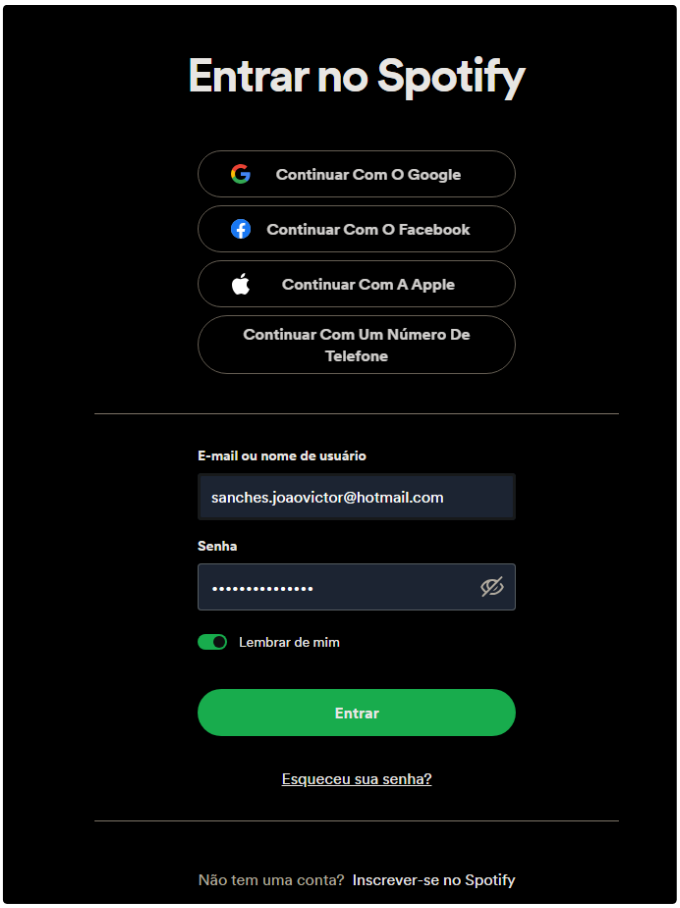
4.1.1. Minimização de Dados

A minimização de dados, um princípio central do *Privacy by Design*, é fundamental para reduzir o risco de violações de dados e pode ser efetivamente implementada em uma interface gráfica através de um design cuidadoso dos formulários de entrada de dados. Durante o processo de inscrição em um serviço online, por exemplo, a interface deve solicitar apenas as informações indispensáveis para a criação de uma conta, como nome de usuário, endereço de *e-mail* e senha.

A solicitação de informações adicionais, como endereço residencial ou número de telefone, deve ser limitada apenas aos casos em que são essenciais para o serviço. A coleta de dados sensíveis deve ser evitada, a menos que seja absolutamente necessária. Isso pode ser alcançado através do uso de campos de formulário condicionais que só aparecem quando certas opções são selecionadas. Por exemplo, um campo para inserir um número de telefone pode aparecer apenas se o usuário selecionar a opção de receber notificações por SMS.

Além disso, a interface pode usar técnicas de ocultação de dados, como mascaramento de campos de entrada, para proteger os dados sensíveis que são exibidos.

Figura 13 – Tela de login *web* do Spotify.

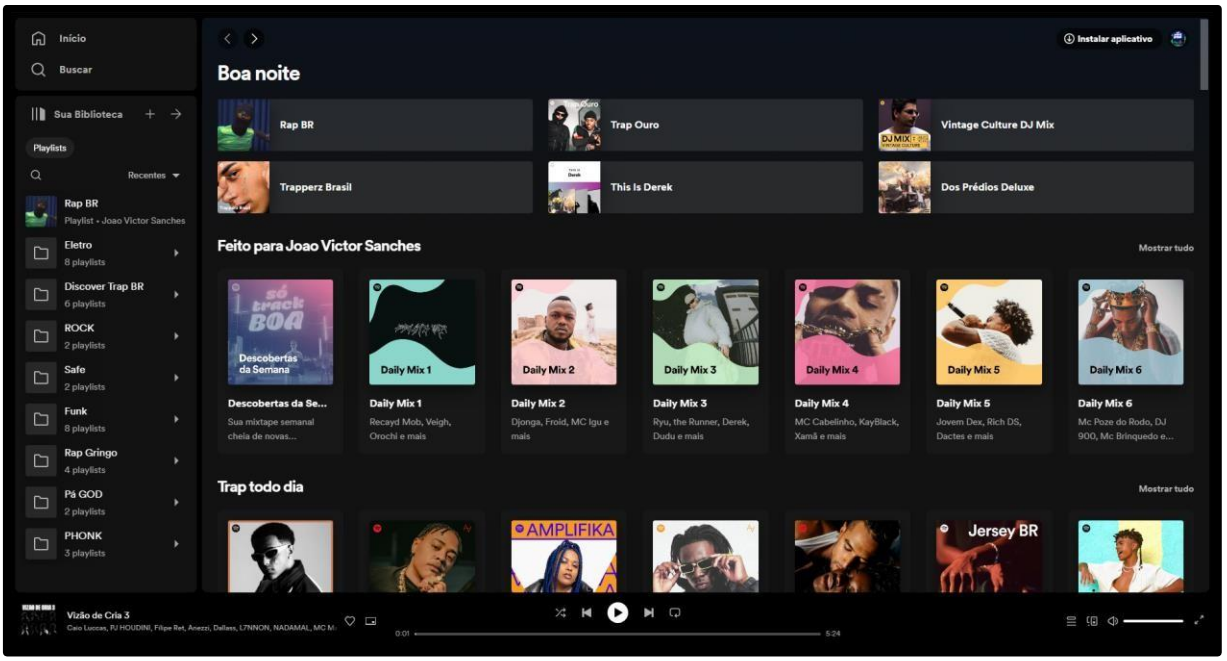


Fonte: Pagina web de login do Spotify: https://accounts.spotify.com/pt-BR/login?continue=https%3A%2F%2Fopen.spotify.com%2Fintl-pt%3F.

Por exemplo, em um campo de senha, os caracteres inseridos podem ser substituídos por asteriscos ou pontos para evitar que outras pessoas vejam a senha.

Um exemplo de produto com excelente minimização de dados em sua interface gráfica é o aplicativo de música Spotify. O Spotify faz um ótimo trabalho ao apresentar uma grande quantidade de informações de maneira clara e concisa. Quando você abre o aplicativo, a primeira coisa que vê é a sua biblioteca de música e as *playlists* que você criou ou seguiu, assimcomo mostra a figura 14 a seguir.

Figura 14 – Print da tela principal do aplicativo Spotify *web*.



Fonte: Pagina web inicial para usuário do Spotify: https://open.spotify.com/intl-pt#_=_

Cada *playlist* é representada por uma pequena imagem quadrada (geralmente a capa do álbumdo primeiro artista na lista) e o nome da *playlist*, como é representado na figura. Isso permite que o usuário identifique rapidamente a *playlist* que deseja ouvir. Além disso, quando o usuárioclica em uma *playlist*, vê uma lista de músicas com o nome da música, o artista e a duração damúsica. Novamente, isso é apresentado de forma intuitiva e direta, tornando fácil para você encontrar a música que deseja ouvir.

Figura 15 – Barra de reprodução do Spotify *web*.

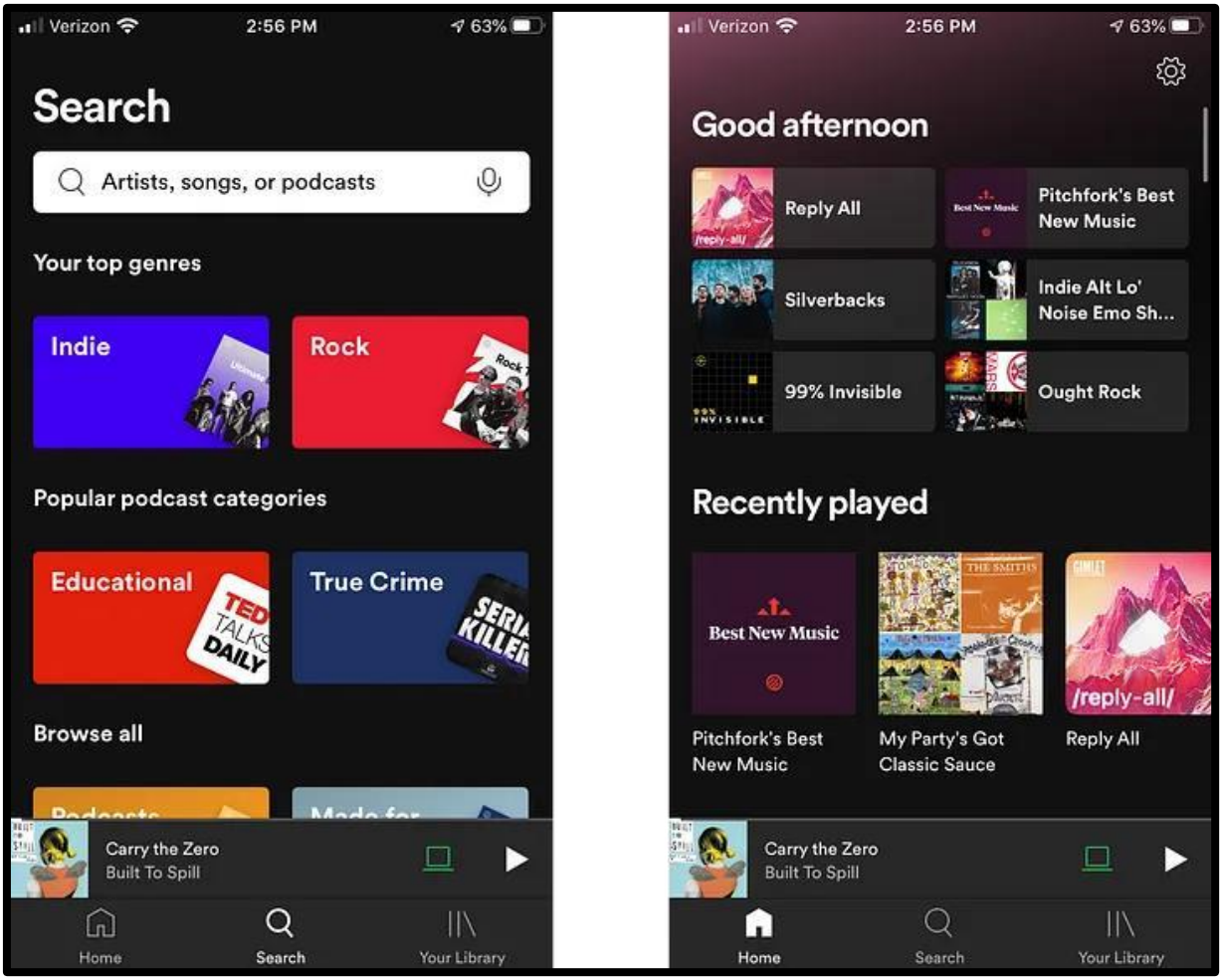
Fonte: Pagina web inicial para usuário do Spotify: https://open.spotify.com/intl-pt#_=_

O Spotify também utiliza ícones simples e intuitivos para representar diferentes ações, como reproduzir, pausar, avançar, retroceder e salvar uma música, mostrado na figura 15. Isso minimiza a quantidade de texto na interface, tornando-a menos confusa e mais fácil de navegar.

Finalmente, o Spotify utiliza um esquema de cores simples e contrastante (principalmente preto, branco e verde) que torna o texto e os ícones fáceis de ler e

identificar. A escolha de cores em uma interface de usuário é uma parte crucial do design de interface, pois pode afetara usabilidade e a experiência do usuário. Cores contrastantes podem ajudar a destacar elementos importantes e orientar o olhar do usuário, enquanto cores harmoniosas podem criar uma sensação agradável e equilibrada.

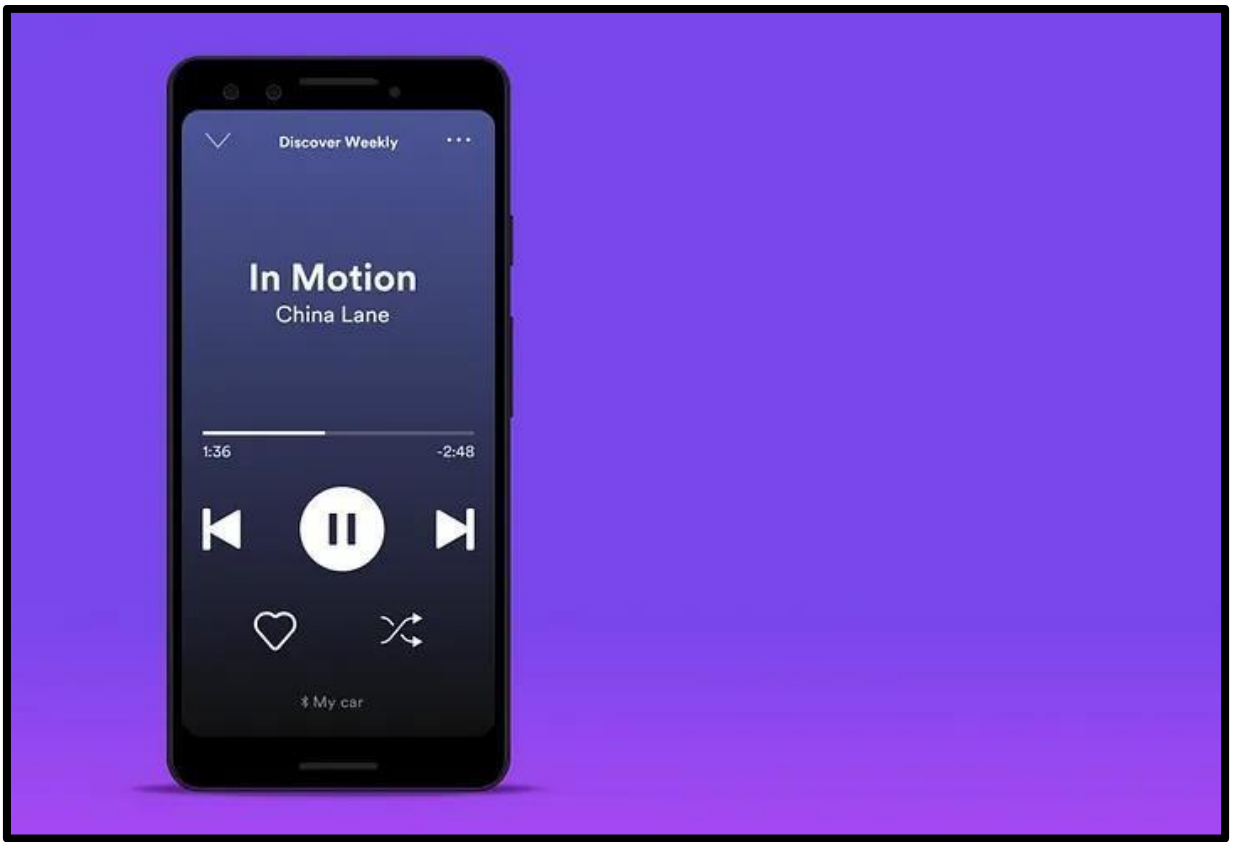
Figura 16 – Menu principal e menu de busca do aplicativo Spotify.



Fonte: https://uxdesign.cc/ux-ui-analysis-spotify-31f3855a1740

Em uma nova inovação, o Spotify criou um modo de visualização móvel especial que é ativadoautomaticamente enquanto se dirige.

Figura 17 – Menu modo Carro.



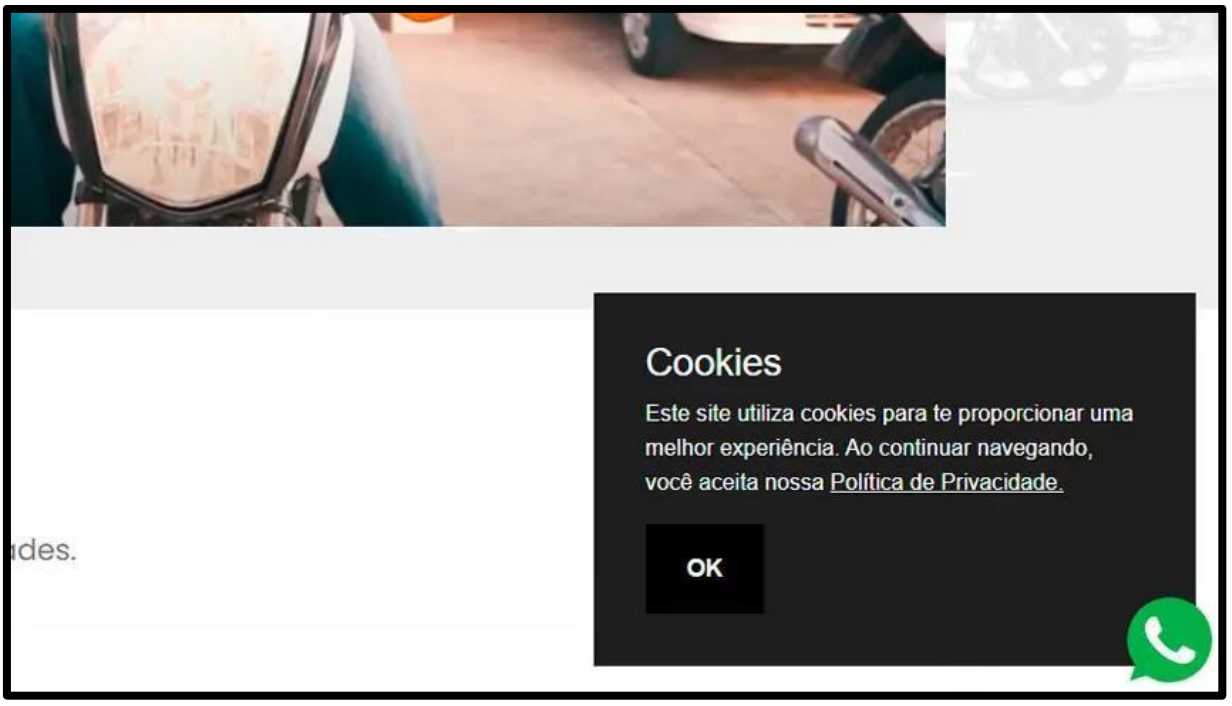
Fonte: https://uxdesign.cc/ux-ui-analysis-spotify-31f3855a1740

Como é mostrado na figura 17, esta interface simplificada remove todas as imagens de fundo e aumenta as funções primárias, como reproduzir/pausar e próximo/anterior. Isso aumenta a clareza para quem olha rapidamente para a tela enquanto está dirigindo.

4.1.2. Transparência e Consentimento Informado

A interface gráfica deve incorporar a transparência e o consentimento informado, conforme estabelecido pela ISO/IEC 29184. Isso implica em fornecer aos usuários avisos de privacidadeclaros e compreensíveis, informando-os sobre a coleta, uso e compartilhamento de seus dados.Isso pode ser implementado através de pop-ups informativos ou banners de consentimento queaparecem na primeira visita do usuário ao site.

Figura 18 – Exemplo de mensagem que pede a confirmação dos cookies.



Fonte: https://ayltoninacio.com.br/blog/como-colocar-popup-aviso-cookies-privacidade-sem-plugins

A figura 18,é um exemplo de um banner de consentimento pode aparecer na parte inferior da tela, informando ao usuário que o site usa *cookies* e solicitando seu consentimento para coletá-los.

Além disso, é essencial que os usuários tenham a liberdade de consentir ou recusar a coleta dedados, o que pode ser viabilizado por meio de caixas de seleção ou botões de opção durante oprocesso de inscrição. Por exemplo, durante o processo de inscrição, o usuário pode ser apresentado com uma lista de caixas de seleção, cada uma correspondendo a um tipo diferentede dado que o site deseja coletar.

Um exemplo de um produto real que possui uma interface gráfica com transparência e consentimento informado excelente é o aplicativo de mensagens Signal Messenger LLC. Signal é um aplicativo de mensagens criptografadas que se destaca por sua dedicação à privacidade e transparência. Durante o processo de configuração, o aplicativo informa claramente ao usuário sobre seus protocolos de criptografia e privacidade. Além disso, antes de solicitar acesso a qualquer informação pessoal, como contatos, o aplicativo explica por que precisa dessainformação e como ela será usada.

A transparência é evidente na forma como o Signal comunica suas práticas de coleta e uso de dados. O aplicativo fornece informações claras e acessíveis sobre o

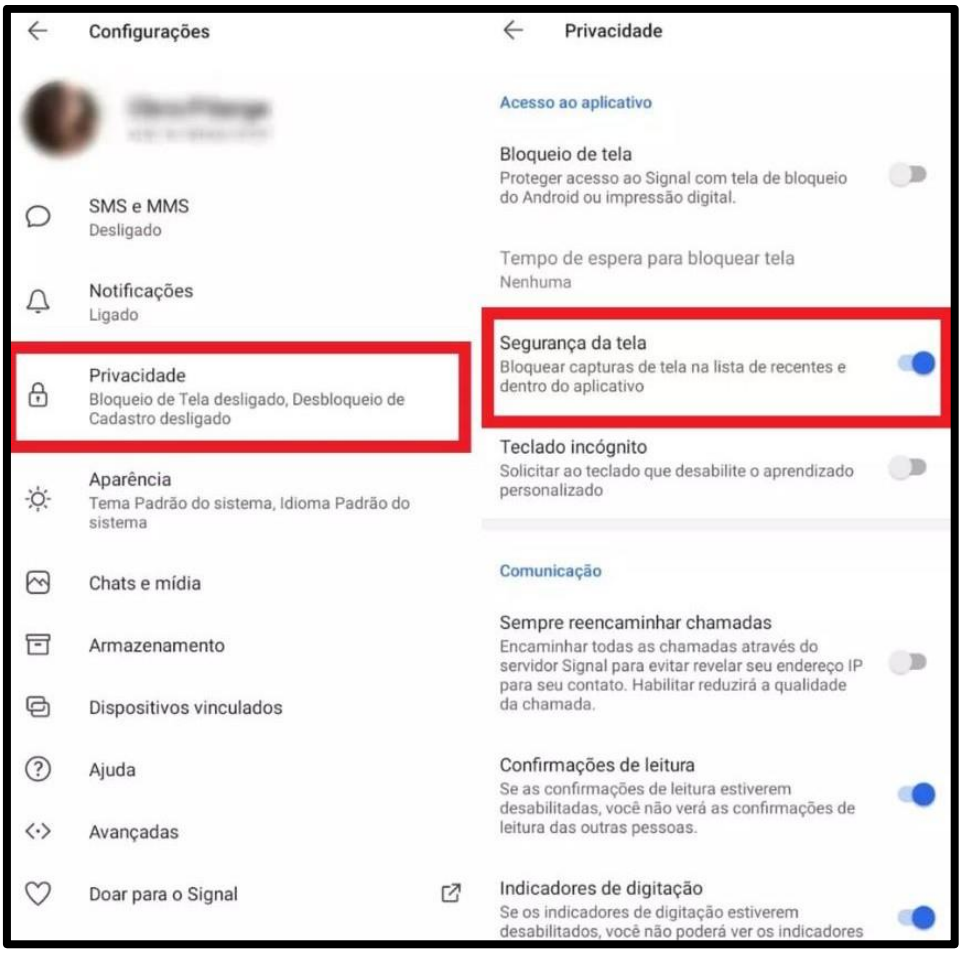
que faz com os dados do usuário. O consentimento informado, por outro lado, é demonstrado pelo fato de que o Signal solicita explicitamente o consentimento do usuário antes de coletar qualquer dado pessoal. O aplicativo também fornece informações claras sobre a finalidade da coleta de dados, o tempo de utilização e a base legal para a coleta de dados.

A interface do Signal é simples e intuitiva, tornando fácil para os usuários entenderem suas configurações de privacidade e fazerem escolhas informadas. Segue a representação da tela do aplicativo:

Figura 19 – Imagem da tela principal do aplicativo Signal.

Fonte: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=pt

Figura 20 – Print exemplo da tela de configurações de privacidade.



Fonte: https://www.techtudo.com.br/listas/2021/01/5-funcoes-de-seguranca-do-signal-o-rival-ultrasseguro-do-whatsapp.ghtml

Por exemplo, na figura 20 mostra as configurações de privacidade são claramente rotuladas e organizadas de forma lógica, e as opções são apresentadas de forma clara e direta.

Além disso, o código-fonte do Signal é aberto, o que significa que qualquer pessoa pode verificar como o aplicativo funciona e como ele protege a privacidade do usuário.

No entanto, é importante notar que nenhum aplicativo é perfeito e a eficácia de qualquer medida de privacidade depende em grande parte do comportamento do usuário. Portanto, é sempre umaboa ideia revisar as configurações de privacidade e fazer uma pesquisa independente ao escolher um aplicativo ou serviço. A transparência e o aviso de consentimento são apenas duasdas muitas considerações a serem levadas em conta ao avaliar a privacidade e a segurança de um aplicativo.

4.1.3. Avaliação de Impacto na Privacidade

A implementação de uma Avaliação de Impacto na Privacidade (AIP), conforme recomendado pela ISO/IEC 29134, é primordial antes do lançamento de novas funcionalidades que coletam dados adicionais do usuário. A AIP é um processo que ajuda as organizações a identificar e reduzir os riscos de privacidade associados a um projeto de dados. Este processo é particularmente importante quando se introduzem novas tecnologias ou quando se processam dados sensíveis em larga escala.

Na interface gráfica, a AIP pode ser realizada através de um processo de design e desenvolvimento cuidadoso, que inclui a identificação de riscos, avaliação da probabilidade e gravidade desses riscos, e a implementação de medidas para mitigá-los. Por exemplo, uma organização pode identificar que a coleta de dados de localização em um aplicativo móvel pode representar um risco à privacidade dos usuários. A organização pode então avaliar a probabilidade de esse risco se materializar e a gravidade do impacto se isso acontecer. Com base nessa avaliação, a organização pode decidir implementar medidas para mitigar o risco, como limitar a precisão dos dados de localização coletados ou permitir que os usuários optem por não compartilhar seus dados de localização.

Além disso, a organização pode realizar testes de penetração e auditorias de segurança para identificar possíveis vulnerabilidades na interface. Por exemplo, um teste de penetração pode envolver a tentativa de acessar dados de usuário protegidos através da interface para identificar possíveis falhas de segurança.

Um exemplo de um produto com uma excelente Avaliação de Impacto na Privacidade (AIP) é o navegador de internet "Firefox" da Mozilla. A Mozilla tem uma forte reputação de respeitar a privacidade do usuário e tem implementado várias medidas para proteger os dados dos usuários.

O Firefox inclui várias características de privacidade, incluindo:

- Proteção de rastreamento: O Firefox bloqueia automaticamente muitos rastreadores de terceiros, o que ajuda a manter privadas as atividades online dos usuários. Isso significa que os anunciantes têm menos dados sobre o comportamento de navegação dos usuários, o que pode ajudar a proteger a privacidade dos usuários.

- Modo de navegação privada: Este modo não salva o histórico de navegação, pesquisas, cookies ou arquivos temporários. Isso significa que as informações sobre as atividadesde navegação do usuário não são armazenadas no dispositivo do usuário, o que pode ajudar a proteger a privacidade do usuário.
- Facebook Container: Esta extensão ajuda a isolar a atividade do Facebook do resto da atividade na web, dificultando o rastreamento do Facebook através de sites de terceiros.Isso pode ajudar a proteger a privacidade do usuário ao limitar a quantidade de dados que o Facebook pode coletar sobre a atividade de navegação do usuário fora do Facebook.
- Proteção contra impressões digitais: O Firefox tem recursos para proteger contra a impressão digital do navegador, uma técnica que os sites usam para rastrear os usuários.
- Criptografia de ponta a ponta para sincronização: Quando você usa a função desincronização do Firefox, seus dados são criptografados de ponta a ponta. Isso significaque apenas o dispositivo do usuário pode decifrar os dados sincronizados. Mesmo se osdados forem interceptados durante a transmissão, eles não poderão ser lidos porterceiros. Isso ajuda a proteger a privacidade do usuário, garantindo que seus dados sincronizados, como favoritos, histórico de navegação e senhas, permaneçam privados.

A Mozilla também é transparente sobre as práticas de coleta de dados e permite que os usuáriosoptem por não participar da coleta de dados. Eles também realizam Avaliações de Impacto naPrivacidade regularmente para avaliar e mitigar os riscos de privacidade associados aos seus produtos e serviços.

4.1.4. Alinhamento com a Lei Geral de Proteção de Dados (LGPD)

Uma seção de configurações de privacidade é uma parte essencial de qualquer interface que lida com dados do usuário. Esta seção permite que os usuários vejam quais dados estão sendocoletados sobre eles e lhes dá a opção de gerenciar ou limitar essa coleta. Isso pode ser implementado através de uma página de perfil de usuário dedicada, onde os usuários podem visualizar e modificar suas informações pessoais.

Para explicar isso de uma maneira que um leigo possa entender, imagine que você está usando um aplicativo de mídia social. Na seção de configurações de privacidade, você pode ver quaisinformações o aplicativo tem sobre você - isso pode

incluir seu nome, endereço de e-mail, número de telefone, e até mesmo informações sobre os posts que você gostou ou os grupos dosquais você faz parte. Se você não se sentir confortável com o aplicativo tendo acesso a algumasdessas informações, você pode alterar suas configurações de privacidade para limitar o que o aplicativo pode ver.

Um exemplo de um produto que possui uma seção de configurações de privacidade bem implementada é o aplicativo de mensagens "Signal". Ele não coleta dados pessoais dos usuáriosalém do número de telefone necessário para a criação da conta.

Aqui estão algumas das maneiras pelas quais o Signal se alinha com os princípios de privacidade:

- Consentimento: O Signal solicita consentimento explícito dos usuários para coletar seunúmero de telefone. Não coleta nenhum outro dado pessoal.
- Transparência: O Signal é transparente sobre suas práticas de coleta de dados. Sua política de privacidade é clara e fácil de entender. Isso significa que eles explicam de maneira simples e direta quais dados estão coletando, porque estão coletando esses dados e como estão usando esses dados.
- Finalidade: O Signal coleta apenas o número de telefone dos usuários, que é necessáriopara o funcionamento do serviço. Não coleta dados para fins de publicidade ou análise.Isso significa que eles só coletam os dados que precisam para fazer o aplicativo funcionar corretamente e não usam esses dados para outros fins, como direcionar anúncios ou vender para outras empresas.
- Responsabilização e prestação de contas: Eles têm um histórico de resistência atentativas de comprometer a privacidade dos usuários. Isso significa que eles tomam medidas ativas para proteger a privacidade dos usuários e resistir a tentativas de forçá-los a revelar informações privadas.

5. CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresentou uma investigação sobre a implementação de *Privacy by Design*, ISO/IEC 29184, ISO/IEC 29134 e LGPD em interfaces gráficas. Através de uma metodologia de pesquisa qualitativa, foram coletados dados detalhados e contextualizados sobre o tema. A análise de documentos e estudos de caso revelou a aplicação prática dessas normas e princípios.

Os resultados indicam que a implementação dessas normas e princípios é viável e benéfica para fins de aumentar a proteção da privacidade do usuário. No entanto, também foi observado que a aplicaçãoprática dessas normas pode variar significativamente dependendo do contexto específico da interface gráfica.

Este estudo contribui para a compreensão da aplicação de *Privacy by Design* e normas relacionadas em interfaces gráficas, fornecendo uma base sólida para futuras pesquisas e práticas de design. Além disso, as recomendações obtidas podem ser úteis para designers e desenvolvedores de interfaces gráficas que buscam incorporar essas normas em seus projetos

Embora este estudo tenha fornecido recomendações valiosas, ainda há muito a ser explorado no campo da privacidade em interfaces gráficas. Trabalhos futuros podem se concentrar emáreas como:

- **Estudos de Caso Mais Abrangentes:** Este estudo analisou 50 interfaces gráficas.Trabalhos futuros podem expandir essa análise para incluir um número maior de interfaces gráficas e de diferentes contextos.
- **Análise Quantitativa:** Este estudo adotou uma abordagem qualitativa. Trabalhos futuros podem incluir uma análise quantitativa para fornecer uma visão mais precisado estado da implementação dessas normas.
- **Impacto do Design na Percepção do Usuário:** Este estudo focou na implementaçãode normas de privacidade. Trabalhos futuros podem investigar como diferentes abordagens de design afetam a percepção do usuário sobre a privacidade.
- **Desenvolvimento de Ferramentas de Design:** Com base nos insights deste estudo, trabalhos futuros podem se concentrar no desenvolvimento de ferramentas de design que facilitem a implementação de *Privacy by Design* e normas relacionadas.

REFERÊNCIAS

APPLE INC. (2021). iOS Human Interface Guidelines. Disponível em: https://developer.apple.com/design/human-interface-guidelines/ios/overview/themes/. Acesso em: 27/04/2023.

BARTLETT, J. C. Privacy by Design: A Counterfactual Analysis of Google Street View. In: Conference on Computers, Freedom and Privacy, 2011.

BHATTA CHARYA, A. et al. From privacy to usability: A survey of the literature on the user-centered design of privacy-enhancing technologies. Journal of the Association for Information Science and Technology, v. 73, n. 2, p. 163 -179, 2022.

BRASIL. (2018). 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: 27/04/2023.

Beckman, S., & Balaam, M. (2019). Designing for privacy and consent in the internet of things. ACM Transactions on Computer-Human Interaction (TOCHI), 26(5), 1-43.

Bilge, L., Kirda, E., & Balduzzi, M. (2012). EXPOSURE: Finding malicious domains using passive DNS analysis. Proceedings of the 21st USENIX Conference on Security Symposium, 195-210.

Cavoukian, A. (2009). Privacy by Design: Delivering the Promise. Identity in the Information Society, 2(2), 143 -151.

CAVOUKIAN, A. (2011). Privacy by design: the definitive workshop. Identity in the Information Society, 3(2), 247 -251.

CISCO. (2020). From Privacy to Profit: Achieving Positive Returns on Privacy Investments. Disponível em:

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2020-gdpr.pdf. Acesso em: 23/05/2023

CHESKY, B., GEBBIA, J., & BLECHARCZYK, N. (2017). Airbnb. Disponível em: https://www.airbnb.com/. Acesso em: 27/04/2023.

COLAS, P. et al. Incorporating privacy-by-design in user-centered design process. Journal of Ambient Intelligence and Humanized Computing, v. 11, n. 3, p. 1147 -1160, 2020.

Calandrino, J. A., Kilzer, A., Narayanan, A., Felten, E. W., & Shmatikov, V. (2011). “You Might Also Like:” Privacy Risks of Collaborative Filtering. Proceedings of the 2011 IEEE Symposium on Security and Privacy, 231-246.