

UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DESIGN
MESTRADO EM DESIGN

FABIANA FRANÇA SILVA

**DESIGN PARA PRIVACIDADE: UMA EXPERIÊNCIA MELHORADA PARA O
CIDADÃO NOS SERVIÇOS DO GOVERNO DIGITAL**

SÃO LUÍS
2025

FABIANA FRANÇA SILVA

**DESIGN PARA PRIVACIDADE: UMA EXPERIÊNCIA MELHORADA PARA O
CIDADÃO NOS SERVIÇOS DO GOVERNO DIGITAL**

Dissertação apresentada ao Programa de Pós-Graduação em Design da Universidade Federal do Maranhão como requisito para obtenção do título de mestre em Design.

Área de concentração: Design de Produtos. Linhas de Pesquisa: Design e Ergonomia

Orientadora: Prof^a Dr^a Cláudia Renata Mont'Alvão Bastos Rodrigues

São Luís
2025

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

França Silva, Fabiana.

Design para privacidade: uma experiência melhorada para o cidadão nos serviços do governo digital / Fabiana França Silva. - 2025.

154 f.

Orientador(a): Claudia Renata Montalvão Bastos Rodrigues.

Dissertação (Mestrado) - Programa de Pós-graduação em Design/ccet, Universidade Federal do Maranhão, São Luís, 2025.

1. Privacidade de Dados Digitais. 2. Privacy By Design. 3. Experiência do Usuário. 4. Governo Digital. I. Rodrigues, Claudia Renata Montalvão Bastos. II. Título.

FABIANA FRANÇA SILVA

**DESIGN PARA PRIVACIDADE: UMA EXPERIÊNCIA MELHORADA PARA O
CIDADÃO NOS SERVIÇOS DO GOVERNO DIGITAL**

Aprovada em: ____/____/____

BANCA EXAMINADORA

Profª Drª Cláudia Renata Mont'Alvão Bastos Rodrigues (Orientadora)
Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)

Profª Drª Fabiane Rodrigues Fernandes
Universidade Federal do Maranhão (UFMA)

Profª Drª Inez Maria Leite da Silva
Universidade Federal do Maranhão (UFMA)

Profª Drª Raquel Corrêa Cordeiro
Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)

AGRADECIMENTOS

Aos meus pais, Antonia França e Antonio Camara, pois nada seria possível sem eles.

À Universidade Federal do Maranhão, minha casa querida, e à Fundação de Amparo à Pesquisa do Maranhão pelo incentivo a esta pesquisa

À professora Claudia Mont'Alvão pela orientação e generosidade no decorrer deste trabalho. Às professoras Fabiane Fernandes, Raquel Cordeiro e Inez Leite, pelas contribuições e participação banca de avaliação. Ao professor Denilson Santos pela solicitude em responder às minhas dúvidas. Aos demais professores e colegas do PPGDg pelo conhecimento compartilhado.

Aos amigos Letícia, Áurea e Belfort por todo companheirismo e ajuda.

A todos que contribuíram de alguma forma com esta dissertação, meu muito obrigada.

RESUMO

Dados pessoais digitais, coletados dos cidadãos-usuários, estão contribuindo na qualidade dos serviços públicos prestados on-line. Nesse contexto, as ameaças à privacidade se tornam ainda mais reais, reverberando em diretrizes como a Lei Geral de Proteção de Dados Pessoais Brasileira, a LGPD. Contudo, a forma como as políticas de privacidade e os termos de consentimento, determinados pela LGPD, são apresentados aos cidadãos é complexa, comprometendo a usabilidade das interfaces que as expõem aos cidadãos. Dessa forma, sob a ótica do design, como objetivo principal, busca-se apontar diretrizes mais amigáveis e centradas nos cidadãos para garantia da privacidade e proteção aos dados pessoais no governo digital. Esta pesquisa justifica-se pela importância do e-gov para o exercício da cidadania do indivíduo, sendo seu uso uma forma de inclusão digital e inovação pública. Sendo assim, a pesquisa foi desenvolvida em quatro etapas. Na primeira, foram realizadas pesquisas bibliográfica e documentais a fim de construir um referencial que consubstancie a justificativa da pesquisa. Na segunda, foi conduzida pesquisa qualitativa, com enfoque fenomenológico. O instrumento utilizado para coleta de dados nessa fase foram *sketch interviews* - entrevistas acompanhadas por mapa mental. Na terceira etapa foi realizada pesquisa quantitativa, a partir de um levantamento de campo. Os dados foram levantados a partir da aplicação de questionários. A quarta e última etapa da pesquisa consistiu na obtenção dos resultados a partir da análise e interpretação dos dados via codificação qualitativa de dados e estatística descritiva. Como resultado, a pesquisa propôs uma diretriz ampla, a implementação da educação e cultura de proteção da privacidade de dados digitais. Também foram apontadas diretrizes mais específicas relativas à experiência da pessoa usuária, como uma versão resumida dos documentos, identificadores de privacidade, design ético, comprometido e centrado no usuário. Além disso, como próximos passos, recomendam-se pesquisas mais críticas e direcionadas, a concretização das diretrizes apontadas, bem como a sua validação com as pessoas de interesse. Outro desdobramento recomendado é a necessidade de pesquisas futuras que envolvam as iniciativas locais em acompanhamento ao seu próprio desenvolvimento. Por fim, espera-se que esta pesquisa, além de contribuir cientificamente com o campo do design, devido ao seu viés interdisciplinar, possa cooperar com os cidadãos que utilizam os serviços do governo digital para que seu direito à privacidade seja assegurado e garantido.

Palavras-chave: privacidade de dados digitais; *privacy by design*; experiência do usuário; governo digital.

ABSTRACT

Digital personal data, collected from citizen-users of public services, is contributing to the quality of public services provided online. In this context, the threats to privacy have become even more real, reverberating in guidelines such as the Brazilian General Personal Data Protection Law, the LGPD. However, the way in which the privacy policies and terms of consent determined by the LGPD are presented to citizens is complex, compromising the usability of the interfaces that expose them to citizens. Thus, from a design perspective, the main objective is to point out more user-friendly and citizen-centered guidelines for guaranteeing privacy and protecting personal data in digital government. This research is justified by the importance of e-gov for the exercise of individual citizenship, its use being a form of digital inclusion and public innovation. The research was carried out in four stages. In the first stage, bibliographical and documentary research was carried out in order to build up a framework to substantiate the justification for the research. The second stage involved qualitative research with a phenomenological approach. The instrument used to collect data in this phase was sketch interviews - interviews accompanied by a mind map. In the third stage, quantitative research was carried out using a field survey. The data was collected using questionnaires. The fourth and final stage of the research consisted of obtaining the results from the analysis and interpretation of the data via qualitative data coding and descriptive statistics. As a result, the research proposed a broad guideline, the implementation of education and a culture of digital data privacy protection. More specific guidelines relating to the user experience were also pointed out, such as a shortened version of the documents, privacy identifiers, ethical, committed and user-centered design. As next steps, more critical and targeted research is recommended, as well as the implementation of the guidelines pointed out and their validation with stakeholders. Another recommended outcome is the need for future research involving local initiatives to accompany their own development. Finally, it is hoped that this research, in addition to making a scientific contribution to the field of design, due to its interdisciplinary bias, can cooperate with citizens who use digital government services so that their right to privacy is ensured and guaranteed.

Keywords: *digital data privacy; privacy by design; user experience; electronic government.*

LISTA DE FIGURAS

Figura 1 - Composição do governo digital no Brasil	34
Figura 2 - Benefícios e riscos da estrutura governo digital	35
Figura 3 - Exemplo de escolhas pré-selecionadas	46
Figura 4 - Exemplo de destaque em opção específica	47
Figura 5 - Integração do <i>Privacy by Design</i> e da Linguagem Simples ao Design	56
Figura 6 - Delineamento da pesquisa	58
Figura 7 - Etapas da pesquisa e seus procedimentos	58
Figura 8 - Fluxo da RSL I	62
Figura 9 - Fluxo da RSL II	64
Figura 10 - Fluxo da Revisão de métodos	65
Figura 11 - Etapas de condução da <i>sketch interview</i>	68
Figura 12 - Locais em que foram realizadas as <i>sketch interviews</i>	68
Figura 13 - Alguns mapas mentais produzidos presencialmente	69
Figura 14 - Alguns mapas mentais produzidos digitalmente	70
Figura 15 - Cartões utilizados para sensibilização dos participantes	70
Figura 16 - Printscreen da página com conteúdo de sensibilização	71
Figura 17 - Sequência da codificação no ATLAS.ti	72
Figura 18 - <i>PrintScreen</i> da tela de codificação no software ATLAS.ti	73
Figura 19 - <i>PrintScreen</i> do TCLE e questionário on-line	76
Figura 20 - Locais de aplicação do questionário	77
Figura 21 - Histograma das classes de idades dos entrevistados	79
Figura 22 - Nível de familiaridade dos participantes com os temas	100
Figura 23 - Percepção dos participantes sobre dados sensíveis	101
Figura 24 - Respostas às afirmações apresentadas aos participantes	103
Figura 25 - Comportamento em relação aos botões de <i>cookies</i>	106
Figura 26 - PrintScreen da pergunta ilustrada sobre cookies	108
Figura 27 - Sugestões dos respondentes da pesquisa	108
Figura 28 - Clareza sobre privacidade e proteção de dados em serviços locais	109
Figura 29 - Diretrizes mais amigáveis e centradas nos cidadãos	111

LISTA DE QUADROS

Quadro 1 - Etapas da pesquisa	15
Quadro 2 - Princípios de <i>privacy by design</i>	50
Quadro 3 - Documentos que compuseram a pesquisa documental	59
Quadro 4 - Protocolo da RSL I	60
Quadro 5 - Trabalhos selecionados na RSL I	61
Quadro 6 - Protocolo da RSL II	62
Quadro 7 - Trabalhos selecionados na RSL II	63
Quadro 8 - Trabalhos selecionados nas RSL I, II e revisão narrativa	65
Quadro 9 - Procedimento do levantamento de dados via questionário	75
Quadro 10 - Códigos analíticos e traços do CD - Definindo privacidade	82
Quadro 11 - Códigos analíticos e traços do CD - Expressando familiaridade	85
Quadro 12 - Códigos analíticos e traços do CD - Levantando conceitos	88
Quadro 13 - Códigos analíticos e traços do CD - Questionando a UX	90
Quadro 14 - Códigos analíticos e traços do CD - Abordando hábitos digitais	91
Quadro 15 - Códigos analíticos e traços do CD - Identificando riscos	92
Quadro 16 - Códigos analíticos e traços do CD - Revelando sentimentos	93
Quadro 17 - Códigos analíticos e traços do CD - Indicando aprendizado	94
Quadro 18 - Códigos analíticos e traços do CD - Explicando por comparações	96
Quadro 19 - Códigos analíticos e traços do CD - Demonstrando falta de conhecimento	96

LISTA DE TABELAS

Tabela 1 - Associação de termos e resultados da RSL I	61
Tabela 2 - Associação de termos e resultados da RSL II	63
Tabela 3 - Códigos descritivos gerados	80
Tabela 4 - Nível de escolaridade dos respondentes	99
Tabela 5 - Matriz de interação dos participantes	105

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Agência Nacional de Proteção de Dados
CA	Códigos Analíticos
CD	Códigos Descritivos
<i>E-gov</i>	<i>Electronic Government</i>
HCD	Design Centrado no Humano
HCI	Interação Humano-Computador
IoT	Internet das Coisas
IxD	Design de Interação
LGPD	Lei Geral de Proteção de Dados
TI	Tecnologia da Informação
TICs	Tecnologias da Informação e Comunicação
UCD	Design Centrado no Usuário
UI	Interface do Usuário
UX	Experiência do Usuário

SUMÁRIO

1 INTRODUÇÃO	15
1.1 Problema e pergunta de pesquisa	16
1.2 Objetivos	18
1.3 Justificativa	18
1.4 Etapas da pesquisa e procedimentos	20
1.5 Estrutura da dissertação	22
2 FORMAÇÃO DO GOVERNO DIGITAL NO BRASIL	23
2.1 Governo Eletrônico	24
2.1.1 Digitalização e modernização do Estado	24
2.1.2 Aplicação de TICs na administração pública	25
2.2 Do Governo Eletrônico para o Governo Digital	26
2.2.1 Prestação de serviços ao cidadão	27
2.2.2 Cidadania e inclusão a partir do governo digital	28
2.2.3 Mobile Government ou governo móvel	30
2.2.4 Proteção de dados pessoais	31
2.3 Ameaças à privacidade	33
2.3.1 Governos e cidades inteligentes	33
2.3.2 Ameaças ao cidadão usuário	36
2.3.3 O valor da privacidade	38
2.4 Considerações do capítulo	40
3 A PRIVACIDADE RELACIONADA A ABORDAGENS DO DESIGN	42
3.1 Contribuições do Design	43
3.1.1 Interação humano-computador (HCI)	43
3.1.2 Design centrado no usuário (UCD), no humano (HCD) e na humanidade	44
3.1.3 Design de interação (IxD)	48
3.1.4 Usabilidade	50
3.1.5 Experiência do usuário (UX)	54
3.2 Privacidade pelo projeto (Privacy by design)	56
3.3 Linguagem cidadã	59
3.4 Considerações do capítulo	61
4 MÉTODOS E TÉCNICAS	63

4.1 Caracterização da pesquisa	63
4.2 Pesquisa bibliográfica e documental	64
4.2.1 Revisões sistemáticas de literatura	65
4.2.2 Revisão de métodos e técnicas	70
4.3 Pesquisa qualitativa	71
4.2.1 Pesquisa com enfoque fenomenológico	72
4.2.2 Entrevistas	72
4.2.3 Análise dos dados qualitativos	77
4.4 Pesquisa quantitativa	79
4.3.1 Levantamento de campo	80
4.3.2 Questionário	80
4.3.3 Análise dos dados quantitativos	83
4.5 Convergência dos dados qualitativos e quantitativos	83
5 RESULTADOS	85
5.1 Sketch Interview	85
5.1.1 Codificação descritiva	85
5.1.2 Codificação analítica	87
5.1.3 Descrição completa	87
5.2 Questionário	104
5.2.1 O perfil dos respondentes	104
5.2.2 Resultados do questionário	105
5.3 Convergência e discussão	115
5.3.1 Diretrizes quanto à privacidade e a proteção de dados pessoais	116
5.3.2 Diretrizes quanto às políticas de privacidade e termos de consentimento	117
5.3.3 Governo digital no Maranhão	120
6 CONSIDERAÇÕES FINAIS	121
6.1 Limitações da pesquisa	122
6.2 Desdobramentos	123
6.3 Lições aprendidas	123
REFERÊNCIAS	125
APÊNDICES	136
Apêndice A. Parecer do Comitê de Ética	137
Apêndice B. TCLE Sketch Interview	140
Apêndice D. Mapas mentais produzidos pelos participantes	146

Apêndice E. TCLE Questionário

149

Apêndice F. Questionário

151

1 INTRODUÇÃO

As facilidades trazidas pela era da informação são evidentes e indispensáveis em várias esferas da sociedade. Foram naturalizadas, não só em iniciativas privadas, mas também na administração pública, em sua prestação de serviços à população. No Estado, esse cenário é visto na consolidação do governo digital, uma estrutura que propõe sua desburocratização e modernização, aproximando-o do cidadão (Brasil, 2021a).

O governo digital é a evolução do governo eletrônico. Este último tem como principal característica a automatização de processos e documentos impulsionado pela evolução tecnológica e pela globalização (OCDE, 2018). Essa transformação foi norteadada por diferentes fases da *web* e aplicação das Tecnologias da Informação e Comunicação (TICs). Elas são recursos tecnológicos usados para mediar e automatizar a comunicação e a informação (Cristóvam *et al.*, 2020).

Com o passar do tempo, a estrutura pública digital passou a propor a autonomia do cidadão. Assim como a sua inclusão digital a partir da obtenção de serviços e políticas públicas (Brasil, 2021a). Além disso, os artefatos do dia a dia também se tornaram conectáveis à internet, um conceito conhecido por Internet das Coisas (IoT) (Kreuz; Viana, 2019).

As cidades também convertem-se em inteligentes, recorrendo à aplicação de TICs e IoTs aos elementos do ambiente na busca por soluções para melhorar a qualidade de vida dos seus cidadãos. O objetivo é apresentar uma gestão mais transparente e eficiente (Reia; Beli, 2021). Dessa forma, a rede conecta não apenas máquinas, mas ambientes, pessoas e organizações.

Para que sejam eficientes, os serviços precisam de informações dos usuários, dados pessoais obtidos da rede. Assim, é possível aprimorar ações e personalizar ainda mais os serviços prestados. Coletar, tratar e armazenar dados mostra-se uma prática comercial e política a depender dos interesses de quem os detém e utiliza¹. Isso estabelece uma realidade de capitalismo de dados (Zuboff, 2018), em que o lucro sobre as informações a despeito do consentimento e compreensão afeta sistemas, empresas e governos.

¹ No escândalo *Cambridge Analytica*, 87 milhões de usuários do *facebook* tiveram dados coletados para uso propaganda política a fim de influenciar as eleições presidenciais de 2016 nos Estados Unidos e o *Brexit* em 2017. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>

A produção de dados digitais hoje em dia é inevitável. Diante dos interesses econômicos relacionados a eles, a privacidade, um direito fundamental e subjetivo, precisa ser considerada nos serviços que envolvam dados pessoais (Véliz, 2021). Tal contexto alavanca regulamentações que fiscalizem e garantam a preservação da privacidade dos cidadãos diante do sistema de coleta de dados. A Lei Geral de Proteção de Dados brasileira (LGPD), Lei nº 13.709/2018, zela para que os cidadãos sejam informados desde o princípio que seus dados estão sendo coletados, como estão sendo e que tratamento receberão pelos operadores das entidades coletoras (Brasil, 2020).

A LGPD é visualizada, de forma prática, pela presença de *pop-ups* de aceitação e gerenciamento de *cookies*², caixas de diálogo e *links*. Eles levam ao texto das políticas de privacidade e dos termos de consentimento em *sites*, plataformas e aplicativos. O que é apresentado aos usuários nessas telas é o que é determinado nos parágrafos e incisos da LGPD, embora em formas complexas.

São recorrentes as expressões jurídicas para explicar o objetivo e etapas de documentos e ações. De acordo com Gervazoni (2023), as organizações buscam apenas se adequar à legislação. Não há preocupação com o cidadão e a elaboração do documento. Para ela, isso torna o processo de entendimento questionável.

Segundo a pesquisa Privacidade e Proteção de Dados Pessoais 2021, do Comitê Gestor da Internet no Brasil (2022), quanto à leitura de políticas de privacidade nas telas de *sites* e aplicativos no país, 81% dos usuários de internet não as lêem integralmente por serem muito longas e 69% por considerarem-nas difíceis de entender.

1.1 Problema e pergunta de pesquisa

A forma como a LGPD é apresentada aos cidadãos revela um problema. Ela não é totalmente compreensível. Considerando que o objetivo da adoção da tecnologia pela esfera pública é democratizar e desburocratizar, apresentações e informações complexas são contraproducentes. Com 38 milhões de habitantes analfabetos funcionais (Costa, 2019) e 42,4% da população brasileira deixando de utilizar internet por não saber (Silva, 2022), essa problemática torna-se um fator de exclusão de grupos já vulnerabilizados no contexto nacional.

² método para rastrear atividades do usuário na internet.

Além disso, a interação dos cidadãos com políticas de privacidade e termos de consentimento estão relacionadas a questões de usabilidade e ergonomia. Estudos anteriores revelam que as janelas, *pop-ups* e *cookies* exibidos aos usuários tendem a compeli-los e induzir suas tomadas de decisões em prol dos interesses de outros agentes, que coletam os dados (Alharbi *et al.*, 2023; Machuletz; Böhme, 2020).

Isso revela, por sua vez, que as interfaces em que estão inseridas os documentos e assuntos relacionados ao direito à privacidade não são amigáveis aos cidadãos (Bartali; Velsen, 2023; Chalhoub, 2023), comprometendo, dessa forma, o que espera-se de uma experiência do usuário com valor e significado, que atenda às suas necessidades satisfatoriamente (Agner, 2023; Kuang; Fabricant, 2022), sem ludibriá-los (Rogers *et al.*, 2023).

Os dados apresentados são usados para fomentar o problema de pesquisa. Há contemporaneamente a necessidade de conexão para serviços básicos por meio do governo digital. Entretanto, o acesso dos usuários à tecnologia e aos dispositivos são baseados em rastros digitais a partir da coleta de seus dados pessoais, cujo valor obedece a interesses econômicos.

Partindo da ideia de Brasil como país não plenamente desenvolvido, com índices de exclusão digital, problemas de alfabetização e acesso à internet, as medidas aplicadas para proteger a privacidade dos cidadãos, determinadas pela LGPD, são projetadas de forma a comprometer o acesso do usuário, sua compreensão a respeito de privacidade e a proteção dos seus dados pessoais.

Portanto, esta pesquisa questiona, **quais as diretrizes mais amigáveis e centradas nos cidadãos para garantia da privacidade e proteção aos dados pessoais no governo digital?**

Em uma perspectiva mais positiva aos usuários, este trabalho pensa no Design, a partir dos seus conceitos, como um caminho para a questão. Ao considerar abordagens que propõem a adoção de habilidades e perspectivas multidisciplinares, prioriza-se toda a experiência do usuário e o envolvimento deles durante todo o processo de design, visando a compreensão dos desejos, necessidades e experiências.

Pensar no contexto dos cidadãos é o que de fato permite que a sua interação com o governo digital seja menos burocrática e mais ágil e inclusiva. Dessa forma, é

possível assegurar que, durante a prestação de serviços, eles estejam conscientes sobre seus direitos. Assim como sobre a forma como seus dados estão sendo utilizados nas tomadas de decisões e projetos que envolvam o governo digital.

Portanto, busca-se promover uma relação entre estudos sobre governo digital e questões de privacidade articulando-as a correntes do Design. Assim, esse encontro proporcionaria uma visão multidisciplinar focada no cidadão, suas particularidades, experiências e expectativas, de modo que possa contribuir com o campo científico e produzir um escopo que seja capaz de auxiliar nas questões de proteção de dados digitais e no trabalho governamental pela inclusão, inovação e digitalização.

1.2 Objetivos

Sob a ótica do design e a partir da proposta de transparência, acessibilidade, emancipação e letramento digital o objetivo geral deste trabalho é:

Apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital.

Para isso, são elencados os seguintes objetivos específicos:

- Descrever o governo digital brasileiro e como a privacidade e proteção de dados estão posicionadas nele;
- Interseccionar conceitos de design e ergonomia à privacidade, ao consentimento, à proteção de dados pessoais e ao governo digital, e identificar suas contribuições para orientar a comunicação e interação relacionadas a essas questões;
- Mapear métodos e técnicas de design que considerem a perspectiva do usuário nos estudos sobre privacidade;
- Conhecer percepções que usuários têm sobre privacidade e proteção de dados pessoais;
- Indicar como usuários do governo digital interagem com as políticas de privacidade e com os termos de consentimento;
- Convergir os resultados para entender os caminhos de abordagem da privacidade e da proteção aos dados pessoais.

1.3 Justificativa

O trabalho justifica-se, primeiro, pelo crescente uso de iniciativas do governo digital e móvel na prestação de serviços à população. Considera-se o atual ciclo da Estratégia brasileira para a transformação digital, que busca "oferecer políticas públicas e serviços de melhor qualidade, mais simples, acessíveis a qualquer hora e lugar e a um custo menor para o cidadão" (Brasil, 2022). Segundo, levando em consideração o ponto de vista da proteção de dados pessoais para promover a segurança dessas pessoas durante o uso do governo digital em uma perspectiva focada de fato no cidadão a partir do Design.

Resultados da pesquisa TIC Domicílios 2022, do Comitê Gestor de Internet no Brasil, indicam que 34% dos usuários de internet usaram a rede para acessar serviços ou *sites* governamentais. Entre esses, 36% acessaram serviços de saúde pública; 32% direitos do trabalhador ou previdência social; 31% a serviços relacionados a documentos pessoais; 24% acessaram serviços relacionados à educação pública (CGI.br, 2023).

Os números demonstram a crescente conexão com o governo digital. Ele possibilita o acesso a direitos básicos orientando a plena cidadania desejada em uma sociedade democrática. Entretanto, não contemplando o todo, se analisados os índices recentes dos usuários de internet no País.

Ainda de acordo com a TIC Domicílios 2022, 15 milhões de residências brasileiras ainda não estão conectadas à internet. No país, 36 milhões de pessoas se consideram não-usuários de internet, sendo 19 milhões delas das classes D e E. 29 milhões dessas pessoas têm educação até o ensino fundamental e 18 milhões têm mais de 60 anos. Esses participantes revelaram que nunca usaram internet por falta de habilidade com computador (69%), pelo preço (39%), por preocupação com privacidade (36%) e por não terem onde usar (28%).

Outra informação trazida pela pesquisa é que 62% dos usuários acessam a internet exclusivamente pelo celular (*ib.*, 2023). Contudo, mesmo com o crescimento do uso de *smartphones* para acesso à serviços, um requisito básico para isso, a conexão, apresenta números significativos no Maranhão. O Estado está em último lugar, entre as outras unidades da federação, em relação à qualidade da conexão de internet no país (Brasil, 2024).

Os dados das pesquisas contribuem para o cenário de expansão do uso da tecnologia brasileira. No entanto, não deixam de quantificar disparidades a respeito

da não democratização e universalização de acesso por diferentes grupos da nossa sociedade. Serviços estão sendo disponibilizados on-line e parte da população brasileira ainda não se encontra totalmente presente no ambiente digital. Ou mesmo tem habilidade para utilizá-lo. Isso inviabiliza o pleno exercício de seus direitos e exemplifica a importância de estudos que abordem essa problemática.

A preocupação com a preservação da privacidade dos cidadãos no contexto do governo digital origina-se da mercantilização de informações pessoais no capitalismo de dados. Como a pesquisa revelou (CGI.br, 2023), mais de um terço dos não-usuários deixam de acessar a internet por preocupações de privacidade. No entanto, essa pode não ser sequer uma preocupação prioritária dos demais. Dessa forma, os dados revelam oportunidades, posicionando esse grupo como alvo, visto a lucratividade que a posse de dados pode gerar.

De acordo com Doss (2020, p. 15), "a privacidade é intrínseca à dignidade individual, à nossa personalidade e à nossa habilidade de viver como seres únicos" e para Véliz (2021, p. 9), "estamos no início de uma luta para proteger dados pessoais na era digital". O que exemplifica a importância de assegurar a preservação da privacidade dos usuários uma vez que ela garante um ambiente e navegação digital saudáveis e seguros a todos.

Portanto, esta dissertação revela a proposta de uma abordagem humanizada para um contato saudável das pessoas com as tecnologias que fazem parte do seu cotidiano. O que demonstra a relevância dessa temática para a atualidade, em prol da inclusão digital e da inovação pública para todos, na busca pela segurança e governança de dados, contribuindo também para a soberania digital brasileira. Além de buscar cooperar com o desenvolvimento da estrutura governo digital e contribuir cientificamente com a disciplina design ao propô-la enquanto mediadora na resolução de problemas que podem trazer impactos negativos para populações mais vulneráveis e já afetam a sociedade, não apenas brasileira.

1.4 Etapas da pesquisa e procedimentos

Esta pesquisa foi desenvolvida em quatro etapas que atendem aos objetivos específicos propostos. A primeira etapa tratou das pesquisas bibliográfica e documental. Elas foram conduzidas por meio de revisão sistemática e assistemática de literatura, com o propósito de fundamentar teoricamente a dissertação.

A segunda etapa da pesquisa consistiu na aplicação da primeira parte de coleta de dados qualitativos em campo. Nela, foram realizadas *sketch interviews*. A técnica propôs aos participantes, além de responder às perguntas da entrevista, produzir mapas mentais para expressar suas ideias, a fim de também atender a um objetivo específico do estudo.

Na etapa seguinte, a terceira, foi realizada a segunda parte de coleta de dados, desta vez quantitativos. Foram divulgados questionários para serem respondidos virtualmente por participantes. Assim como também houve a aplicação dos mesmos questionários de forma presencial com outros respondentes.

A quarta etapa da pesquisa compreendeu a análise dos dados coletados nas etapas 2 e 3. Em relação às *sketch interviews*, ela foi realizada por meio da codificação de dados qualitativos no *software* de análise de dados Atlas.ti e da interpretação dos códigos criados. Quanto aos questionários, foram analisados por meio de estatística descritiva. Todas as etapas da pesquisa podem ser visualizadas no quadro 1, abaixo.

Quadro 1 - Etapas da pesquisa

Etapas	Técnicas	Capítulo	Objetivo
Etapa 1	Pesquisa bibliográfica e documental Revisões sistemática e assistemática de literatura	Capítulo 2	Descrever o governo digital brasileiro e como a privacidade e proteção de dados estão posicionadas nele.
		Capítulo 3	Interseccionar conceitos de design e ergonomia à privacidade, ao consentimento, à proteção de dados pessoais e ao governo digital, e identificar suas contribuições para orientar a comunicação e interação relacionadas a essas questões.
		Capítulo 4	Mapear métodos e técnicas de design que considerem a perspectiva do usuário nos estudos sobre privacidade.
Etapa 2	Pesquisa qualitativa <i>Sketch Interview</i>	Capítulo 5	Conhecer percepções que usuários têm sobre privacidade e proteção de dados pessoais.
Etapa 3	Pesquisa quantitativa Questionário	Capítulo 5	Indicar como usuários do governo digital interagem com as políticas de privacidade e com os termos de consentimento.

Etapa 4	Análise e interpretação dos dados Codificação de dados qualitativos, estatística descritiva e convergência dos dados	Capítulo 5	Convergir os resultados para entender os caminhos de abordagem da privacidade e da proteção aos dados pessoais.
---------	--	------------	---

Fonte: elaborado pela autora, 2024.

1.5 Estrutura da dissertação

Este trabalho apresenta 6 capítulos. Seguente à introdução, no segundo capítulo, são apresentadas as ideias a respeito da evolução da prestação de serviços on-line e do governo eletrônico, a instituição das políticas de proteção de dados e seu impacto na sociedade. Este capítulo cumpre o primeiro objetivo específico: descrever o governo digital brasileiro e como a privacidade e proteção de dados estão posicionadas nele.

No terceiro capítulo são apresentados conceitos de design, *privacy by design* e linguagem simples em perspectiva a uma privacidade centrada no usuário-cidadão. Este capítulo cumpre o segundo objetivo específico: interseccionar conceitos de design e ergonomia à privacidade, ao consentimento, à proteção de dados pessoais e ao governo digital, e identificar suas contribuições para orientar a comunicação e interação relacionadas a essas questões.

O quarto capítulo apresenta os métodos e técnicas utilizados, além de cumprir o terceiro objetivo específico: mapear métodos e técnicas de design que considerem a perspectiva do usuário nos estudos sobre privacidade.

No quinto capítulo, há os resultados a partir da análise dos dados obtidos via pesquisa bibliográfica e documental, *sketch interview* e aplicação de questionários. Ele cumpre o último objetivo específico da pesquisa: convergir os resultados para entender os caminhos de abordagem da privacidade e da proteção aos dados pessoais. Por fim, o capítulo sexto traz as considerações finais, lacunas e oportunidades futuras para a pesquisa.

2 FORMAÇÃO DO GOVERNO DIGITAL NO BRASIL

As transformações tecnológicas visualizadas na transição do século XX para XXI mudaram não só o relacionamento dos cidadãos com produtos e serviços, mas também com o Estado. A digitalização em prol da modernidade (Vaz, 2002) também se estendeu aos papéis e processos que tanto caracterizavam o serviço público. Foram os primeiros passos do governo eletrônico até o governo digital como é conhecido hoje.

O presente capítulo pretende, portanto, lançar luz sobre essa evolução por meio de uma pesquisa bibliográfica acerca dos trabalhos atuais através de conceitos como governo eletrônico, transformação digital, tecnologias da comunicação e informação, internet das coisas, governo digital, inclusão e exclusão digital e alfabetização, cidadania digital, vigilância, viés algorítmico e proteção aos dados pessoais, no contexto nacional.

Além disso, pretende-se apresentar a pesquisa documental através da legislação brasileira. Como ela desenha o formato e as propostas de governança que visam desburocratizar e aproximar o Estado da população. Além da relação com a proteção da privacidade e dados pessoais, a fim de entender as relações entre as determinações legais e a compreensão do cidadão.

Dessa forma, a primeira seção deste capítulo aborda o surgimento e estruturação do governo eletrônico no cenário dos serviços públicos brasileiros. Há o diálogo com vozes que revelam as características do *e-government* e a aplicação das Tecnologias de Informação e Comunicação (TICs). Assim como as iniciativas bem sucedidas da administração pública em prol da modernização do Estado.

A segunda seção aborda o processo transicional em que o governo eletrônico brasileiro torna-se governo digital. Trata também da publicação de legislações que o fortaleceram, como o Marco Civil da Internet e a Lei do Governo Digital. Além da perspectiva da prestação de serviços e manutenção do exercício da cidadania a partir da inclusão digital.

Na terceira seção, a proteção aos dados pessoais é discutida no contexto do *smart government* e das cidades inteligentes. Por fim, na quarta seção são sintetizadas e apresentadas as principais considerações a respeito deste capítulo. O objetivo é identificar o governo digital brasileiro e como a privacidade e a proteção de dados estão posicionadas nele.

2.1 Governo Eletrônico

O *e-government*, *e-gov*, *electronic government* ou governo eletrônico, no Brasil, surge oficialmente a partir do ano 2000, por meio da instituição da Política de e-governo, do Programa Sociedade da Informação e da criação do Comitê Executivo do Governo Eletrônico (CEGE), do governo federal (Cerquinho, 2017; Diniz *et al.*, 2009; Martinuzzo, 2007; Matos Neto, 2020; OCDE, 2018; Viana, 2021).

Segundo Viana (2021), o *e-gov* se caracteriza pelo desenvolvimento de quatro etapas, sendo a primeira a digitalização e o fornecimento de informações em que há apenas presença on-line; na segunda, serviços começam a ser prestados; a terceira consiste em possibilitar transações, de forma segura e em tempo real; a quarta etapa é marcada pela integração entre os sistemas, mostrando que os órgãos estão conectados assim como os cidadãos e seu governo.

2.1.1 Digitalização e modernização do Estado

Na administração pública brasileira, à época, o cenário que recepcionou o desenvolvimento dessas etapas foi de necessidade de racionalização de recursos. O contexto político era o processo de redemocratização e da pressão social pela transparência governamental. Havia expectativa pela melhoria do atendimento e da qualidade dos serviços públicos, além das possibilidades trazidas pela tecnologia da informação (Vaz, 2002).

Dessa forma, o advento do *e-gov* está relacionado a um processo de digitalização dos trabalhos. Ele foi embasado em uma ideia de agilidade, produtividade e conectividade que se consolidou durante as décadas de 1990 e 2000. Enquanto senso comum, tem-se como marco do processo de digitalização e modernização dos processos o uso dos microcomputadores ou computadores pessoais.

A popularização da internet e os *softwares* de produtividade, que vieram na esteira, contribuíram ainda mais. A possibilidade do bug do milênio, por exemplo, influenciou determinantemente a estruturação do governo eletrônico brasileiro (Balbe, 2010; Diniz *et al.*, 2009; Vaz, 2002). Ano a ano novas ações foram instituídas a fim de alimentar a estratégia do *e-gov* brasileiro, como

- portal do governo eletrônico (2001);

- portal da transparência e departamento de governo eletrônico da Secretaria de Logística e Tecnologia da Informação - SLTI (2004);
- portal de inclusão digital (2006);
- decreto de simplificação do atendimento ao cidadão (2009);
- programa nacional de banda larga (2010);
- programa cidades digitais (2013);
- lei do marco civil da internet (2014);
- estratégia brasileira de transformação digital (2018);

entre outros (Brasil, 2018; Cerquinho, 2017; Diniz *et al.*, 2009; OCDE, 2018).

Com a mudança de gestão no governo federal em 2003, como aponta Martinuzzo (2007), o então formato de governo eletrônico brasileiro voltou seu foco para a oferta de serviços aos cidadãos das classes C, D e E. A relação com municípios e Estados em prol de soluções e sistemas integradores foi priorizada.

A redução dos custos no acesso a serviços on-line e os incentivos à indústria e pesquisa brasileiras também foram priorizados. Para o autor (Martinuzzo, 2007), houve uma transição de perspectiva do governo eletrônico focado nos desafios da globalização para um *e-gov* que considerava o contexto e as problemáticas sociais e econômicas da população.

2.1.2 Aplicação de TICs na administração pública

O *e-gov* também foi responsável por uma mudança na perspectiva de interação não só com os seus cidadãos, mas com empresas e outros governos (Balbe, 2010; Diniz *et al.*, 2009; Martinuzzo, 2007; Viana, 2021). E o seu desenvolvimento de fato só foi possível pela aplicação das Tecnologias de Informação e Comunicação dentro do serviço público.

De acordo com Balbe (2010), no *e-government* brasileiro, o uso dessas tecnologias possibilitou conquistas como a implementação do Portal da Transparência (2014); o Programa Nacional do Livro Didático; o uso de PDAs computadores portáteis e pessoais pelo censo (2006); o Receitanet, para entrega da declaração do imposto de renda pela internet; e as Urnas Eletrônicas, em sua totalidade em todos os municípios brasileiros (2004), todas reconhecidas e premiadas como iniciativas inovadoras às suas épocas.

Embora o processo eletrônico trouxesse novas possibilidades, no Brasil dos anos 2000, a democratização do acesso à informação digital ainda era difícil. Entre a tentativa de modernizar para facilitar, havia também a probabilidade de modernizar e excluir. Para Vaz (2002), a interação da população com o governo eletrônico estava diretamente relacionada à capacitação em vista da inclusão digital, assim como "a exclusão digital não só é consequência da exclusão social, como também vem a reforçá-la" (*ib.*, p. 20).

Dessa forma, a exclusão no acesso à informação comprometendo a transparência governamental, só poderia ser mudada por políticas públicas orientadas. Para ele, as diferenças da nossa sociedade revelam a ineficácia de ações de curto prazo e unidimensionais e "é importante criar condições para que as organizações da sociedade civil possam apropriar-se da internet para trocar e disseminar informações que permitam o reforço da cidadania" (Vaz, 2002, p. 21). Afinal, é na promoção da participação cidadã que as necessidades da população são identificadas e podem ser satisfeitas (Cerquinho, 2017).

No *e-government*, o cidadão não influenciava no processo do governo eletrônico, ele era apenas um receptor de informações. O movimento de popularização da internet aumentou o grau de participação do cidadão e trouxe o que Cerquinho (2017) chama de "*i-government*", ou o governo digital, e para que ele de fato seja efetivo a participação cidadã precisa ser convertida em políticas públicas que se concretizem.

O governo eletrônico fica então caracterizado enquanto primeira representação do Estado na era da informação. No entanto, os novos hábitos e dinâmicas dos anos 2010 impõem uma outra perspectiva sobre o que significa estar presente no ambiente digital. De eletrônico, o governo da cibersociedade desenha um novo formato e deve tornar-se governo digital.

2.2 Do Governo Eletrônico para o Governo Digital

De acordo com a revisão do Governo Digital brasileiro feita pela Organização para Cooperação e Desenvolvimento Econômico - OCDE em 2018, a transformação do eletrônico para o digital se baseia em seis dimensões de políticas públicas.

Sendo elas na transição (1) de uma administração centrada no usuário para uma que seja conduzida pelo usuário; (2) de reativo a proativo na elaboração de

políticas públicas e prestação de serviços; (3) de um governo centrado na informação para um setor público orientado por dados; (4) da digitalização de processos existentes ao processo por concepção digital; (5) de um governo provedor de serviços para um governo como plataforma para cocriação de valor público; (6) do acesso à informação para abertura como padrão.

2.2.1 Prestação de serviços ao cidadão

Segundo Cristóvam *et al.* (2020), o governo digital atende à evolução da sociedade brasileira possibilitando de fato o cumprimento dos direitos dos cidadãos através da prestação de serviços. Para Kreuz e Viana (2019), além do uso das TICs, a inserção de computação em nuvem e da Internet das Coisas (*IoT*) nos serviços digitais trouxe novos padrões de produção. Isso porque os avanços atuais, mais velozes, com maior alcance e impacto fomentaram o que é conhecido por quarta Revolução Industrial.

Nesse processo de interconexão entre Estado e tecnologia, a plena participação do cidadão é o que vai legitimar a transparência pública, assim como o exercício da dignidade digital. Segundo Martinuzzo (2007), o *e-government* também é uma oportunidade de mediação sociopolítica. Isso porque ele possui capacidade tecnológica de influenciar fenômenos sociais.

Na internet, classificada por ele como uma promessa de nova ágora política, instrumentos de participação cidadã se consolidam. Programas como e-cidadania, do Senado, e o orçamento participativo, sintetizam esse movimento. E, também, o estabelecimento do conceito de e-democracia, em que instrumentos digitais são usados para facilitar o exercício à democracia por meio da interatividade política (Kreuz; Viana, 2019).

Portanto, o governo digital nasce como uma evolução natural do *e-government*. Um conceito para abarcar todas as transformações tecnológicas que marcaram a chegada da década 2010. Nele, a sensação de agilidade e facilidade, que caracteriza a identidade digital neste século, é indispensável para o cidadão.

Essas pessoas interagem ativamente com produtos tecnológicos, *big techs*³ e redes sociais focadas em aprimorar a experiência dos seus usuários. Dessa forma, a população desenvolve os mesmos tipos de expectativas em relação aos serviços

³ Grandes conglomerados tecnológicos que dominaram o segmento nas últimas décadas. Disponível em: <https://hbr.org/2022/01/can-big-tech-be-disrupted>

públicos on-line. Ou seja, visam a usabilidade, a praticidade e a simplicidade por meio deles (OCDE, 2018).

Esse processo é retratado no Brasil pela publicação da Lei do Governo Digital (Lei nº 14.129/2021). Ela oficializa a proposta de tornar os serviços e atendimentos ao cidadão mais eficientes. Se antes ele automatizava e agilizava processos, agora foca no cidadão, em atender suas demandas e simplificá-las aproximando-o do Estado.

De acordo com a diretriz, o objetivo é "desburocratização, modernização, fortalecimento e simplificação da relação do poder público com a sociedade mediante serviços digitais, inclusive por meio de dispositivos móveis" (Brasil, 2021a). Para cumprimento da lei levam-se em consideração, os conceitos de autosserviço, dados abertos e, inclusive, tratamento adequado a idosos.

Segundo o Art. 3º, são necessárias a simplificação e a desburocratização em prol de serviços digitais mais acessíveis, transparentes e de qualidade. O Art. 4º propõe a facilitação do uso de dados de acesso público em prol da inovação e desenvolvimento econômico. Enquanto no art. 14, as tecnologias que possibilitam acesso ao governo digital devem estar acessíveis a todos, independente da renda e da localização

De acordo com o Art. 25º, as plataformas do governo digital devem ter ferramentas de controle e transparência esclarecedoras. Inclusive em relação aos dados pessoais dos usuários em conformidade com a LGPD. Essa última determina, por sua vez, "a transparência na execução dos serviços públicos e o monitoramento da qualidade" (Brasil, 2021a).

Essas diretrizes corroboram a Lei de Proteção ao Usuário do Serviço Público, Lei nº 13.460/2017. Ela prevê o "uso de linguagem clara e compreensível a qualquer cidadão". Também determina o dever da autoridade pública em promover "soluções para melhoria do desempenho das organizações" (Brasil, 2017).

2.2.2 Cidadania e inclusão a partir do governo digital

Dentro da estrutura Governo Digital, o conceito de exercício à cidadania pelos canais digitais é uma necessidade. Na legislação brasileira, o pleno acesso à internet, indispensável a esse exercício, perpassa a garantia à inviolabilidade da intimidade, à vida privada e aos dados pessoais. Assim como ao dever das

plataformas de disponibilizar ferramentas de transparência e controle no tratamento de dados pessoais, fazendo isso de forma clara e acessível para que os cidadãos possam exercer tais direitos (Brasil, 2014; Brasil, 2017; Brasil, 2021a).

Desde a promulgação da Lei de Acesso à Informação (Lei nº 12.527/2011), a democratização ao acesso do ambiente digital já havia sido prevista. De acordo com o art. 5º, “é dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão” (Brasil, 2011).

O Marco Civil da Internet em 2014, Lei nº 12.965, também reflete questões relativas à cidadania digital e garantia de inclusão no ambiente digital. Além da importância da proteção aos cidadãos para a governança brasileira. No art. 4º, o documento reforça o objetivo de promover o direito de acesso à rede a todos bem como “à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos”, e à inovação com a democratização de novas tecnologias (Brasil, 2014).

Além disso, o fomento, a democratização e o exercício da cidadania foram previstos no Marco Civil em demais partes. Segundo o art. 26, o Estado deve educar e capacitar para o uso seguro, consciente e responsável da internet no exercício da cidadania. Já no art. 27, está determinado a promoção da inclusão digital, a busca da redução de desigualdades no acesso às TICs nas iniciativas públicas de incentivo à cultura digital (Brasil, 2014).

No país, há também a necessidade de metas e planos estratégicos para o desenvolvimento da internet no território nacional (Brasil, 2014). Entretanto, as dimensões continentais, a variabilidade cultural e as diferenças populacionais tornam complexo o processo de inclusão da população no ambiente digital no Brasil (OCDE, 2018).

Ainda assim, a atualização e reformulação da administração pública do país precisa prosseguir e não deve perpetuar a marginalização dos grupos vulnerabilizados (Cristóvam *et al.*, 2020) para atender a interesses comerciais de outros. Dessa forma, as soluções tecnológicas da administração pública e do governo digital precisam atender a população de forma eficiente e universal. Além de promover não apenas a plena satisfação do cidadão, mas a construção de um poder

público mais acessível, que não exclua a população que mais precisa das políticas públicas do Estado.

2.2.3 *Mobile Government* ou governo móvel

Recursos e plataformas digitais redefiniram a evolução do governo digital no setor público (Matos Neto, 2020). Essa trajetória vai desde a repartição digitalizada até um sistema que busca a participação social e permite a prestação de serviços aos cidadãos. Este último, nos anos recentes, se evidencia com o crescimento do uso de dispositivos móveis pela população, como *smartphones* e *tablets*, e redes sem fio.

A versão *mobile* do governo é um processo inevitável da digitalização governamental. No Brasil, 98,9% dos habitantes já usam o *smartphone* como principal meio de acesso à internet (IBGE, 2023). Retornando à pesquisa TIC domicílios 2022, dos usuários de internet no Brasil, 99% acessam pelos celulares e 62% usam exclusivamente esse tipo de dispositivo para entrar na rede (cgi.br, 2023).

Na esteira dessa tendência tecnológica, instituições e marcas precisaram se adaptar. Portanto, o governo móvel surge como uma extensão dentro do governo digital. O termo expande possibilidades e atende às especificidades do dispositivo móvel (Hanada *et al.*, 2020; Matos Neto, 2020).

Matos Neto (2020) pontua que a questão da superação dos smartphones frente aos computadores é uma característica dos países em desenvolvimento. Como no Brasil, em que o acesso à tecnologia ainda não é pleno e custa caro para muitos. Isso corrobora com a ideia da necessidade de trazer o governo para mais perto de todos e principalmente para aqueles que mais precisam dos serviços públicos.

Além da questão econômica, é inegável que o uso dos dispositivos móveis impactou na interação humana com a tecnologia. Um destaque é a disponibilidade irrestrita daqueles que estão conectados. A mobilidade alcançada permite que uma tarefa on-line seja realizada a qualquer momento e de qualquer lugar.

Antes as atividades dependiam de uma série de outras tecnologias e hoje são possíveis apenas com um celular na mão (Matos Neto, 2020). Essa característica ubíqua deste tempo se reproduz no governo móvel, *mobile government*, ou *m-government* (Hanada *et al.*, 2020).

O governo federal brasileiro mantém aplicações com altos índices de *download* e avaliação nas lojas de aplicativos. Em novembro de 2023, o aplicativo gov.br se tornou o terceiro *app* mais baixado no Brasil⁴, com 4,4 milhões de downloads durante o mês. Assim como a plataforma da qual ele faz parte, já fornece mais de 4.000 serviços on-line⁵.

Aplicativos como Carteira de Trabalho Digital, Meu INSS, CadÚnico, Meu SUS digital (antigo ConecteSUS) tinham respectivamente mais de 100 milhões, 50 milhões e 10 milhões de *downloads* na *PlayStore* até abril de 2025. Entre os principais aplicativos da Caixa Econômica Federal, os *apps* Bolsa Família, FGTS e CaixaTem possuem mais 50 milhões, 100 milhões, e 100 milhões de *downloads*, respectivamente, na mesma loja e período⁶.

Para Matos Neto (2020), o governo móvel está muito mais relacionado ao deslocamento do serviço público, do que ao dispositivo em si, e a como seus serviços podem atender à população em diferentes locais. Já Hanada *et al.* (2020) pontua que o valor maior está nas características distintas que as aplicações receberão em função da versão *mobile*.

O autor (Hanada *et al.*, 2020) identifica que as oportunidades, barreiras e fatores críticos de sucesso para iniciativas de adoção de tecnologias móveis no setor público

estão relacionadas à acessibilidade e disponibilidade, aumento da efetividade, redução de custos, localização e personalização de serviços, melhoria da imagem do governo e aumento da transparência. Já as barreiras e fatores críticos de sucesso estão relacionados a fatores de suporte ao projeto (suportes da autoridade administrativa, financeiro, dos fornecedores e de políticas e legislação), tecnológicos (custo da tecnologia, sua complexidade, compatibilidade com sistemas legados, recursos de hardware, habilidades de TI e adoção de tecnologia) e organizacionais (relacionados ao tamanho e à complexidade organizacional, à capacidade de comunicação, coordenação e cooperação entre departamentos, à existência de um campeão do produto e aos processos) (Hanada *et al.*, 2020)

2.2.4 Proteção de dados pessoais

Hoje os *smartphones* têm capacidade de gerar uma quantidade infinita de dados rastreáveis (Fonseca, 2020). Lemos e Araújo (2018) consideram a criação de

⁴ Disponível em: <https://www.tudocelular.com/android/noticias/n213736/gov-br-e-o-terceiro-app-com-mais-downloads.html>.

⁵ Disponível em: <https://www.gov.br/governodigital/pt-br/noticias/gov-br-ja-oferece-4-mil-servicos-publicos-digitais-para-o-cidadao>.

⁶ Informação acessada em abril de 2025.

aplicativos como um mecanismo para na verdade extrair dos cidadãos dados que revelem mais sobre seus hábitos, opiniões e perfis. E, para os autores, ao utilizar a versão *mobile* do *e-gov*, o usuário fornece seus dados ao governo, uma vez que "os aplicativos oficiais são uma das formas mais eficazes de colher informações voluntárias".

Portanto, há um processo de troca em que, ao oferecer informações, o cidadão tem acesso mais fácil aos serviços públicos. Dessa forma, os autores explicam que esse uso que os cidadãos fazem dos *apps* pode mostrá-los como indivíduos fiscalizadores do governo. Isso também faz com que o Estado tenha duas possibilidades para os dados: usá-los para agilizar solução a problemas identificados ou simplesmente para ter informações a respeito de locais e pessoas.

Sendo assim, os conceitos de participação social e cidadania digital propostos pelo governo digital podem mostrar-se equivocados. Isso porque o cidadão nesse contexto tecnológico pode ser reduzido a um usuário que não age criticamente. Ou seja, um indivíduo que apenas fornece dados sem questionar.

Esse cenário também fomentaria a exclusão digital. Pois, considera-se que os usuários fiquem à mercê da obrigatoriedade do uso de ferramentas digitais para comunicar-se com o governo (Lemos e Araújo, 2018). Além de estarem inseridos em um sistema de economia de dados, ou capitalismo de dados (Zuboff, 2018), em que os seus dados são coletados em função do valor econômico que possuem.

Com os novos recursos, todas as ações dos usuários no ambiente virtual geram rastros digitais. Isso aumentou a geração de dados e consequentemente a preocupação com a proteção aos dados pessoais pelo poder público e sociedade civil. Enfim, o direito à privacidade digital foi notado e o risco a sua garantia considerado. Fez-se necessário o estabelecimento de leis que regulassem em prol do cidadão comum.

Dessa forma, foi publicada no Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. Segundo a LGPD, no fornecimento dos dados pessoais dos cidadãos, o consentimento deve ser expresso e livre. Isso implica que sejam apresentadas informações suficientes e claras sobre a coleta, o uso e o tratamento dos dados pessoais, inclusive no exercício da cidadania digital no âmbito do governo digital (Brasil, 2020).

Segundo o art. 7º, o consentimento do usuário é requisito indispensável para o tratamento de seus dados pessoais, e na administração pública está sujeito à execução de políticas públicas devidamente regulamentadas. Já o art. 9º afirma que as informações sobre o tratamento dos dados devem ser acessíveis, fáceis e claras atendendo ao princípio de livre acesso ao usuário (Brasil, 2020). Na seção seguinte serão tratadas problemáticas que envolvem a grande geração de dados no atual contexto tecnológico e sua relação com o governo digital.

2.3 Ameaças à privacidade

Como visto, o governo digital no Brasil ressignificou a digitalização do Estado, voltando seu foco à prestação de serviços, a diferentes grupos sociais e à mobilidade. Ultrapassado esse nível, ele se torna governo inteligente, ou *smart government*. Um modelo que transcende a plataforma digital e o oferecimento de serviços, propondo revolucionar a governança pública (Souza; Ribeiro, 2021), envolvendo abordagens centradas no cidadão (Silva, 2020).

Assim, nesta seção a abordagem será sobre como o governo inteligente está dentro de um escopo maior. Ele envolve as *smart cities*, que, dada a sua complexidade, encaram o fenômeno capitalismo de dados. A partir daqui conceitos de cidade inteligente, o cenário brasileiro e como ela contribui para a formação da estrutura do governo digital. Assim como os riscos em uma sociedade e economia movidas a dados.

2.3.1 Governos e cidades inteligentes⁷

Kitchin (2016) reconhece que há diferentes visões para uma *smart city*. Ela pode ser aquela cujas tecnologias são usadas para configurar e gerenciar a infraestrutura urbana e os serviços. Ou pode ser a que usa TICs estrategicamente para melhorar as políticas urbanas por meio do *e-government* e dados abertos.

Romani *et al.* (2023) considera a integração dessas tecnologias a principal característica do modelo. Já Freitas e Silva (2020) e Rennó (2016) destacam como qualidade fundamental o funcionamento contínuo baseado em geração de dados.

⁷ Parte do material revisado nesta seção constituiu o artigo Contribuições sobre conceitos e características associadas à privacidade de dados nas Smart Cities submetido à V Jornada de Pesquisa do Programa de Pós-Graduação em Design - UFMA (JOP'24 Design).

Dessa forma, serviços e redes tradicionais tornam-se mais eficientes com a tecnologia sendo utilizada para solucionar problemas.

Essa cidade também pode ser a que aplica TICs para promoção da inovação e justiça social e transparência pública. Ela é, portanto, uma oportunidade de transformação social pela qual direitos, bem-estar social e dignidade se consolidam (Parini; Pegoraro, 2021). Para a carta brasileira para cidades inteligentes, são urbes

comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação (Brasil, 2021b).

Portanto, elas são caracterizadas pela integração tecnológica relacionada à inovação social, à segurança, à qualidade de vida, à inclusão, à sustentabilidade em prol do engajamento com seus cidadãos e da melhoria institucional (Bernardo, 2019; Rodrigues, 2021; Silva, 2020). Hoje o conceito também é entendido como Cidades Humanas Inteligentes e Sustentáveis (Brasil, 2021b; Porto *et al.*, 2020).

Dessa forma, há visões diferenciadas, mas que se complementam. Kitchin (2016) propõe uma síntese da principal expectativa de um *smart city*. Isso é, uma cidade em que a tecnologia e os dados podem ajudar a melhorar aspectos cotidianos para enfrentar os problemas urbanos. Os produtos dessa expectativa seriam economia, governo, mobilidade, ambiente, vida e pessoas inteligentes.

Como visto, os dados que movem as *smart cities* podem ser obtidos por meio do uso de dispositivos conectados à Internet das Coisas. A aplicação dele têm diversas possibilidades quando processados via *Big Data*⁸ ou utilizados no treinamento de sistemas de inteligência artificial e de aprendizagem por máquina. Para a cidade inteligente, esses dados são usados como informação e indicadores.

As informações que circulam por *smart cities* permitem a quantificação de diversos tipos de fatores sociais. Da produção de alimentos ao mapeamento de doenças, o objetivo é obter previsões que orientem ações estatais (Duarte, 2023). Por revelarem escolhas e preferências dos habitantes, esses dados contribuem na sustentação da administração pública e na atuação dos gestores da cidade.

⁸ Big Data é um poder computacional capaz de interpretar quantidade massiva de dados, também atendendo a usos governamentais. Embora esteja relacionado à quantidade, o mais importante são as várias possibilidades de pesquisa, informação e referências adquiridas a partir do tratamento em larga escala (Kremer, 2023).

Os dados também estão submetidos a interesses que podem ameaçar a privacidade dos cidadãos (Antonialli e Kira, 2020; Reia e Beli, 2021). Há diversidade de formas de coleta e elas muitas vezes fogem do conhecimento e concordância do cidadão. Principalmente quando têm em vista a identificação e o mapeamento dos indivíduos (Duarte, 2023; Löfgren; Webster, 2020; Romani *et al.*, 2023).

Na carta brasileira para cidades inteligentes também são definidos objetivos estratégicos para o desenvolvimento da proposta no país. Inclusive sendo utilizado para orientar os planos municipais para as *smart cities*, como o Plano Municipal São Luís Inteligente. Ambos os documentos levam em consideração a privacidade no estabelecimento de uma *smart city* (Brasil, 2021b; São Luís, 2023). Consideram-se agora, especificamente, os segundo e terceiro objetivos estratégicos apresentados pelo governo federal no documento renovado de 2021.

O segundo objetivo estratégico da carta propõe o provimento do acesso equitativo à internet. Ela deve ser de qualidade, reforçando a determinação da Lei do Marco Civil (Brasil, 2014), com acesso democratizado em todas as cidades (Brasil, 2021b). O que deve ser feito em alinhamento com a versão corrente da Estratégia Brasileira de Transformação Digital (Brasil, 2022).

Isso prevê dados e conectividade digital transparentes, apresentados em linguagem inclusiva, com tratamento direcionado aos municípios. O segundo objetivo também prevê a garantia dos padrões de segurança cibernética e de proteção aos dados pessoais nos projetos envolvendo IoT. Assim como a garantia à privacidade por meio da anonimização de dados e outros procedimentos (Brasil, 2021b).

O terceiro objetivo estratégico da carta determina o estabelecimento de sistemas de governança de dados e de tecnologias, com transparência, segurança e privacidade. Eles devem ser estruturados de acordo com cada realidade para de fato integrar e contribuir com o desenvolvimento urbano. A ideia é a cooperação entre governos e setores em que dados abertos possam ser compartilhados com a garantia da privacidade pessoal (Brasil, 2021b).

Dessa forma, deverá haver adesão completa à LGPD. Isso para garantir direitos fundamentais de liberdade intimidade e privacidade, obedecendo princípios de transparência e desenvolvimento ético, em concordância com a Autoridade Nacional de Proteção de Dados (ANPD).

Para Bernardo (2019), apenas digitalizar as cidades não as torna inteligentes. Levando-se em consideração a disparidade de acesso às TICs em países como o Brasil. Essas cidades estão, bem mais, atreladas à boa governança. Isso significa uma administração aberta, transparente, participativa e inclusiva.

Nesse sentido, é necessária a geração de estatísticas que recomendem pontos de atenção e melhoria. Isso é possível através da disponibilização acessível e gratuita de informações em uma política de dados abertos (Freitas; Silva, 2020), que cumpra o princípio de transparência na administração pública e da lei de acesso à informação.

No país, o decreto nº 8.777 institui a política brasileira de dados abertos do poder executivo federal. O objetivo do documento é de que sejam divulgadas informações que contribuam com a pesquisa, o desenvolvimento tecnológico, a inovação e a integração de serviços digitais (Brasil, 2016). Dados abertos significam uma grande quantidade de dados, que precisam de tecnologia adequada para serem processados.

As formas usadas para processá-los e tratá-los levantam questionamentos. Desde a forma como é definido quais dados são de interesse público até como o consentimento que deve ser declarado em sua coleta pode ser exibido, comunicado e confirmado (Löfgren; Webster, 2020). Visto que a privacidade deve ser fator central nessa operacionalização, de acordo com as determinações já abordadas aqui, os dados abertos também precisam ser regulamentados (Rezende *et al.*, 2019).

2.3.2 Ameaças ao cidadão usuário

Muitas são as ações da administração pública para 'smartizar' o Estado, destacam-se agora ações voltadas para a educação e a segurança pública que apresentam riscos à privacidade. Em relatório da organização *Privacy International* (2022), o uso de *EdTechs*⁹ na educação brasileira pós-pandemia representa uma preocupação. A conclusão é que "os alunos foram conduzidos a sacrificar o direito à privacidade em nome do direito à educação".

A adoção desse tipo de plataforma implica em acessos para organizações movidas a dados que fazem do processo de coleta o seu lucro. Dessa forma, a privacidade deveria ser também um dos critérios na escolha das tecnologias

⁹ *EdTechs* são empresas e organizações que fornecem e implantam serviços e recursos tecnológicos para a educação. Disponível em: <https://www.nu.edu/blog/what-is-edtech-education-technology/>

educacionais pelos estados brasileiros. Entretanto, isso parece não acontecer como deveria.

Segundo o relatório, as instituições privadas contratadas têm acesso irrestrito aos dados. Os serviços adotados para uso em sala de aula têm permissão para coletar dados dos estudantes, acessar fotos, câmeras e microfones dos seus dispositivos, e para armazenar essas informações. Os alunos e educadores estão em estado de vigilância, sem qualquer esclarecimento a respeito do armazenamento dos seus dados pessoais (Privacy International, 2022).

Para a organização, é necessário transparência nas relações e acordos público-privados. Quando *EdTechs* são contratadas para os serviços do governo digital deve-se saber qual o destino dos dados coletados e armazenados pelas empresas. Isso impõe limites sobre possíveis ações negativas consequentes do armazenamento dos dados (Privacy International, 2022).

Uma consequência negativa desse tipo de armazenamento é a contribuição desses dados para padrões tecnológicos de discriminação. Um desses padrões é viés algorítmico. Ele é um fenômeno em que preconceitos e visões de mundo das pessoas são incorporadas às tecnologias (Kremer, 2023). Isso acontece pois os dados coletados dos cidadãos são utilizados para treinar os algoritmos de aprendizagem de máquina¹⁰.

Alguns desses algoritmos herdam julgamentos pré-concebidos das pessoas que os criaram. Eles são baseados em pessoas, criados por elas e com impacto sobre elas, muitas dessas pessoas com vieses e preconceitos estabelecidos (Kremer, 2023). Atitudes discriminatórias, como o racismo algorítmico, por exemplo, passaram a ser registradas na segurança pública brasileira¹¹.

No governo inteligente, ações de videomonitoramento para reconhecimento facial não são mais novidade. O uso das câmeras de vigilância faz parte do cotidiano de vários municípios brasileiros para controlar grupos então classificados como perigosos. Tecnologias como essa combinam biometria e estatística aliadas a

¹⁰ Campo da inteligência artificial que se concentra no desenvolvimento de algoritmos e técnicas que permitem aos computadores aprenderem a partir de dados, sem serem explicitamente programados para tarefas específicas. Disponível em: mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained

¹¹ Disponível em: <https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoas-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-presos-por-26-dias.ghtml>

práticas automatizadas e sistemas baseados em aprendizado de máquinas para compreender fatores do crime e preveni-lo (Duarte, 2023).

A aplicação desse recurso aumenta cada vez mais, criando um paradigma. A privacidade diminui ao passo que a segurança supostamente aumenta. Isso desvirtua a proposta de uma cidade verdadeiramente inteligente, que promove a emancipação dos cidadãos e não os controla (Parini; Pegoraro, 2021).

Segundo a *Privacy International* (2022), o reconhecimento facial não deveria ser utilizado para mediar o acesso ao bem-estar social. Além disso, em função da proteção à privacidade e para mitigação das consequências negativas, requisitos mais específicos sobre os tipos de dados coletados deveriam ser determinados. Isso porque eles incluem, por exemplo, informações mais sensíveis como imagens, localização e biometria (Silva *et al.*, 2019).

2.3.3 O valor da privacidade

No decorrer de vinte anos de mudanças no comportamento e uso de recursos tecnológicos, a guarda de dados digitais tornou-se lucrativa. Uma vez que revela preferências, opiniões e perfis de consumo. O que gera uma verdadeira economia que privilegia quem os detêm, atribuindo um caráter comercial à privacidade que era prevista ser tratada como um direito a ser assegurado (Netto, 2020; Mafra, 2020).

Para Véliz (2021), esse é o cenário da sociedade da vigilância, que tornou aqueles que antes eram cidadãos, em provedores de dados digitais. Assim como

a economia de dados, e a vigilância onipresente da qual ela se alimenta, nos pegou de surpresa. As empresas de tecnologia não informaram aos usuários como nossos dados eram utilizados, muito menos pediram nossa permissão. Elas também não pediram aos nossos governos. Não havia leis para regular o rastro de dados deixado por cidadãos desavisados enquanto realizamos nossos negócios em um mundo cada vez mais digital. Na época em que percebemos que isso estava acontecendo, a arquitetura de vigilância já estava em vigor. Grande parte da nossa privacidade já havia desaparecido (*ib.*, p. 21).

Grandes empresas tecnológicas, que oferecem serviços gratuitos em troca da criação e fornecimento de dados de seus usuários, explicam o processo em seus termos de consentimento e até prometem fazer bom uso das informações. Contudo, elas nem sempre comunicam de forma transparente e prévia como esses dados serão tratados (Franco Jr., 2020; Netto, 2020).

Na sociedade movida a dados, o respeito à privacidade pode ser mais que uma questão de confiança. Ele pode ser o direito de preservar ideias, conversas, decisões e pensamentos para si mesmo. Ele é uma garantia à autonomia dos

cidadãos dentro do Estado, visando a preservação da democracia governamental (Mafra, 2020; Véliz, 2021).

Para Franco Jr. (2020), as variações sobre o nível de legalidade e legitimidade do uso de dados são permanentes. Segundo o autor, "houve, há e haverá países onde a garantia dos direitos humanos é no mínimo limitada, e o uso das informações por esses governos pode ser um problema para esses usuários" (*ib.*, p. 70).

As pessoas que fazem uso da internet nesse cenário preocupam-se com a sua privacidade e sentem-se vulneráveis. Principalmente em um mundo com redes sociais em que a exposição é ininterrupta. O grande desafio jurídico é adequar a proteção da privacidade frente ao avanço tecnológico desenfreado, constante e conscientemente para os cidadãos, à complexa demanda por regulamentações (Netto, 2020).

Segundo Mafra (2020), a dignidade humana é uma característica única e está diretamente ligada à proteção da privacidade. Para ele, ainda que a coletividade seja essencial para a sobrevivência humana, deve sempre ser subordinada à vontade do indivíduo. Ou seja, ele jamais deveria ser obrigado a ceder ao "inalienável direito de estar só" (*ib.*, p. 12).

O fato é que se faz necessário compreender o que significa o tratamento desses dados gerados uma vez que eles revelam tanto sobre a intimidade de muitos. Mas, mais do que isso, é necessário saber com qual finalidade eles estão sendo utilizados. E se isso de alguma forma não pode ser convertido em mais uma forma de opressão social, como afirma Netto (2020),

precisamos saber se os cidadãos são ou não discriminados a partir do que fazem nas redes sociais, ou dos conteúdos que visitam, produzem e compartilham na Internet. Precisamos saber se os dados das pessoas são utilizados apenas para os fins aos quais sua coleta foi consentida e se empresas vendem os dados que foram somente a elas confiados. Precisamos, portanto, da conquista de uma proteção legal, para nos sentirmos seguros e termos a quem recorrer em caso de usos ilegais e abusivos (Netto, 2020, p. 28).

Como visto anteriormente, os dados coletados indiscriminadamente através do comprometimento da privacidade das pessoas podem ser usados para manipulá-las. É possível induzir comportamentos e opiniões em função de interesses econômicos e políticos. Cidadãos podem ser submetidos a situações discriminatórias como o viés e o racismo algorítmicos alimentados por opiniões tendenciosas.

Isso demonstra a importância de preocupar-se com a privacidade de cada indivíduo e com as leis com a LGPD. Mas principalmente com pessoas que, mesmo à margem do processo digital-tecnológico e do acesso à internet, também têm seus dados coletados e armazenados. E, principalmente, o que o Estado deve fazer para protegê-los.

2.4 Considerações do capítulo

A partir das ideias apresentadas neste capítulo, é possível verificar que a estrutura do governo digital é essencial para facilitar o acesso a serviços e direitos. Especialmente pela possibilidade da disponibilidade a todo momento e de qualquer lugar. Para chegar nesse ponto, o *e-gov* passou por adaptações em função das novidades tecnológicas. A figura 1 sintetiza a composição do governo digital no Brasil ao longo do seu desenvolvimento.

Tem-se como prova a administração pública frequentemente adequando-se às demandas técnicas de seus usuários em períodos específicos. Como na busca em aproximar o Estado de uma população autônoma que utiliza uma estrutura que faz mais que digitalizar processos. Assim como na transformação *mobile* e na emergência do *smart government* orientado a dados em prol de uma cidade mais sustentável com qualidade de vida para a população.

Figura 1 - Composição do governo digital no Brasil

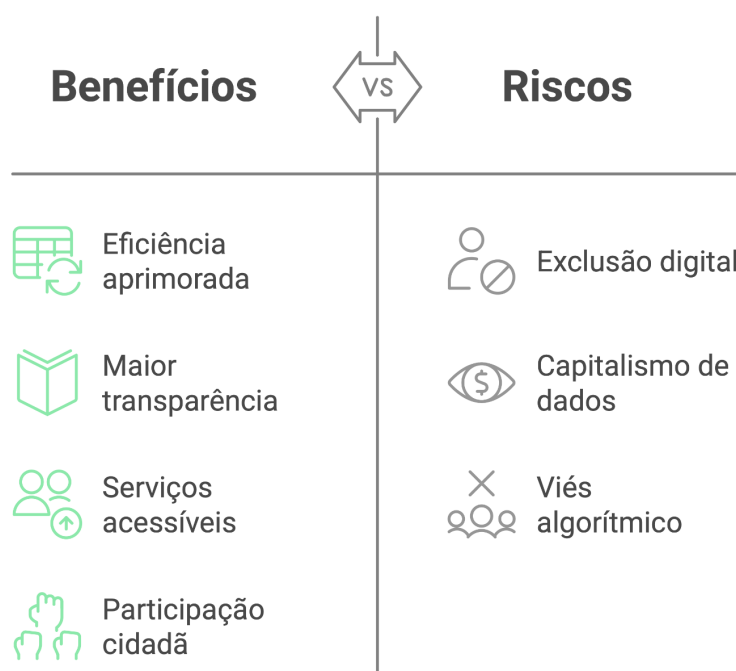


Fonte: a autora, 2025.

Considerando o presente cenário sócio-tecnológico, é notório a importância do governo digital para relação do Estado com os cidadãos. Tendo-o como um braço

mais presente, que garanta acesso a políticas públicas livres de fronteiras em todo o território nacional. Assim, é necessário avaliar suas falhas e reduzir danos que impactem seu objetivo em relação aos cidadãos. Ou seja, é uma estrutura que possui seus riscos e benefícios, conforme figura 2.

Figura 2 - Benefícios e riscos da estrutura governo digital



Fonte: elaborado pela autora, 2025.

Neste levantamento teórico o tratamento dado à privacidade no *e-government* surge como um ponto de atenção. O que foi descrito até aqui ressalta como as ações relacionadas à privacidade e proteção de dados demandam a inclusão e a participação de cidadãos nos processos em que está envolvida. O que, por sua vez, demonstra a necessidade de metodologias que cumpram tais propósitos de forma plural e centrada nesses indivíduos. É a partir de perspectivas do Design, a serem relacionadas no capítulo a seguir.

3 A PRIVACIDADE RELACIONADA A ABORDAGENS DO DESIGN

O objetivo deste capítulo é interseccionar conceitos de design e ergonomia à privacidade, ao consentimento, à proteção de dados pessoais e ao governo digital, e identificar suas contribuições para orientar a comunicação relacionadas a essas questões. Assim como também apresentar as abordagens: privacidade por projeto e linguagem simples que podem servir como aliadas aos conceitos de design.

É sabido como as transformações da era da informação alteraram dinâmicas de interação. Isso reflete na formação do governo digital, como visto no capítulo anterior. Compreende-se que tais atividades são movidas a dados. Assim como impõem sua proliferação, e podem apresentar riscos à privacidade dos indivíduos.

Isso é próprio do mundo complexo em que a humanidade se encontra. Nele, a tecnologia está repleta de elementos, camadas e estruturas. Seu funcionamento é constantemente redefinido pelas inter-relações que tem-se com eles (Cardoso, 2012), ou seja, pelas interações.

Dessa forma, contemporaneamente, a intenção é que essas tecnologias sejam encaminhadas para atender as necessidades de quem as utiliza. Para isso, são necessárias, entre outros fatores, interfaces que permitam um fluxo pleno em relação ao desejado, transmitindo mensagens compreensíveis e eficazes (Cardoso, 2012).

Nesta pesquisa, abordam-se aquelas que envolvem o consentimento à coleta de dados e a concordância com as políticas de privacidade. Portanto, neste capítulo são trazidos conceitos de design e ergonomia por entender sua função na busca por melhorar experiências dos indivíduos, ao considerar seus desejos e características.

A primeira seção deste capítulo é destinada aos conceitos Interação humano-computador (HCI), Design centrado no usuário (UCD), Design centrado no humano (HCD), Design de interação (IxD), Usabilidade e Design de experiência do usuário (UXD). Dessa forma, a pretensão é explanar suas contribuições e como podem ser relacionadas às experiências dos cidadãos em relação às questões de privacidade.

Na segunda seção são abordados o conceito Privacidade por projeto, ou *privacy by design*. Já na terceira seção, o conceito de Linguagem cidadã. A finalidade é constituir um referencial teórico com as discussões do design e identificar como priorizar o usuário, sua proteção e experiência.

3.1 Contribuições do Design

Com a popularização da internet, nomes próprios foram convertidos em *usernames* que, por sua vez, se tornaram uma identidade on-line. Por meio deles pode-se navegar anonimamente pelas comunidades do ciberespaço. Os dados não eram amplamente disponibilizados, o que aumentava a dificuldade em identificar uma pessoa na internet.

Para McNeil (2020), trocar uma marca única e individual humana - o nome - foi o que indicou a mudança de visualização do 'indivíduo ser' para o 'indivíduo usuário' no mundo digital. De acordo com Lialina (2012; 2021, p. 17) “os usuários eram vistos e comercializados como pessoas cujos trabalhos, sentimentos, pensamentos, interesses, talentos - tudo o que importa - estavam fora de sua interação com computadores pessoais”.

Mas então, disciplinas relacionadas à ergonomia e ao design de pronto preocuparam-se em debruçar-se sobre as interações que esse usuário desenvolvia com as máquinas (Morais; Loper, 2014) agora na sociedade em rede (Castells, 1996). Para isso, são considerados os objetivos da ergonomia, que busca facilitar as tarefas do homem por meio de máquinas amigáveis de acordo com suas capacidades e limites, e do design, que intenta que essas sejam atrativas e funcionais (Moraes, 2013).

Para Lialina (2018; 2021) o propósito original dos computadores, que popularizaram a interação dos usuários com a rede, não era simplificar a vida, mas a simbiose homem-computador. O objetivo era “garantir uma ótima compatibilidade ergonômica dos componentes do sistema com as metas globais” (*ib.*, p. 101).

A partir daqui serão tratadas áreas que se relacionam à ergonomia e ao design para melhorar a relação do indivíduo com o sistema. A proposta é contribuir para experiências mais positivas por meio das ideias absorvidas das revisões de literatura.

3.1.1 Interação humano-computador (HCI)

O mundo moderno é centrado em dados que se tornaram mercadoria. A forma como as empresas coletam, processam e usam esses dados não são facilmente vistas ou compreendidas pelos usuários. Dessa forma, deveriam ser um

ponto de atenção para as áreas de HCI e Experiência do usuário (UX) (Bowyer *et al.*, 2022).

A interação humano-computador, que trata de uma comunicação efetiva entre os seres humanos e os computadores, também visa a satisfação dos usuários no contato com a interface (Agner, 2009). Para a HCI o objetivo é que o acesso aos sistemas seja rápido, com disponibilidade ininterrupta, cada vez mais adaptado ao ser humano (Morais; Loper, 2014). Além disso, um fator de suma importância é que, na perspectiva da HCI, o ser humano consiga depositar sua confiança no sistema (Oliveira; Oliveira, 2015).

A HCI se preocupa que a usabilidade da interface seja adequada, mas não necessariamente esteticamente mais precisa. Entretanto, o estilo da interface é capaz de determinar o quão agradável é a interação do indivíduo com ela. Dessa forma, se isso significar menor esforço ao desempenho dos usuários, mais amigável lhes parecerá o sistema (Rogers *et al.*, 2005).

Quando se relaciona a HCI à privacidade, a área encontra contextos desafiadores. Um deles é adequar a urgência em explorar e aplicar tecnologias para proteção à privacidade. Além de estar em conformidade às leis, em prol da transparência e responsabilidade na promoção da confiança dos cidadãos.

Para Krebs *et al.* (2019), tais tecnologias "devem ser projetadas para implementar e promover efetivamente os direitos e obrigações de proteção de dados". Ainda que complexo, os autores pontuam como a área é capaz de proporcionar uma abordagem verdadeiramente interdisciplinar. Inclusive, indo além das ciências legais.

As técnicas da Interação humano-computador foram idealizadas para tornar artefatos, anteriormente difíceis de usar, mais fáceis de entender e interagir. Elas se aplicam tanto para usuários especialistas quanto para os mais novos e inexperientes (Johansen *et al.*, 2021). Pensar nelas, aponta um caminho para descomplicar a relação de variados perfis de usuários com questões relativas à privacidade nas interfaces do governo digital.

3.1.2 Design centrado no usuário (UCD), no humano (HCD) e na humanidade

As correntes Design centrado no usuário e Design centrado no humano surgem com a necessidade de priorizar quem faz uso de um produto ou serviço. Isso

faz desse indivíduo o centro do processo de design. No UCD, os esforços de projeto focam os usuários e suas necessidades em todas as fases do processo de design, que é iterativo.

Dessa forma, esses usuários são envolvidos e participam do trabalho. Eles fornecem avaliações e feedbacks que orientam a criação de produtos e soluções eficazes e eficientes (Chammas *et al.*, 2015; Norman, 2018; Schlemmer; Padovani, 2021). Ou seja, centrar no usuário significa integrá-lo o máximo possível (Agner, 2023).

Para tal, de acordo com Agner (2023), é necessário que haja uma pesquisa adequada acerca dos usuários. Além disso, considerar a usabilidade e a amigabilidade é primordial nesse procedimento. E que os requisitos estabelecidos no projeto dos produtos considerem a incorporação desses usuários.

Com o tempo, o termo cunhado por Norman (UCD) passou por uma transformação. A palavra usuário foi substituída por humano. Essa mudança buscou humanizar os indivíduos, suas necessidades, experiências e contextos (Norman, 2023).

Giacomin (2014) explica que o Design Centrado no Humano possui raízes na ergonomia, nas ciências da computação e na inteligência artificial. De acordo com ele,

o Design centrado no humano é baseado na aplicação de técnicas de comunicação, interação, empatia e estímulos à participação dos envolvidos para entender suas necessidades, desejos e experiências, que por vezes transcendem o que as próprias pessoas são capazes de perceber (*ib.*).

Assim sendo, a escolha do termo humano se deve à intenção de abarcar as diversidades de interesses dos envolvidos. O que o mostra mais alinhado às pessoas para quem o produto se destina do que outras práticas tradicionais do design. As ferramentas do HCD orientam suas práticas de design por meio de abordagens criativas.

Essas abordagens incentivam pessoas a imaginar futuros possíveis. A partir da experimentação de produtos, sistemas e serviços para criar perspectivas e opiniões pessoais (Giacomin, 2014). Efetivamente, na perspectiva centrada no humano, os produtos, sistemas e serviços são mais intuitivos.

Para entender o HCD, quatro princípios básicos (Norman, 2023) são dispostos para materializá-lo:

- Ir até a raiz dos problemas, não apenas o que é apresentado, que muitas vezes é um sintoma;
- Focar nas pessoas;
- Ter o ponto de vista do sistema, percebendo como a maioria das complicações resulta de interdependências de diversas partes;
- Testagem contínua e refinamento do design proposto para assegurar que atende às necessidades e preocupações das pessoas para as quais foi projetado.

O conceito HCD também passou por uma modificação. A fim de abarcar as especificidades do século XIX e os desafios do design nesta época, Norman propõe uma alteração em prol do termo humanidade. Agora o objetivo é considerar todas as formas de vida, o ecossistema natural, as comunidades e o seu papel (Norman, 2023) naquilo já conhecido pela relação com design difuso, como proposto por Manzini (2017).

Dessa forma, Norman (2023) revisita os princípios que estabeleceu para o HCD, remodelando-o para a proposta do Design Centrado na Humanidade. Assim, eles caracterizam-se por:

- Ir até a raiz dos problemas, não apenas o que é apresentado, que muitas vezes é um sintoma;
- Focar como um todo no ecossistema de pessoas, todas as coisas vivas e o ambiente físico;
- Ter o ponto de vista do sistema a longo prazo, percebendo como a maioria das complicações resulta de interdependências de diversas partes, considerando que as implicações mais prejudiciais à sociedade e à ecoestrutura só serão reveladas depois de anos ou décadas;
- Testagem contínua e refinamento do design proposto para assegurar que atende às necessidades e preocupações das pessoas para as quais foi projetado;
- Fazer design com a comunidade, tanto quanto apoiar suas formas de design, devendo os designers profissionais atuarem como facilitadores, fontes, ajudando a comunidade a atender suas necessidades.

Entretanto, para Lialina (2012; 2021), essa visão faz sentido apenas dentro do design de interfaces. Para ela, renegar a palavra usuário, em favor de pessoas ou

humanos, pode ser perigoso. Uma vez que o termo usuário seria o lembrete remanescente de que a interação acontece com um programa ou um computador, seja ele visível, ou não.

Isso implica na subtração da diferença que há entre os desenvolvedores e projetistas e os usuários. Além dessa possibilidade ocasionar perda de direitos e oportunidades de proteção dos usuários. Tais como reclamar por melhores softwares, consentir, deletar suas informações e ver a interface.

Na visão da teórica (Lialina, 2012; 2021), mais positiva sobre a adoção de termo *user*, todos podem ser usuários universais. Ou, *turing complete users*¹². Ainda que existam diferentes níveis de expertise entre cada um. Esses, são aqueles que conseguem alcançar seus objetivos independente do objetivo principal do artefato.

Ela cunhou o termo “*turing complete users*” para explicar que, disponibilizados tempo e respeito suficientes ao indivíduo, não há tarefa feita por um usuário que outro não consiga cumprir. Além disso, eles devem ser conscientizados sobre o que significa ser um usuário. Pois, eles são “fruto de culturas tecnológicas que os impulsionaram a se desenvolverem, ajustarem, improvisarem e controlarem as suas tarefas” (Lialina, 2012; 2021, p. 27).

O usuário tratado aqui, agente da interface e das experiências é aquele cunhado por Norman. O usuário no qual os projetos e o design devem ser centrados. O mesmo que, posteriormente, foi renomeado para humano e está sendo chamado por outros de humanidade (Gorichanaz, 2024; Norman, 2023).

É este indivíduo que a usabilidade atende. Para quem os *sítes*, aplicativos, plataformas e forma de usar devem ser fáceis e compreensíveis. Principalmente se envolvem seu direito à privacidade, coleta de dados pessoais e consentimento.

No UCD, para Grafenstein *et al.* (2022), usuários são a fonte primária de pesquisa para entender as necessidades no design do sistema, por isso

uma abordagem centrada no usuário para a proteção de dados é adequada para projetar especificações viáveis que possam incorporar a conformidade legal, a margem de manobra organizacional para a inovação e a transparência sobre as consequências para os titulares dos dados (*ib.*).

A disciplina Design pode contribuir com a transparência digital no governo. Com ela, é possível que erros sejam evitados e abusos de poder revelados.

¹² A autora defende o uso dos termos *Universal Users* e *Turing Complete Users* ao invés dos *General-purpose users*.

Matheus *et al.* (2021) propõem 16 princípios de design que podem ser utilizados como guia.

Considera-se o quinto princípio, que indica evitar jargões ou termos desconhecidos pelo público. E o sétimo princípio, relacionado a características técnicas como uma UI (*user interface*) bem projetada e uma boa UX (*user experience*). Eles correspondem ao que esperam os usuários regulares em relação a facilidade para navegar ao utilizarem o sistema.

Contudo, optar por uma abordagem centrada no usuário ou no humano é a certeza de que o cidadão, o principal favorecido pelo respeito ao direito da privacidade, será considerado e envolvido no processo. O Design, para criar *frameworks* ou *guidelines*, parece a melhor oportunidade de promover a adequação à legislação. Mas não se restringir a isso, deve considerar a experiência do usuário assim como a adaptabilidade ao seu contexto e necessidades (Krebs *et al.*, 2019).

3.1.3 Design de interação (IxD)

De acordo com Rogers *et al.* (2005), o design de interação se preocupa em trazer a usabilidade para dentro do processo de design. Há também a consideração à perspectiva do usuário. Por meio dele, são criadas experiências que melhoram e ampliam a interação, comunicação e trabalho humano com artefatos projetados.

Para os autores, ele consiste em quatro atividades: 1. Estabelecer requisitos; 2. Criar alternativas de design; 3. Prototipar; 4. Avaliar. Essa disciplina teve origem na HCI e durante as primeira e segunda ondas da disciplina, era a engenharia das interfaces para a usabilidade e utilidade.

Com o passar dos anos, os artefatos foram miniaturizados. A capacidade de sistemas aumentaram consideravelmente. Eles se conectaram, provendo um campo de materiais híbridos, físicos e digitais. O que aumentou o complexo fluxo em que os serviços são interlinkados (Höök; Löwgren, 2021).

A ideia é que os artefatos alvos do design de interação sejam uma representação do conhecimento que as pessoas têm do mundo físico. Ou, do dia a dia delas. O projeto, segundo o design de interação, precisa otimizar interações que se modificam e expandem.

As escolhas também devem ser guiadas baseadas em uma maior compreensão acerca dos usuários. Ou seja, é necessário pensar o que qualifica a

experiência dos usuários. Para isso é preciso conhecer seus desejos e envolvê-los no processo de design (Rogers *et al.*, 2005).

Para Höök e Löwgren (2021), o design de interação funciona “tentando atingir um alvo em movimento”. Isso porque ela é uma disciplina relativamente nova do design. Uma vez que envolve materiais digitais que estão em constante evolução técnica e tecnológica.

Além disso, para os autores, ela providencia resultados significativos em tecnologias interativas. Essas últimas que surgem e ressignificam ou interrompem hábitos e processos sociais (Höök e Löwgren, 2021). O objetivo da disciplina hoje é projetar interfaces em prol das experiências e com significado.

Avaliar é fundamental para o design de interação. Para isso é utilizada uma abordagem centrada no usuário, na qual ele é envolvido em todo o processo. São aplicadas técnicas como entrevistas, teste de desempenho e execução de tarefas, respostas a questionários e sua participação como co-designers.

De acordo com Rogers *et al.* (2025, p. 35), as descobertas são interpretadas para entender como as pessoas realizam as tarefas. Pois, os usuários têm necessidades distintas que por sua vez devem orientar cada projeto. Ainda segundo os autores, o IxD deve ser composto de três características-chave do processo de interação:

- “os usuários devem estar envolvidos no desenvolvimento do projeto”;
- “a usabilidade específica e as metas decorrentes da experiência do usuário devem ser identificadas, claramente documentadas e acordadas no início do projeto”;
- a iteração é inevitável nas quatro atividades¹³ que constituem o IxD.

Antes o design de interação tinha como função ajudar os usuários. Seu escopo alcançava atividades de relações pessoais e sociais, manutenção da boa forma. E até mesmo na melhora da produtividade no trabalho e redução do consumo de energia.

¹³ “1. Identificar necessidades e estabelecer requisitos; 2. Desenvolver designs alternativos que preencham esses requisitos; 3. Construir versões interativas dos designs, de maneira que possam ser comunicados e analisados; 4. Avaliar o que está sendo construído durante o processo” (Rogers *et al.*, 2005, p.33)

Hoje o design de interação é atravessado por técnicas que são usadas para enganar os usuários. Como no uso generalizado de *dark patterns*¹⁴ pelos designers de interação. O que representa uma crescente preocupação para a área (Rogers *et al.*, 2020)

Do ponto de vista do design de interação, os dados dos usuários também são uma ferramenta valiosa de *feedback* para os serviços. Eles podem fornecer funções personalizadas e adaptáveis (Höök; Löwgren, 2021). Entretanto, a coleta dos dados está envolta em formas de persuasão projetadas nas interfaces para induzir usuários a fazer coisas que não pretendiam.

Os padrões obscuros induzem o consentimento e à negligência à privacidade. Dessa forma, eles aparecem como uma adição enganosa e desonesta à experiência dos usuários. Além de se tornarem “uma parte integrante da forma como os dados dos usuários são coletados” (Rogers *et al.*, 2020) devido ao valor comercial envolvido.

Nesta perspectiva, o design de interação não só pode, como deve ajudar a conscientizar os cidadãos. Johansen *et al.* (2021) pontuam que os designers de interação tem participação fundamental nisso. Pois podem ajudar a implementar, de modo mais fácil, o que está nas políticas de privacidade e nas regulamentações nos artefatos tecnológicos, em apoio aos advogados e programadores.

3.1.4 Usabilidade

A inclusão digital buscada pelo *e-gov* entende que os seus *sites*, plataformas e aplicativos devem ser fáceis de usar. Derrubando, assim, as barreiras originadas da falta de conhecimento e de experiência de uso (Agner, 2009). Isso significa que esses sistemas devem ser usáveis, ou ter uma usabilidade apropriada.

De acordo com Moraes (2013), “a usabilidade trata de adequação entre o produto e as tarefas a cujo desempenho ele se destina, da adequação com o usuário que utilizará, e da adequação ao contexto em que será usado”. Ela é, portanto, um objetivo específico e fundamental ao design. Consequentemente, é necessário avaliá-la em um processo que seja holístico e interativo para verificar a integração entre usabilidade e as necessidades do usuário.

¹⁴ Padrões obscuros: abordagem eticamente dúbia para influenciar usuários a tomar determinadas decisões.

Rogers *et al.* (2005) pontuam que a usabilidade considera onde e quem utilizará o produto ou design. E também quais atividades simultâneas as pessoas realizam quando interagem com o produto.

Dentro do Ergodesign, área que integra objetivos e conceitos da ergonomia e do design, as interfaces de sistemas tecnológicos são fundamentalmente consideradas. Nele, Agner (2009) explica que é importante entender qual o seu grau de dificuldade e facilidade de uso assim como um projeto centrado no usuário. Ou seja, preocupar-se com as necessidades dos usuários, mantém o foco na usabilidade.

Agner (2009), postula a usabilidade como uma ideologia cujos princípios relacionam-se com direitos inalienáveis dos homens, como o de (1) ser superior a tecnologia; (2) ao empoderamento; (3) à simplicidade; e (4) ter seu tempo respeitado. Para ele (2023) usar com facilidade não é suficiente, é preciso certificar-se que o uso evoca respostas emocionais e positivas dos indivíduos.

Para que a usabilidade seja de fato adequada é necessário que ela cumpra as metas: ser eficaz; ser eficiente; ser segura; ser útil; ser fácil de aprender; ser fácil de lembrar como usar (Rogers *et al.*, 2005). Além disso, obedecer também aos princípios (ou heurísticas, quando avaliados) (Nielsen, 1990; Rogers *et al.*, 2005):

- visibilidade do status do sistema;
- compatibilidade do sistema com o mundo real;
- controle do usuário e liberdade;
- consistência e padrões;
- ajuda os usuários a reconhecer, diagnosticar e recuperar-se de erros;
- prevenção de erros;
- reconhecimento em vez de memorização;
- flexibilidade e eficiência de uso;
- estética e design minimalista;
- ajuda e documentação.

Para tratar da usabilidade em relação à privacidade abordam-se aqui os *cookies*. Esses arquivos são utilizados para coletar informações dos usuários, pois permitem que os *sites* melhorem sua usabilidade e experiência ao traçar e reconhecer seus padrões e comportamentos de navegação. Além de poderem ser

utilizados em diferentes atividades ou propósitos, como na publicidade direcionada (Alharbi *et al.*, 2023).

As formas usuais de interação com os *cookies* são *banners* ou janelas de diálogo *pop-up* que aparecem na primeira visita do usuário a um *site*. Eles informam sobre a coleta de dados e se os usuários consentem àquelas práticas. Entretanto, as formas que eles são projetados parecem, na verdade, estimular o consentimento dos usuários a escolhas específicas (Machuletz; Böhme, 2020).

Essas interfaces estão sendo projetadas utilizando *dark patterns* que induzem os usuários a tomarem decisões que favorecem *sites* e provedores. Entre os 243 *sites* governamentais pesquisados por Alharbi *et al.* (2023), mais de 90% das interfaces dos cookies apresentam esses padrões.

Alguns tipos de *dark patterns* identificados são escolhas pré-selecionadas (figura 3), configuradas por padrão antes que o usuário possa tomar uma decisão. Outros são botões destacados por padrão, esteticamente projetados para captação da atenção do usuário em função de uma opção específica (figura 4), manipulando os caminhos da escolha de forma desigual (Alharbi *et al.*, 2023).

Figura 3 - Exemplo de escolhas pré-selecionadas

Our site uses cookies ×

What is a cookie ? What cookies do we use and why? Read more in our [cookie policy](#).

Accept optional cookies Decline optional cookies

ESSENTIAL (ALWAYS REQUIRED)
These cookies are necessary for purely technical reasons for a normal visit to the website. Given the technical necessity, only an information obligation applies, and these cookies are placed as soon as you access the website.
Purpose: basic service
ENABLED

FUNCTIONAL (ALWAYS REQUIRED)
You cannot refuse these cookies if you wish to browse this website, but they are only placed after a choice has been made regarding the placement of cookies.
Purpose: basic service
ENABLED

MATOMO
These are cookies that allow us to know how many times a specific page has been visited. We only use this information to improve the content of our website. These cookies are only placed if you accept their placement.
Purpose: Statistics
DISABLED

Confirm my choice

Fonte: Alharbi *et al.*, 2023.

Figura 4 - Exemplo de destaque em opção específica

Utilizamos cookies no Portal da SPMS para lhe fornecermos a melhor experiência de navegação. Ao clicar em "Aceitar Todos", permitirá que sejam usados todos os cookies. Contudo, poderá visitar as "Definições de Cookies" para configurar o seu consentimento de forma controlada.

Definições de Cookies

Aceitar Todos

Fonte: Alharbi *et al.*, 2023.

Há também avisos legais que não oferecem escolhas ao trazer as políticas de privacidade. Os que descrevem o uso dos *cookies* ao invés de oferecer opções sobre eles aos usuários. Além de barreiras de consentimento impedindo o uso pleno do *site* a não ser que o usuário consinta com o uso dos *cookies* (Alharbi *et al.*, 2023).

Machuletz e Böhme (2020) observaram elementos comuns ao design dos *pop-ups* e caixas de diálogo, antes de acessar o *site*. São eles os botões para selecionar tudo e as *checkboxes*¹⁵. As últimas servem para confirmar variados procedimentos de processamento de dados.

Assim como fizeram Alharbi *et al.* (2023), Machuletz e Böhme (2020) identificaram características que comprometem a usabilidade. Primeiro, o botão em destaque aceita automaticamente todos os propósitos, sem esperar pela ação de selecionar, ou não, outra opção de *checkbox*. Dessa forma, esse tipo de botão não melhora as opções dos usuários, mas os dissuade a aceitar tudo sem ter escolhido tudo de forma ativa.

Os usuários aceitam tipos de coleta de dados quando as caixas de diálogo de consentimento são integradas ou destacadas para selecionar tudo de uma única vez. Para Machuletz e Böhme (2020), há um padrão moralmente dúbio. Nele, os usuários seriam induzidos a consentir contra suas próprias intenções.

Isso fica explícito no pesar dos usuários. Quando informados na íntegra sobre os propósitos, eles tendem a se arrepender das próprias decisões (Machuletz; Böhme, 2020). Entretanto, opções de design podem contornar o problema, melhorar a usabilidade das interfaces de *cookies* e a experiência dos usuários (Alharbi *et al.*, 2023).

Dessa forma, é necessário que os projetistas criem interfaces *user-friendly*. Elas permitem aos usuários "compreender e escolher quais dados e com quem eles querem compartilhar" (Bartali; Velsen, 2023). Uma vez que isso fortalece a confiança no serviço, algo que apenas um sistema fácil de usar, projetado para a privacidade proporciona (*ib.*).

¹⁵ Caixas utilizadas para marcar a opção desejada entre outras disponíveis.

Para Johansen *et al.* (2021) é importante ter uma abordagem multidisciplinar a respeito da privacidade. Eles desdobram diferentes perspectivas para avaliá-la. Entre essas, a da usabilidade e da ergonomia, focada nas pessoas, sua facilidade de compreender por completo as tarefas, considerando seus contextos.

Os autores propõem a adoção de *privacy labels* (selos de privacidade), que são um rótulo “vinculado juridicamente que contém informações sobre a privacidade que um produto ou serviço fornece” (*ib.*, 2021). Esses rótulos podem ser físicos ou digitais. Eles são definidos e apresentados visualmente e permitem ter uma visão geral de informações simples e complexas. O que facilita a comparação entre produtos diferentes em função dos critérios mais relevantes para cada usuário (*ib.*).

O que Johansen *et al.* (2021) defendem a partir desses rótulos é que eles possam ser utilizados por diferentes tipos de usuários. Especialmente usuários leigos. Para isso é necessário que os aspectos de usabilidade sejam igualmente incluídos na avaliação da privacidade.

Não apenas isso, mas também de segurança. Pois as violações de segurança ainda ocorrem porque a usabilidade das interfaces não são adequadas e induzem os usuários a erros. Este cenário é o reflexo da privacidade que é definida como tarefa secundária.

Ao comprar passagens de trem com um aplicativo de passagens, o principal objetivo do usuário não é verificar o quão bem o aplicativo protege sua privacidade, mas chegar a um determinado destino. Além disso, é difícil para uma pessoa comum acompanhar todos os dados digitais que ela está gerando, já que muitas atividades hoje em dia acontecem on-line (Johansen *et al.*, 2021).

As leis apresentam objetivos de usabilidade que são normalmente muito gerais. Isso abre precedente para diferentes interpretações subjetivas que atendam aos interesses dos administradores. Por isso, a usabilidade é ainda mais importante para a privacidade.

Entretanto, a usabilidade não importa apenas porque “a privacidade é um conceito altamente complexo, relacionado a tecnologias complexas, como IA e *Big Data*” (Johansen *et al.*, 2021). Ela é importante por considerar os tipos diferentes de usuários, dos especialistas aos não especialistas.

3.1.5 Experiência do usuário (UX)

De acordo com Kuang e Fabricant (2022), a experiência do usuário (*user experience*; UX) é, como nunca antes, o centro da vida moderna. É o que orienta a

presença de todos no ambiente digital. Segundo os autores, as pessoas hoje esperam que as ferramentas sejam fáceis e simples de usar como um jogo *mobile* para crianças.

Isso significa, ferramentas que sejam usadas tanto para o diagnóstico de doenças graves quanto para o de problemas de engenharia. Lialina (2014; 2021) pontua que a popularização do termo nos anos recentes causou a sua perda de sentido. Ainda assim, continua-se a compreender a UX como um processo do projeto de um produto que vai alcançar as necessidades do usuário.

Para Agner (2023) a experiência do usuário adiciona novos critérios a usabilidade, como emoção, credibilidade da marca, desejo, estética, performance e segurança. Quando o design é adicionado ao UX a ideia é que a experiência do indivíduo seja relevante e significativa. Ou seja, que faça a diferença na vida das pessoas.

A *User Experience*, segundo Rogers *et al.* (2005), trata dos sentimentos dos usuários em relação ao produto. Assim como da sua satisfação e prazer em utilizá-lo, “olhá-lo, abri-lo ou fechá-lo” (*ib.*, p. 13). Dessa forma, na UX serão refletidas impressões sobre o quão bom é uso.

Nela são consideradas minúcias, como os efeitos aos sentidos. Uma vez que eles consideram o uso do produto no mundo real. Para os autores, os aspectos de experiência do usuário mais importantes a serem considerados são: a usabilidade; a funcionalidade; a estética; o conteúdo; o *look and feel* e os apelos sensoriais e emocionais (*ib.*).

Além disso, a experiência do usuário também dispõe de metas que querem saber como os usuários experimentam os produtos e como esse se sentiu ao interagir com o sistema. Rogers *et al.* (2005) os classificam como: satisfatórios; agradáveis; divertidos; interessantes; úteis; motivadores; esteticamente apreciáveis; incentivadores de criatividade; compensadores; e emocionalmente adequados.

Antes dos impactos tecnológicos já discutidos neste trabalho, ao utilizar plataformas digitais não haviam grandes dilemas éticos para os usuários, afirma McNeil (2020). A princípio, eles eram apenas navegantes da internet.

Tinham a opção de se apresentar em três espectros: privado ou público; anônimo ou nomeado; factual ou faz de conta, pontua a autora. Isso, de certa forma,

atrasou em algum tempo as preocupações a respeito do consentimento, privacidade e identidade dos usuários.

Hoje em dia, a experiência que é vivida em produtos digitais e on-line tende a ser reduzida a uma moeda que vale pouco. Mas não deveria. Os usuários precisam ser orientados em relação ao consentimento e privacidade e precisam disso na forma de *feedbacks* e *guidelines* que não visem lucro (McNeil, 2020).

De acordo com Grafenstein *et al.* (2022), focar na avaliação da efetividade do design de interface do usuário e no campo de pesquisa de design de experiência do usuário pode oferecer muito. Para eles, métodos além das ciências legais podem ser melhores em avaliar se a implementação das medidas de proteção são efetivas e cumprem o que dizem as leis. Além disso, a UX tem uma história de longa data com a avaliação de fatores como efetividade, transparência e controlabilidade.

Projetar a experiência do usuário, para esses autores, é atividade interdisciplinar, não ideológica. Também é pragmaticamente metodológica, devido ao seu uso de métodos quantitativos. Ou seja, combina diferentes pontos de vista e a expertise de diferentes agentes de interesse nas soluções de design.

Tais métodos objetivam sistemas e processos que atendam a necessidades universais dos usuários. Projetar a experiência do consentimento e permissão do usuário envolve desenvolver interfaces de privacidade amigáveis, transparência e garantia do controle do usuário (Chalhoub *et al.*, 2023).

3.2 Privacidade pelo projeto (*Privacy by design*)

Privacy by design é um conceito desenvolvido por Ann Cavoukian, quando era comissária de informação e privacidade da província de Ontário, no Canadá. Ele pode ser entendido como privacidade pelo projeto ou privacidade desde a concepção. Em 2009, ela postulou os 7 princípios (quadro 2) que deveriam orientar qualquer projeto que considerasse o respeito e a preservação da privacidade dos usuários.

Quadro 2 - Princípios do privacy by design

7 PRINCÍPIOS DE <i>PRIVACY BY DESIGN</i>
1 Proatividade, não reatividade; prevenir e não remediar
2 Privacidade por padrão
3 Privacidade incorporada no design

- 4 Funcionalidade completa
- 5 Segurança de ponta a ponta, proteção durante todo o ciclo
- 6 Visibilidade e transparência
- 7 Respeito a privacidade do usuário

Fonte: traduzido pela autora, com base em Cavoukian (2009), 2025.

O conceito indica que a privacidade deve ser pensada desde o princípio. Ou seja, não deve ser adicionada posteriormente como uma solução a problemas identificados nos sistemas no decorrer do processo. Com essa abordagem, o objetivo é a proteção aos dados pessoais dos usuários no desenvolvimento de produtos e serviços digitais. Isso em todas as etapas do projeto (Cavoukian, 2009).

De acordo com Bartali e Velsen (2023), em seu corpo de pesquisa, um princípio possível de aplicar na parte visual do projeto é o 'Respeito à privacidade do usuário'. Isso porque consiste em manter os interesses do indivíduo em primeiro lugar. O que implica na solicitação permanente do consentimento dos usuários na coleta, uso e compartilhamento de dados pessoais.

Além de considerar que os indivíduos devem sempre ter acesso aos próprios dados e alterá-los quando e se assim desejarem. Dessa forma, o visual das opções de compartilhamento de dados devem ser intuitivas para os usuários. Assim, eles não encontrarão dificuldades para confirmar o consentimento e utilizar os serviços. Para Bartali e Velsen (2023), as pessoas se preocupam menos com a privacidade quando confiam no sistema.

Bartali e Velsen (2023) conduziram uma pesquisa sobre o design de opções de compartilhamento de dados para intervenções *eHealth*. Os participantes disseram que 1. gostariam de ter a opção de selecionar não compartilhar nenhum dado com ninguém; 2. não foi explicitamente declarado que se pode escolher não compartilhar dados.

Outros mostraram-se preocupados com a falta de informações sobre como os dados coletados seriam utilizados. Assim como com a possível divulgação das suas informações pessoais na internet e o armazenamento delas por diferentes agentes interessados.

Diante dos benefícios que o compartilhamento de dados em serviços *eHealth* pode trazer, identificados na pesquisa, Bartali e Velsen (2023), consideram importante a inclusão de características do *privacy by design* para diminuir o nível de

preocupações com a privacidade e consequentemente aumentar os níveis de confiança e controles dos usuários.

Grafenstein *et al.* (2022) argumentam em prol de uma proteção de dados por projeto (*by design*), ou seja, não resumido apenas ao nível tecnológico da segurança de dados, mas durante todo o processo e operações do projeto. Alharbi *et al.* (2023) abordam o conceito de *usable privacy*¹⁶ em que o design de interfaces de privacidade precisa que elas sejam úteis para que o usuário possa ser hábil encontrando, compreendendo e tendo controle sobre as informações.

Para os autores, “o principal foco do *privacy by design* é que a privacidade e as medidas de proteção de dados devem ser operadas em um produto desde a sua fase inicial de projeção até o desenvolvimento, uso e descarte final” (*ib.*). Para isso, devem ser implementados meios e processos que cubram todos os estágios. Ao passo que o objetivo do conceito é proteger os usuários e garantir-lhes controle sobre as próprias informações, ele é capaz de, simultaneamente, garantir segurança.

Segundo Alharbi *et al.* (2023), os designers deveriam guiar-se pelos princípios de *privacy by design* para criar interfaces de privacidade úteis e utilizáveis. O que, por sua vez, permite interações efetivas aos usuários. Além disso, devem considerar as necessidades dos usuários, apoiar suas escolhas e permitir que as tomem de forma consciente e informada.

Para tal, “precisam compreender os fatores que influenciam a *usable privacy*, particularmente na internet, assim como os projetos devem ser compatíveis com as regulamentações e leis e seguir os princípios estabelecidos” (*ib.*).

Para Cordeiro *et al.* (2020), é necessário que os designers que trabalham com captura de dados compreendam que decisões possuem resultados. E como precisam respeitar a privacidade dos usuários. De acordo com as autoras, ao considerar o design, a mudança social está relacionada à participação do cidadão no seu processo. Assim, o papel do designer é mais de facilitador e mediador do diálogo entre atores sociais variados.

Para Aylo e Toch (2021), a maior contribuição do design centrado no usuário ao *privacy by design* é de fato incluir os usuários nas diferentes etapas. Uma vez que os feedbacks serão completamente diferentes dos projetistas que já tem uma

¹⁶ Em *usable privacy*, as *privacy interfaces* são projetadas para serem úteis (*useful*) e utilizáveis (*usable*) obedecendo aos princípios transparência, legibilidade, relevância, escolha e agenciamento.

visão influenciada pelas suas habilidades. Assim, diferentes percepções, contextos e origens podem contribuir verdadeiramente para avaliações apropriadas e na redução dos riscos à privacidade.

3.3 Linguagem cidadã

Com o objetivo de melhorar o acesso de todos a textos oficiais, começa a ser disseminado a *plain language*, ou linguagem simples, um estilo de escrita que surge com o objetivo de melhorar o acesso de todos com uma linguagem fácil de ler. No país, as informações escritas relacionadas ao governo e à legislação ainda carregam essência jurídica e, por consequência, excludente.

Para Pires (2021), o estilo da escrita burocrática é marcado por estrutura sintática complexa, vocabulário pouco familiar e alta carga informacional. Ou seja, impactam na compreensão plena de usuários comuns. Ainda assim, vocabulário jurídico e termos específicos estão presentes em boa parte das plataformas, *sites* e aplicativos utilizados no território nacional.

Mesmo não sendo familiares para parte da população brasileira, são apresentados a cidadãos de diferentes origens e níveis de escolaridade. No cumprimento da LGPD, na apresentação de termos de consentimento e políticas de privacidade, muitos documentos apenas reproduzem determinações na linguagem da lei. Há o reforço do uso de expressões e características da escrita legal.

Nesse contexto, a linguagem simples faz a diferença, uma vez que contribui para que os leitores com pouca alfabetização possam compreender o mundo ao seu redor. Isso acontece pois ela se utiliza de recursos de organização visual e escrita para facilitar a busca por respostas. Aplicando-a, podem ser adaptados "documentos, gráficos, figuras, modelos de processos, modelos organizacionais, *websites* e interfaces de sistemas" (Capelli *et al.*, 2021).

A linguagem cidadã, como também é identificada, funciona no âmbito dos serviços públicos como ferramenta de inclusão aos serviços (Mont'Alvão, 2021). Ela melhora e aumenta a compreensão à medida que prioriza o leitor. As informações referentes a LGPD, ainda complexas, se informadas adequadamente, resultarão em cidadãos prontos para decisões conscientes ou até questionamentos a respeito dos seus direitos.

Além disso, segundo Capelli *et al.* (2021), a *plain language* recorre à usabilidade e acessibilidade para alcançar a transparência. Isso porque é a compreensão que permite ao cidadão ser ativo e participativo, lembrado aqui como um dos objetivos das cidades inteligentes, movidas a dados.

Ao analisar a legislação de dados europeia, Bowyer *et al.* (2022) detectam que ela não foi bem sucedida em empoderar os direitos e controles dos indivíduos sobre a sua privacidade. O que indicou experiências não satisfatórias dos usuários em relação a GDPR em função da complexidade da sua apresentação.

O fato é que problemas estão relacionados à linguagem utilizada nas políticas de privacidade. Difíceis de entender, elas podem comprometer a confiança dos usuários em relação ao sistema, a empresas e ao governo. Há ruído de comunicação na compreensão de quais dados estão sendo coletados, como são compartilhados e com quem, sem as devidas explicações.

O que significa ainda mais, quando considerado que os usuários não deveriam consentir sem ser previamente informados e estarem conscientes, no controle, de todos os aspectos envolvidos nas suas tomadas de decisões (Bartali; Velsen, 2023; Bowyer *et al.*, 2022).

Como visto, a arquitetura do visual é fundamental para contribuir com a comunicação e interação em relação às políticas de privacidade. Entretanto, a emancipação dos indivíduos não será apenas devido a projeção de interfaces melhores. Mas sim com políticas estrategicamente desenvolvidas que considerem o contexto multiparticipativo e sociotécnico de explicação das informações sobre os dados (Bowyer *et al.*, 2022).

Os usuários devem receber mais e melhores explicações sobre como seus dados serão usados, para quais propósitos são coletados. Para que, primeiro, as pessoas saibam se aquelas informações pessoais têm uma finalidade comercial ou não (Bartali; Velsen, 2023). O consentimento deve ser claramente explicado, especificado, com informações que permitam aos usuários controlar os próprios dados (Alharbi *et al.*, 2023).

A linguagem simples visa facilitar a compreensão, localização e uso das informações em função da transparência e participação cidadã. Portanto, é possível usá-la como *guideline* para que questões de privacidade e consentimento sejam apresentadas mais claramente.

3.4 Considerações do capítulo

A partir das abordagens do design identificou-se como é possível centrar a privacidade em torno do usuário, aqui o cidadão. Como visto, a interação humano-computador prioriza a satisfação do usuário e a confiança no sistema. Isso porque se preocupa com a usabilidade e a acessibilidade. Entretanto, a integração com a privacidade apresenta desafios. Uma vez que revela a necessidade da promoção da transparência e responsabilidade e da conformidade legal.

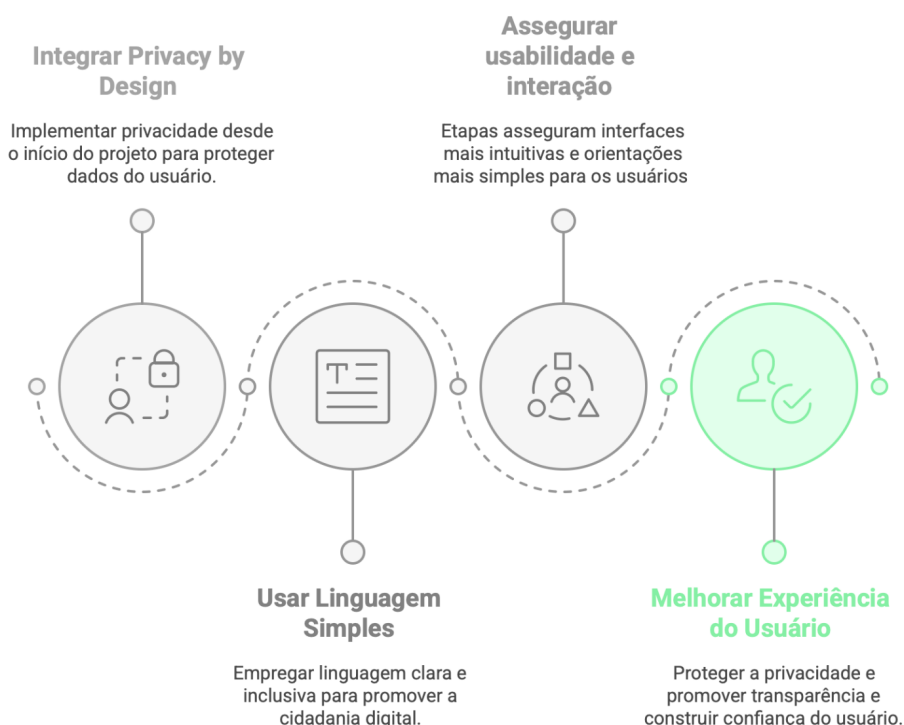
O design centrado no usuário ou no humano busca o envolvimento do usuário em todas as etapas do processo. Enquanto o design de interação foca na usabilidade e perspectiva desse usuário, criando experiências interativas melhoradas. Dessa forma, relacioná-los à privacidade pode fornecer soluções eficazes e eficientes. Uma vez que eles possibilitam entender como as pessoas realizam as tarefas fazendo com que as necessidades delas sejam orientadoras do trabalho.

Apesar dos propósitos dessas abordagens, a usabilidade em sistemas governamentais enfrenta desafios. Interfaces de comunicação dos *cookies* utilizam *dark patterns* e induzem o consentimento dos usuários. Isso ameaça o objetivo de serviços governamentais de uso fácil e seguro. Consequentemente, compromete a experiência dos usuários, um aspecto central da vida moderna.

A forma de superar os desafios que as abordagens e disciplinas enfrentam em relação à usabilidade, interação e experiência dos usuários acontece na absorção da metodologia *privacy by design* e da linguagem cidadã. O primeiro prioriza a consideração da privacidade desde o início do projeto. Ou seja, é importante para os designers, projetistas e demais profissionais e equipes envolvidos no projeto de um serviço de governo digital.

Utilizando-o, espera-se a entrega de interfaces visuais intuitivas no compartilhamento de dados que aumentem a confiança dos usuários. Já a linguagem cidadã, atua diretamente na inclusão e garantia do exercício da cidadania digital do usuário do serviço. Isso promove a transparência e permite que as pessoas tomem decisões mais conscientes sobre a privacidade e o consentimento de dados. A figura 5 ilustra esse processo.

Figura 5 - Integração do Privacy by Design e da Linguagem Simples ao Design



Fonte: elaborado pela autora, 2025.

Interseccionar esses conceitos possibilitou mostrar as contribuições de pesquisas existentes. Com isso, pôde-se verificar desafios e discutir o *privacy by design* e a linguagem cidadã com recursos importantes do processo de design que busca uma experiência transparente e cuidadosa com a privacidade do usuário.

As informações levantadas serviram não apenas para entender como relacionar a privacidade aos conceitos de design, mas orientar o percurso metodológico desta dissertação. Os conceitos trazidos destacaram como e quais instrumentos usar para envolver essas pessoas. Dessa forma, por meio deles e suas propostas, as formas de considerar a privacidade e um caminho para as perspectivas e experiências de um usuário comum e local. No capítulo seguinte, os métodos e técnicas que constituíram esta pesquisa.

4 MÉTODOS E TÉCNICAS

Neste capítulo, dividido em cinco seções, são apresentados os procedimentos metodológicos que orientam a pesquisa. Na primeira, discorre-se sobre como ela se caracteriza em relação à natureza, aos objetivos e à abordagem. As seções segunda, terceira e quarta tratam dos tipos de pesquisa adotados, bem como a sua fundamentação. Por fim, a quinta seção aborda as considerações do capítulo.

4.1 Caracterização da pesquisa

Esta pesquisa é de natureza aplicada, uma vez que visa apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital. Schwartzman (1979) considera que a pesquisa aplicada busca vincular o trabalho acadêmico às necessidades sociais. Segundo Moreira e Caleffe (2008), o objetivo é solucionar problemas. E para Prodanov e Freitas (2013), os conhecimentos gerados devem ter aplicação prática nessa solução de problemas.

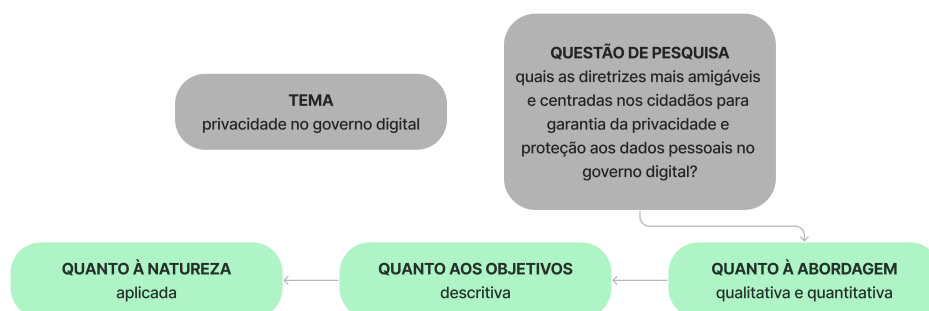
A pesquisa possui objetivos de caráter quantitativo, que buscam descrever percepções e interações. Mas também qualitativos que, de forma exploratória, pretendem fornecer visualização sobre fatos não plenamente explorados em estudos anteriores, de acordo com a literatura revisada. Apesar disso, como um todo, a pesquisa se classifica como descritiva, uma vez que adota preferencialmente técnicas padronizadas para coleta de dados.

Para Gil (2021), o objetivo da pesquisa descritiva é se debruçar sobre as características de um fenômeno e também de uma população. Isso porque ela tem como “objetivo levantar opiniões, atitudes e crenças” desse grupo social (Gil, 2021, p. 27). Ou seja, por meio dela, é possível descrevê-los, classificá-los e interpretá-los (Mont’Alvão; Moraes, 2010).

Quanto à abordagem, a pesquisa utiliza propriedades da pesquisa qualitativa e quantitativa. Sendo assim, é uma pesquisa de métodos mistos. Para Creswell (2021), adotar as duas abordagens está relacionado à interdisciplinaridade da pesquisa. Ou seja, para lidar com a complexidade dos problemas, o ideal é a aplicação das duas abordagens, até mesmo para que mais *insights* e uma melhor compreensão sejam obtidos.

Gil (2021) aponta que optar por métodos mistos de pesquisa justifica-se quando há a necessidade de aprofundamento do estudo com o segundo método. Para tanto, o objetivo é assegurar um nível de realidade que não pode ser quantificado, mas que pode ser complementado (Minayo, 2002) com informações numéricas (Lakatos e Marconi, 2010). Na figura 6, o esquema com o delineamento da pesquisa de acordo com o tema e a questão de pesquisa.

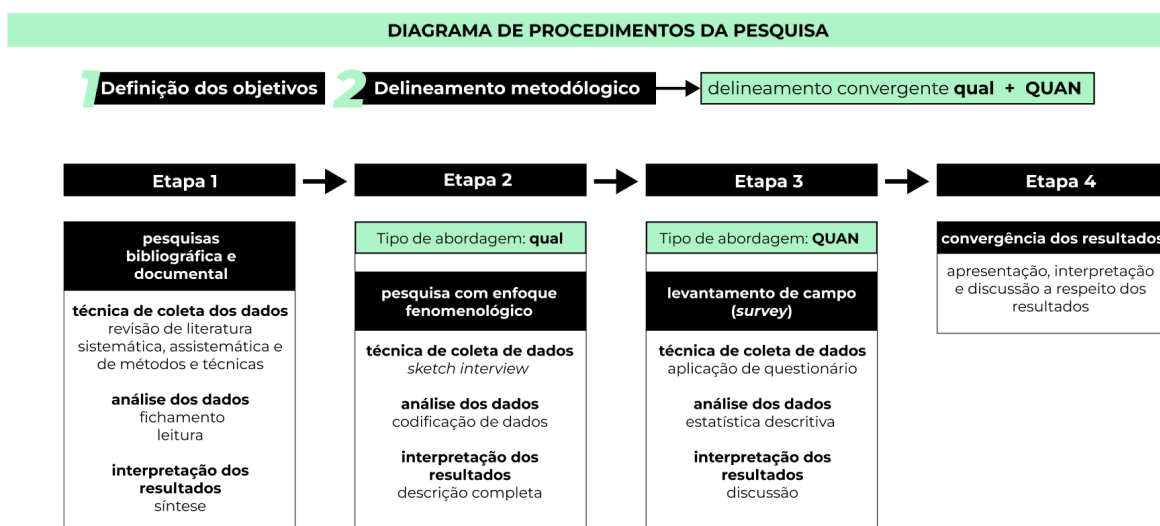
Figura 6 - Delineamento da pesquisa



Fonte: elaborado pela autora, 2024.

A partir do delineamento apresentado, a pesquisa foi desenvolvida em quatro etapas. O diagrama da figura 7 apresenta a ordem das etapas e seus procedimentos. Suas especificidades serão apresentadas nas seções seguintes.

Figura 7 - Etapas da pesquisa e seus procedimentos



Fonte: elaborado pela autora, 2025.

4.2 Pesquisa bibliográfica e documental

Segundo Lakatos e Marconi (2002), a pesquisa documental é constituída de fontes primárias. Para Gil (2021), esta é uma pesquisa cuja fonte de dados é rica e

estável. Dessa forma, com a pesquisa documental foi possível situar as questões referentes à privacidade e à proteção de dados dentro do governo digital segundo o próprio Estado brasileiro.

A pesquisa documental deste estudo foi realizada entre julho e outubro de 2023 on-line no portal eletrônico do planalto. Plataforma referente à subchefia para assuntos jurídicos da Casa Civil da Presidência da República. Foram selecionados, lidos e sintetizados nove documentos para fundamentação teórica. No quadro 3, a seguir, a lista dos documentos pesquisados.

Quadro 3 - Lista de documentos que compuseram a pesquisa documental

Documentos relacionados na pesquisa documental
Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011
Decreto nº 8.777, de 11 de maio de 2016 que Institui a Política de Dados Abertos do Poder Executivo Federal
Lei de Proteção ao Usuário do Serviço Público, Lei nº 13.460, de 26 de junho de 2017
Marco Civil da Internet, Lei nº 12.965, de 23 de abril 2014
Lei Geral de Proteção de Dados Pessoais Lei nº 13.853, de 14 de agosto de 2018
Lei do Governo Digital, Lei nº 14.129, de 29 de março de 2021
Estratégia brasileira de transformação digital, de 2018
Carta brasileira para as cidades inteligentes, de 2021
Estratégia Brasileira para a Transformação Digital (E-Digital), Ciclo 2022 - 2026

Fonte: elaborado pela autora, 2025.

Na pesquisa bibliográfica, optou-se por uma revisão de literatura, pois, de acordo com Creswell (2021), ela é importante para delimitar o recorte da pesquisa, compartilhar resultados anteriores, assim como destacar a relevância do assunto. Isso foi importante para descrever o cenário e relacioná-lo a conceitos como cidades inteligentes, capitalismo de dados e viés algorítmico.

4.2.1 Revisões sistemáticas de literatura

Durante a pesquisa bibliográfica foram realizadas duas revisões sistemáticas de literatura¹⁷ (RSL). De acordo com Santos *et al.* (2018), este método apresenta vantagens visto que proporciona uma estrutura teórica adequada que suporte a

¹⁷ Parte dos materiais revisados nesta seção constituíram os artigos Privacy and Consent in Digital Interfaces: A Literature Review e Privacy at the e-government within user-centered design and human-centered design context: a literature review. Eles foram submetidos ao evento IEA2024 (22nd Triennial Congress of the International Ergonomics Association) e à revista DAT Journal, 9(2), 88–102. <https://doi.org/10.29147/datjournal.v9i2.806>, respectivamente.

interdisciplinaridade das pesquisas do Design. Isso se deve a como a RSL se propõe a abarcar o conhecimento gerado e acumulado nas mais diversas áreas.

a) Revisão sistemática de literatura I (RSL I)

A primeira revisão sistemática foi elaborada em junho de 2023. O foco da busca era verificar pesquisas anteriores que relacionassem a interação dos usuários com as políticas de proteção à privacidade em interfaces digitais. O que consistiu no protocolo (quadro 4) de pesquisa abaixo:

Quadro 4 - Protocolo da RSL I

Protocolo de critérios para identificação	
Base de dados	Capes; Oasis; Scielo
Tipos de documento	Artigos; Anais de eventos
Área de concentração	Ciências sociais aplicadas; Ergonomia; Inovação pública
Período	7 anos (2016 - 2023)
Idioma	Português; Inglês
Localização dos termos	Assuntos; Palavras-chave
Palavras-chave	GDPR; privacy by design; privacidade por projeto; LGPD; proteção de dados; data protection; human factors; ergonomia; termos de consentimento; consent; linguagem simples; plain language
Critérios de inclusão	1: Pesquisas que discutam privacy by design, questões de consentimento e regulamentação de dados; 2: Pesquisas que abordem a proteção de dado e a privacidade digital.
Critérios de exclusão	1: Pesquisas que tratem de aspectos referentes a engenharia e arquitetura de softwares; 2: Pesquisas que não versem sobre questões de consentimento e privacidade em face à regulamentação de dados.

Fonte: elaborado pela autora, 2024.

A aplicação deste protocolo nas bases de dados escolhidas encontrou um total de 122 trabalhos. Desse número, 33 foram selecionados após uma leitura dos resumos e identificação das palavras-chave utilizadas pelos autores. Entretanto, apenas 20 trabalhos deste grupo estavam disponíveis abertamente para pesquisa e *download*, conforme ilustrado pela tabela 1.

Tabela 1 - Associação de termos e resultados da RSL I

Termos Pesquisados	Capes	Oasis	Scielo
"GDPR" AND "privacy by design"	32	2	0
"GDPR" AND "privacidade por projeto"	0	0	0
"GDPR" AND "human factors"	12	0	0
"GDPR" AND "ergonomia"	0	0	0
"GDPR" AND "plain language"	2	0	0
"GDPR" AND "linguagem simples"	0	0	0
"LGPD" AND "privacy by design"	1	3	0
"LGPD" AND "privacidade por projeto"	0	0	0
"LGPD" AND "ergonomia"	0	2	0
"LGPD" AND "linguagem simples"	0	0	0
"privacy by design" AND "consent"	35	2	0
"privacy by design" AND "termos de consentimento"	0	0	0
"data protection" AND "human factors"	24	0	0
"data protection" AND "plain language"	4	0	0
"proteção de dados" AND "ergonomia"	0	3	0
"proteção de dados" AND "linguagem simples"	0	0	0
Total de trabalhos encontrados	110	12	0
Total de trabalhos selecionados	32	1	0
Total de trabalhos disponíveis	19	1	0

Fonte: elaborado pela autora, 2024.

Nos artigos disponíveis foi realizada uma leitura parcial de suas introduções e conclusões. Aqueles que não estavam alinhados ao objetivo da revisão de literatura foram descartados. Por fim, 5 trabalhos foram incluídos para construção do referencial teórico, e podem ser identificados no quadro 5. O fluxo completo da RSL I pode ser visto na figura (8) em seguida.

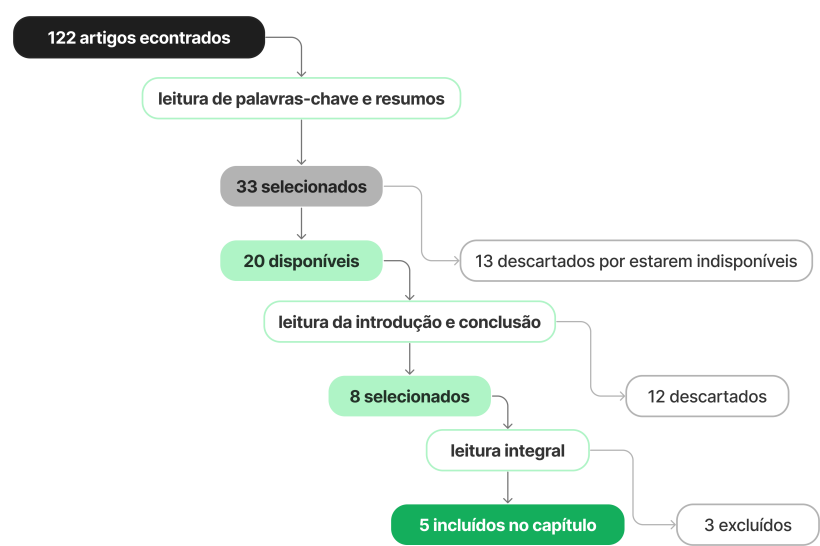
Quadro 5 - Trabalhos selecionados na RSL I

Título	Autores
Tell Me What You Know: GDPR Implications on Designing Transparency and Accountability for News Recommender Systems	Krebs <i>et al.</i> (2019)
Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR	Machuletz; Böhme (2020)
A Multidisciplinary Definition of Privacy Labels	Johansen <i>et al.</i> (2021)
Human-GDPR Interaction: Practical Experiences of Accessing Personal Data	Bowyer <i>et al.</i> (2022)

An Empirical Analysis of E-Governments' Cookie Interfaces in 50 Countries	Alharbi <i>et al.</i> (2023)
---	------------------------------

Fonte: elaborado pela autora, 2024.

Figura 8 - Fluxo da RSL I



Fonte: elaborado pela autora, 2024.

b) Revisão sistemática de literatura II (RSL II)

Em novembro de 2023 foi desenvolvida uma nova revisão sistemática de literatura. Dessa vez, o foco consistia em investigar como o *User Centered Design* e o *Human Centered Design* podem contribuir para a consciencialização dos cidadãos. Assim como na abordagem às questões de privacidade no *e-government*.

Na RSL II, o protocolo concentrou-se em uma base de dados que indexa uma diversidade de *journals*, a *ScienceDirect*. Foram revisados trabalhos apenas em língua inglesa e em um período de cinco anos. No quadro (6), o protocolo que orientou a RSL II.

Quadro 6 - Protocolo da RSL II

Protocolo de critérios para identificação	
Base de dados	ScienceDirect
Tipos de documento	Artigos de revisão de literatura e de pesquisa
Período	5 anos (2019 a 2023)

Palavras-chave	UCD; HCD; privacy; privacy by design; e-government
Cr�terios de exclus�o	Artigos n�o relacionados com o objetivo estabelecido para a revis�o, duplicados e n�o dispon�veis gratuitamente; artigos sobre computa��o focados em arquitetura da informa��o e web.

Fonte: elaborado pela autora, 2024.

Na RSL II, entre os 330 trabalhos dispon veis na busca, 29 foram selecionados para leitura parcial dos resumos e palavras chave. Ap s a leitura da introdu  o e conclus  o, 11 artigos foram selecionados para leitura integral. O quantitativo de resultados dispon veis e selecionados baseados na combina  o de termos pesquisados na RSL II pode ser visto na tabela 2.

Tabela 2 - Associa  o de termos e resultados da RSL II

Termos pesquisados	Dispon�veis	Selecionados
"UCD" AND "privacy by design"	6	1
"UCD" AND "privacy"	64	5
"HCD" AND "privacy"	29	1
"HCD" AND "privacy by design"	1	0
"e-government" AND "privacy by design"	10	6
"e-government" AND "privacy"	220	16
Total	330	29

Fonte: elaborado pela autora, 2024.

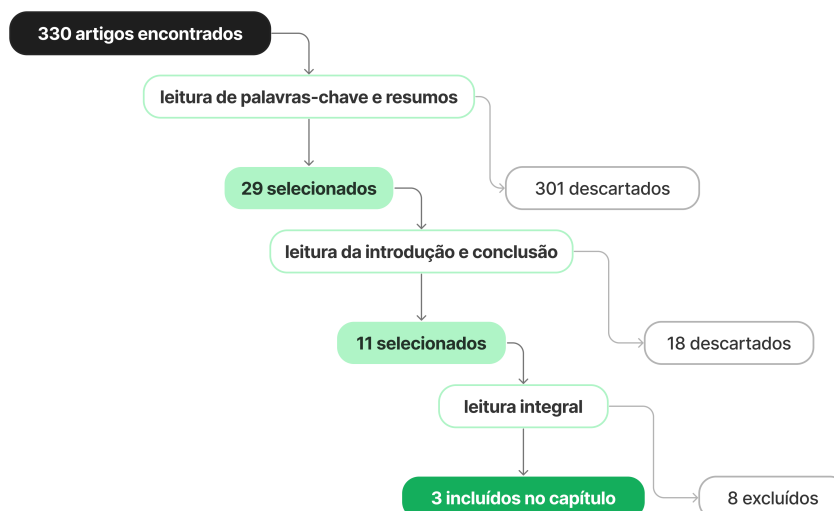
Na figura 9,   poss vel visualizar o fluxo completo da RSL II. Como resultado, 3 artigos foram inclu dos nesta pesquisa e podem ser visualizados no quadro 7. em seguida. Os demais (8) foram desconsiderados definitivamente.

Quadro 7 - Trabalhos selecionados na RSL II

T�tulo	Autores
Design principles for creating digital transparency in government	Matheus <i>et al.</i> (2021)
Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods	Grafenstein <i>et al.</i> (2022)
An experiment on data sharing options designs for eHealth interventions	Bartali; Velsen (2023)

Fonte: elaborado pela autora, 2023.

Figura 9 - Fluxo da RSL II



Fonte: elaborado pela autora, 2023.

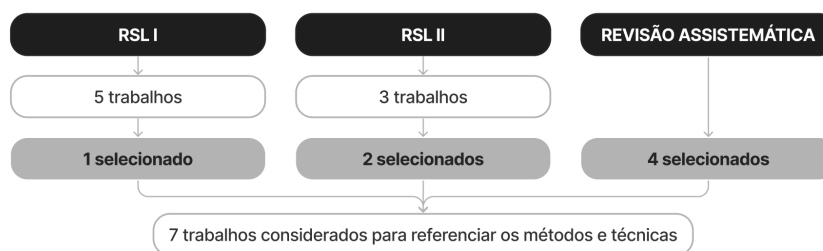
Os 8 trabalhos (cinco da RSL I e três da RSL II), elencados anteriormente, foram relacionados e utilizados na constituição da fundamentação teórica apresentada no capítulo 3. Além disso, o contexto geográfico e o perfil dos participantes de pesquisa foram identificados como lacunas a serem exploradas.

Os trabalhos também foram utilizados enquanto referencial metodológico para os procedimentos de coleta de dados utilizados nesta pesquisa. Essa revisão de métodos e técnicas será apresentada em seguida.

4.2.2 Revisão de métodos e técnicas

Realizar uma revisão de métodos e técnicas teve como objetivo mapear métodos e técnicas de design que considerem a perspectiva do usuário nos estudos sobre privacidade. Um trabalho foi selecionado a partir da leitura dos trabalhos incluídos na RSL I e dois foram selecionados entre os incluídos na RSL II. Posteriormente, mais quatro trabalhos fruto de uma revisão assistemática foram adicionados ao grupo. O fluxo desse processo de seleção pode ser visto na figura 10.

Figura 10 - Fluxo da revisão de métodos



Fonte: elaborado pela autora, 2024.

A lista de 7 trabalhos incluídos para a revisão dos métodos pode ser verificada no quadro 8, a seguir.

Quadro 8 - Trabalhos selecionados nas RSL I, II e revisão narrativa

RSL I	Autores	Técnicas
Human-GDPR Interaction: Practical Experiences of Accessing Personal Data	Bowyer <i>et al.</i> (2022)	Entrevistas (<i>Sketch interview</i>)
RSL II	Autores	Técnicas
Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods	Grafenstein <i>et al.</i> (2022)	Workshops e entrevistas
An experiment on data sharing options designs for eHealth interventions	Bartali; Velsen (2023)	<i>Online design experiment</i> (Questionários)
Revisão Narrativa	Autores	Técnicas
User-Centered Privacy-by-Design: evaluating the appropriateness of design prototypes	Ayalon; Toch (2021)	<i>Online experimental design</i> (Questionários)
Assessing behavioral data science privacy issues in government artificial intelligence deployment	Saura <i>et al.</i> (2022)	Entrevistas
Designing for privacy: exploring the influence of affect and individual characteristics on users' interactions with privacy policies	Kitkowska <i>et al.</i> (2023)	<i>Online design experiment</i> (Questionários)
The construction of self-sovereign identity: extending the interpretative flexibility of technology	Weigl <i>et al.</i> (2023)	Entrevistas

Fonte: elaborado pela autora, 2024.

4.3 Pesquisa qualitativa

Segundo Gil (2021), uma pesquisa qualitativa se caracteriza pelo seu viés interpretativista. Nele, o processo de compreensão das interações sociais passa pelo foco na perspectiva de quem de fato vivencia essas experiências. Para Lakatos

e Marconi (2010), é o tipo de pesquisa que retoma as histórias de vida, uma vez que há contato direto e até prolongado com os atores e situações estudadas.

Creswell e Clark (2017) partem também dessa caracterização para dizer que os métodos envolvidos pelo pesquisador na pesquisa qualitativa são interativos e humanísticos. O autor destaca que esse processo não é imutável assim como a análise é fundamentalmente interpretativa. Considerando Gil (2017; 2021) e Creswell (2014) e Creswell e Clark (2017), este estudo tem características de uma pesquisa com enfoque fenomenológico.

4.2.1 Pesquisa com enfoque fenomenológico

Esta parte da pesquisa discute como cidadãos locais vêem a privacidade e a proteção dos seus dados digitais. Esse tópico é explorado sob o ponto de vista fenomenológico porque a intenção é entender o conceito privacidade como fenômeno. A pesquisa fenomenológica consegue descrever o significado que os participantes atribuem às experiências vivenciadas sobre certo conceito. Para isso se vale de técnicas que permitem que os participantes se expressem mais livremente (Creswell, 2014; Gil, 2021).

Creswell (2014) explica que no enfoque fenomenológico a intenção é que a amostra da pesquisa seja formada por um grupo pequeno e heterogêneo de participantes. Para o autor, entrevistas aprofundadas são as mais recomendadas para essa abordagem. Ademais, nesse enfoque, os resultados das entrevistas precisam, descrever e discutir a essência das experiências dos participantes.

4.2.2 Entrevistas

Bowyer *et al.* (2022) utilizam um instrumento pensado e centrado no usuário e no design de experiência dos usuários para conduzir suas entrevistas. Os autores recorreram à *sketching interview* para que os usuários pudessem falar de experiências práticas ao acessar dados pessoais por meio de uma interação Humano-GDPR. Assim, na técnica utilizada de Bowyer *et al.* (2022), foi encontrada a opção de entrevista que correspondesse aos propósitos desta pesquisa.

Na *sketch interview* de Bowyer *et al.* (2022), os participantes são entrevistados em um primeiro momento chamado *Life sketching*. Nele, eles produzem rabiscos, palavras ou mapas de associação sobre suas percepções a

respeito dos seus dados, além de responderem a perguntas. Depois de uma sensibilização a respeito da GDPR, os participantes foram consultados posteriormente sobre novas contribuições às suas produções.

Inicialmente, nesta pesquisa, a ideia era que os entrevistados fizessem rabiscos de associação. Entretanto, após a condução dos pré-testes¹⁸, verificou-se que seria uma atividade desagradável para os participantes. Dessa forma, os rabiscos foram substituídos por mapas mentais, também utilizados no *Life sketching* de Bowyer *et al.* (2022).

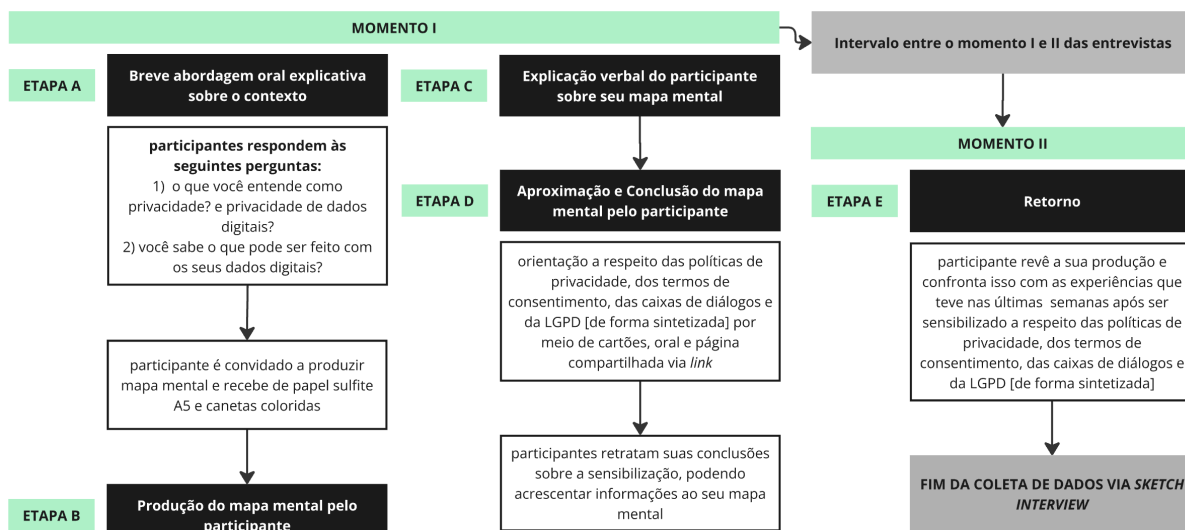
A pauta de condução da *sketch interview*, bem como o Termo de Consentimento Livre e Esclarecido - TCLE, conforme resolução CNS 466/2012, foram submetidos à aprovação do comitê de ética da UFMA. O último informava previamente os participantes sobre o objetivo e justificativa, procedimentos, riscos, benefícios, custos, confidencialidade do estudo e participação voluntária da pesquisa. O parecer favorável pode ser visualizado no Apêndice A e a pauta da entrevista no Apêndice D.

Na adaptação da *sketch interview* feita para esta pesquisa, o instrumento foi conduzido em dois momentos. No primeiro, os participantes responderam às perguntas I) O que você entende como privacidade? E privacidade de dados digitais? e II) Você sabe o que pode ser feito com os seus dados digitais?. Após as respostas, foram convidados a produzir o mapa mental, caso se sentissem confortáveis, e explicá-lo.

Por último, recebiam informações de sensibilização sobre a LGPD, políticas de privacidade e termos de consentimento, cookies e consentimento. Isso foi realizado através de cartões explicativos lidos pelos participantes ou em conjunto com a pesquisadora. Na versão on-line, os participantes receberam *link* de uma página hospedada na plataforma *Notion*, com o mesmo conteúdo dos cartões, para leitura.

No segundo momento, semana depois, os participantes deveriam relatar sobre suas experiências pós-sensibilização e se gostariam ou não de acrescentar algo ao mapa. A figura 11 apresenta esquema de condução da *sketch interview*.

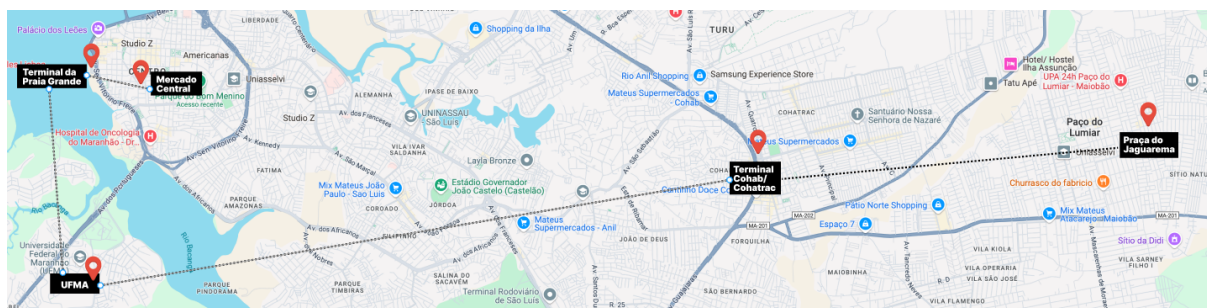
¹⁸ conduzidos com 4 voluntários presencialmente e 1 via aplicativo de mensagens

Figura 11 - Etapas de condução da *sketch interview*

Fonte: elaborado pela autora, 2025.

O primeiro momento da *sketch interview* (entrevista acompanhada de esquema/mapa mental) foi realizado em outubro de 2024. À campo, foram coletadas falas de 21 participantes. Destes, 11 aceitaram produzir mapas mentais sobre o tema "privacidade de dados digitais", os outros 10 participantes não se sentiram confortáveis em cumprir esta etapa da entrevista.

As entrevistas foram conduzidas no Mercado Central de São Luís, no Terminal de Integração da Praia Grande; no Terminal de Integração da Cohab/ Cohatrac; na Universidade Federal do Maranhão; e na praça do Jaguarema, em Paço do Lumiar. Conforme o mapa da figura 12.

Figura 12 - Locais em que foram realizadas as *sketch interviews*

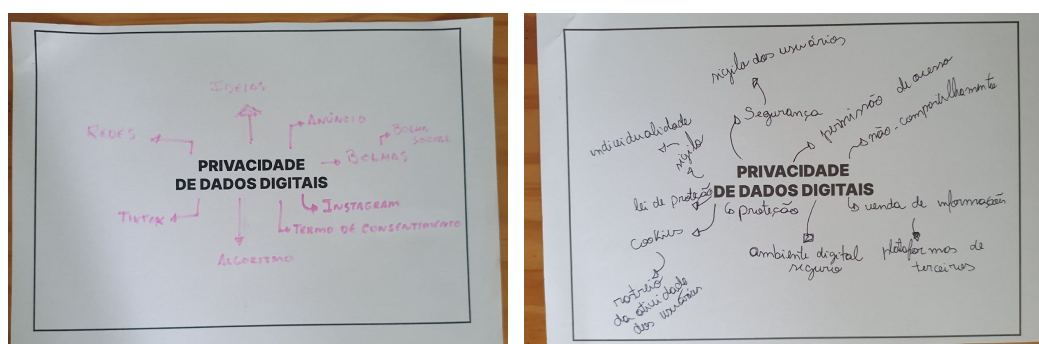
Fonte: Google, 2025.

Foram escolhidos para participar trabalhadores formais e informais e estudantes desses ambientes, em uma amostra de oportunidade. O momento I da *sketch interview* foi realizado durante duas semanas. Todos consentiram em

participar da pesquisa mediante assinatura do Termo de Consentimento Livre e Esclarecido - TCLE (Apêndice B).

Os participantes, que foram entrevistados presencialmente nos locais mencionados anteriormente, receberam uma folha em formato A5 com a expressão “PRIVACIDADE DE DADOS DIGITAIS” ao centro. Eles foram informados, após responderem às perguntas anteriores, que ali, no espaço livre, deveriam compor o seu mapa mental, conforme a etapa B do momento I (figura 8). Alguns dos mapas produzidos nessa fase podem ser vistos na figura 13.

Figura 13 - Alguns mapas mentais produzidos pelos participantes presencialmente. À esquerda entrevistado E12 - F - 20 a 24 e à direita entrevistado E3 - M - 25 a 29.

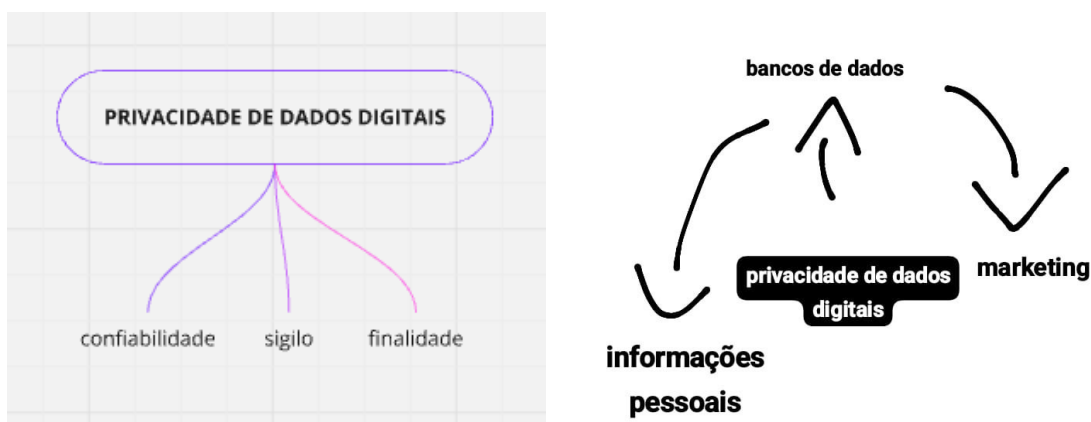


Fonte: Entrevistados [E12 - F - 20 a 24] e [E3 - M - 25 a 29], 2024.

Diante da necessidade de coletar mais mapas mentais para extrair dados que contribuíssem com a pesquisa, foram conduzidas mais 5 *sketch interviews*. Todos os participantes da segunda etapa aceitaram produzir os mapas mentais. Essas entrevistas foram realizadas on-line via aplicativo de mensagens *WhatsApp*.

Os participantes optaram por fazer por recursos (*apps*) nos próprios celulares, usando a plataforma *Miro* ou indicando as palavras para que a pesquisadora construísse o mapa virtualmente. Dessa forma, como saldo final foram produzidas 26 *sketch interviews*, das quais 16 resultaram em mapas mentais produzidos pelos participantes. Na figura 14, a seguir, alguns dos mapas feitos pelos participantes que foram entrevistados virtualmente.

Figura 14 - Alguns mapas mentais produzidos pelos participantes digitalmente. À esquerda entrevistado E24 - M - 40 a 44 e à direita entrevistado E26 - F - 18 a 19.

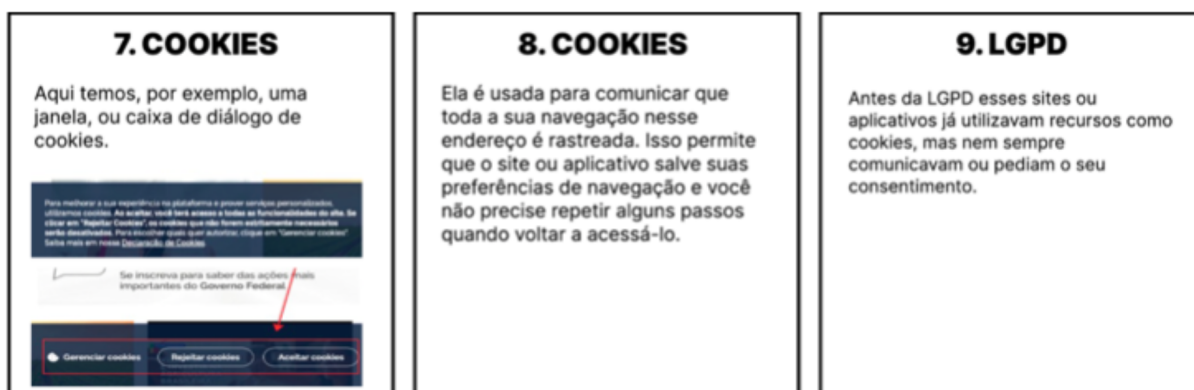


Fonte: Entrevistados [E24 - M - 40 a 44] e [E26 - F - 18 a 19], 2024.

Depois de produzirem os mapas mentais, os participantes foram sensibilizados em relação à LGPD, aos conceitos de consentimento, termos de consentimentos e políticas de privacidade e cookies. Eles receberam uma série de cartões (figura 15) com as informações sintetizadas e leram com o apoio da pesquisadora.

Figura 15 - Cartões utilizados para sensibilização dos participantes





Fonte: Elaborado pela autora, 2025.

Os entrevistados que participaram virtualmente receberam a informação via *link* de uma página hospedada (figura 16) on-line.

Figura 16 - *Printscreen* da página com conteúdo de sensibilização [link na imagem]



PROTEÇÃO DE DADOS E PRIVACIDADE

- ▶ LGPD
- ▶ POLÍTICAS DE PRIVACIDADE E TERMOS DE CONSENTIMENTO
- ▶ CAIXAS DE DIÁLOGO E COOKIES

Fonte: Elaborado pela autora, 2025.

Dos 26 participantes do momento I da *sketch interview*, 9 pessoas aceitaram ou foram encontradas para participar do momento II entre dezembro de 2024 e janeiro de 2025. A eles foi questionada sua percepção acerca da privacidade de dados digitais após a primeira etapa. Desse grupo, 3 participantes decidiram incluir novas palavras nos mapas mentais produzidos na primeira etapa.

4.2.3 Análise dos dados qualitativos

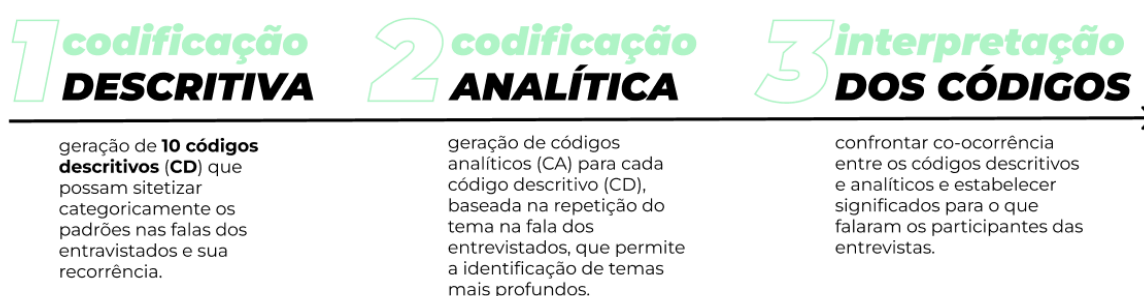
As informações obtidas via *sketch interview* foram analisadas por meio de codificação de dados. Charmaz (2009), Bowyer *et al.* (2022), Creswell (2014; 2021),

Creswell e Clark (2017), Gibbs (2009) e Gil (2021) forneceram fundamentação para que uma forma própria de codificar pudesse ser desenvolvida para esta pesquisa.

Segundo os autores, a codificação reduz informações e revela padrões e tendências ao categorizar e resumir as falas dos entrevistados a ideias através de códigos. Para os autores, esses códigos são rótulos, segmentos ou conjuntos significativos capazes de transmitir a essência geral da experiência dos participantes. Por meio de análise profunda e organização metódica e analítica dos códigos temáticos, eles revelam e permitem entender desde atitudes e cenários até emoções.

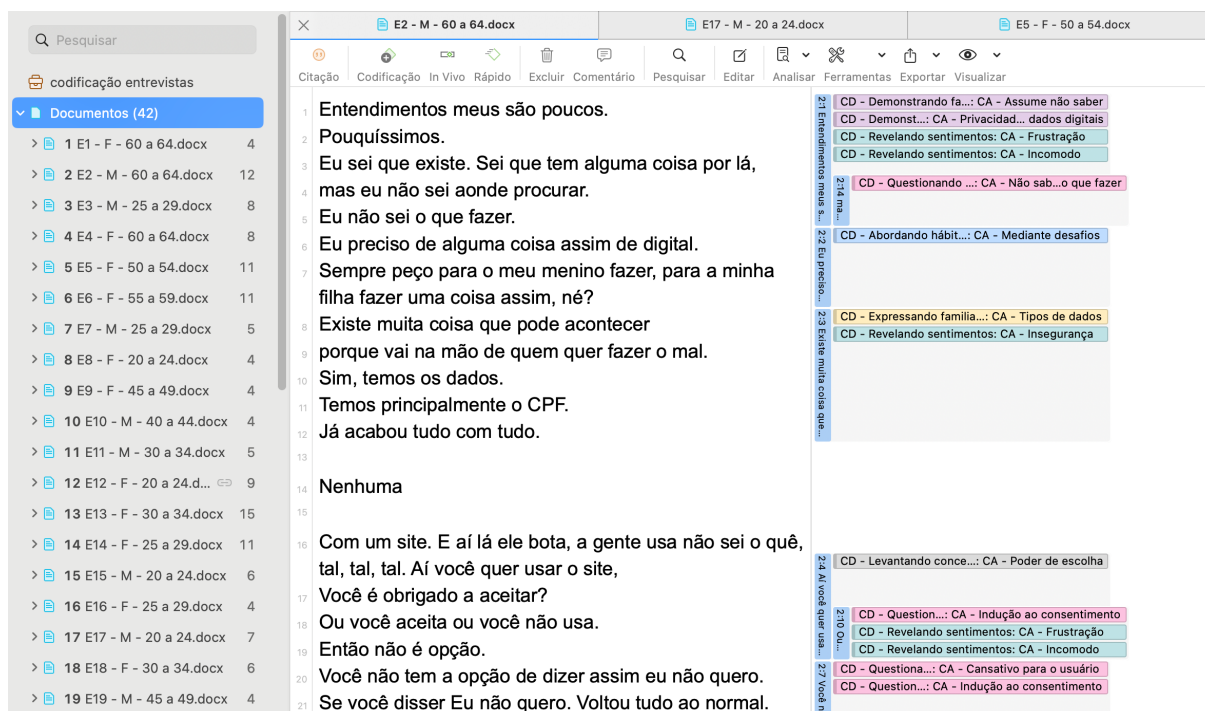
Nesta pesquisa, a codificação das *sketch interviews* aconteceu por meio de três fases, codificação descritiva; codificação analítica; e interpretação dos códigos. A primeira - **codificação descritiva** - consistiu na análise linha a linha das falas dos participantes durante as entrevistas e dos mapas mentais, utilizando o software de análise de dados ATLAS.ti. Conforme as figuras 17 e 18.

Figura 17 - Sequência da codificação no ATLAS.ti



Fonte: Elaborado pela Autora, 2025.

Para cada entrevistado foi gerado um arquivo no formato .docx, que continha a transcrição completa das suas falas, explicação sobre os mapas e palavras escolhidas. O processo de transcrição foi realizado nas plataformas *Speechtext.ai* e *Sonix.ai*, que utilizam inteligência artificial para transformar áudio em texto. Depois do processo, os textos foram lidos para verificar se estavam de acordo com o que foi dito pelos entrevistados.

Figura 18 - *PrintScreen* da tela de codificação no software ATLAS.ti

Fonte: elaborado pela Autora, 2025.

Cada arquivo foi nomeado com uma identificação padrão iniciada pela letra E (entrevistado). Assim como pela aplicação do número correspondente a ordem em que a pessoa foi entrevistada, a letra maiúscula do gênero do entrevistado e a sua faixa etária para ser codificado no ATLAS.ti. Por exemplo: E1 - F - 60 a 64; E2 - F - 60 a 64. Os resultados obtidos a partir das codificações serão apresentados no capítulo seguinte.

4.4 Pesquisa quantitativa

A pesquisa quantitativa, de acordo com Gil (2021), usa dados numéricos para alcançar a explicação dos fenômenos ou população que se estuda. E para Boudon (1989), ela é a que permite comparar as informações recolhidas de elementos determinados. Já para Lakatos e Marconi (2010), esse tipo é vantajoso pela precisão e controle uma vez que propõe objetividade, sistematização e quantificação de conceitos. Nesta pesquisa, ela acontece por meio de levantamento de campo, ou *survey*.

4.3.1 Levantamento de campo

Com o levantamento de campo, segundo Gil (2021, p. 61), é possível a “interrogação direta das pessoas cujo comportamento se deseja conhecer”. Ainda segundo o autor, essas informações fornecidas são submetidas a tratamentos estatísticos. Em função disso, tornam “possível verificar com mais propriedade as opções” (*ib.*, 2021, p. 61) do público de interesse sob um caráter descritivo.

De acordo com Balbe (2003), essa pesquisa possibilita a verificação empírica da informação levantada. Seu objetivo principal é a descrição uma vez que o formato possibilita medir, indiretamente, comportamentos a partir da descrição das respostas dos participantes. Além disso, se adequadamente coletados, os dados do levantamento de campo podem ser fonte contínua para outros estudos.

Na presente pesquisa, o levantamento é aplicado em conjunto com outro método qualitativo, a entrevista. Segundo Balbe (2003), essa junção torna o levantamento de campo ainda mais eficaz. Como forma de instrumentalizá-lo, foi utilizado um questionário, por ser uma técnica clássica de estudo quantitativo (Balbe, 2003; Gil, 2017; Lakatos; Marconi, 2003; Laville; Dionne, 1999; Santos *et al.*, 2018).

4.3.2 Questionário

Para Ayalon e Toch (2021), é fundamental envolver os verdadeiros usuários finais na aplicação de questionários em pesquisas de design. De acordo com as pesquisas de Kitkowaska *et al.* (2023), que relacionam design às políticas de privacidade, o instrumento consegue descrever níveis de afeição e preocupação em relação ao assunto. Assim, seu desenho pode indicar as necessidades, reclamações e satisfação com os designs e conteúdos das políticas de privacidade (Bartali; Velsen, 2023; Kitkowaska *et al.*, 2023).

Nesta pesquisa, da construção à aplicação, o levantamento de campo teve todo o seu procedimento definido em etapas baseadas em Gil (2021). Primeiro, a pesquisa foi atrelada a um objetivo específico. Depois foram delimitados variáveis, instrumento e pré-teste. Após a definição da coleta de dados, foi estabelecido como seria sua análise e apresentação dos resultados. As etapas são indicadas a seguir, no quadro 9.

Quadro 9 - Procedimento do levantamento de dados via questionário

Etapa	Ação
a Objetivo a ser cumprido com o levantamento de dados	Indicar como usuários do governo digital interagem com as políticas de privacidade e com os termos de consentimento
b Variáveis consideradas	• Residentes no Maranhão • Usuários e não usuários do <i>app</i> VIVA/Procon MA • Pessoas de todas as faixas etárias a partir de 18 anos
c Instrumento	Questionário hospedado no <i>googleforms</i>
d Pré-teste do instrumento	Compartilhamento virtual via <i>app</i> de mensagens <i>WhatsApp</i> , em dois grupos com 13 integrantes, ao todo. Questionário respondido por 5 pessoas.
e Coleta de dados	Submissão ao comitê de ética Realizada virtual e presencialmente entre dezembro/2024 e janeiro 2025
f Análise e interpretação dos dados	Tabulação de dados e estatística descritiva
g Resultados	Apresentados no capítulo 5 da dissertação.

Fonte: elaborado pela autora, com base em Gil (2021), 2025.

O questionário (Apêndice F) foi formulado com base nas referências coletadas durante as revisões sistemática, assistemática e de métodos e técnicas realizadas anteriormente. Após pré-teste, ele, assim como a pauta da entrevista, foi submetido a parecer do comitê de ética e aprovado para aplicação (Apêndice A).

Assim como também foi aprovado o termo de consentimento livre e esclarecido (Apêndice E), que o antecede em relação às respostas dos participantes. Além de informar o objetivo e os riscos mínimos da pesquisa. Conforme figura 19.

Figura 19 - PrintScreen do TCLE e questionário on-line

Seção 1 de 5

PROTEÇÃO DE DADOS E DA PRIVACIDADE NAS INTERFACES DO GOVERNO DIGITAL

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Título da pesquisa: Proteção de dados pessoais e da privacidade no governo digital

Nome da pesquisadora responsável: Fabiana França Silva

Nome da orientadora da pesquisa: Profª Drª Cláudia Renata Mont'Alvão

Gostaríamos de convidar você a participar como voluntária (o) de um questionário. O estudo é uma etapa da dissertação que estamos desenvolvendo no Programa de Pós Graduação em Design, da Universidade Federal do Maranhão (UFMA).

OBJETIVO

O objetivo do estudo é apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital.

JUSTIFICATIVA

É crescente o uso de iniciativas de governo digital no país, visando oferecer serviços públicos de forma mais fácil e prática. Isso é próprio de uma sociedade em rede cujos dados dos seus cidadãos operam em fluxo ininterrupto a fim de fornecer indicadores que melhorem a atuação da administração pública. Dessa forma, se revela a necessidade de estudos que contribuam para a conhecer o que os cidadãos entendem sobre o assunto, e, principalmente, para colaborar na proteção da privacidade e dos dados pessoais para que eles acessem tais serviços do governo digital com segurança ao passo que tenham seu direito à privacidade assegurado.

PROCEDIMENTOS METODOLÓGICOS

Para a realização desta etapa da pesquisa, você preencherá este formulário online que foi pré-estruturado sobre o tema elencado no título da dissertação.

RISCOS

Seção 2 de 5

Apresentação

Olá, me chamo Fabiana e sou aluna do Mestrado em Design pelo Programa de Pós-graduação em Design da Universidade Federal do Maranhão (UFMA).

Este formulário faz parte da minha pesquisa sobre a proteção de dados e da privacidade no âmbito das interfaces do governo digital.

Você pode entrar em contato comigo a qualquer tempo para informação adicional no e-mail fabiana.fs@discente.ufma.br

Desde já, agradeço sua colaboração.

0.1 Você já utilizou o aplicativo VIVA PROCON/MA? *

☐ Não

☐ Sim, já utilizei para 1 serviço

☐ Sim, já utilizei para mais de 2 serviços diferentes

Seção 3 de 5

Parte 1

Agora, vamos falar sobre privacidade de dados digitais.

1.2 Você já ouviu falar sobre a LGPD? *

☐ Sim

☐ Não

Fonte: elaborado pela autora, 2025.

A aplicação do questionário teve início em dezembro de 2024 e foi concluída em janeiro de 2025. Para alcançar os respondentes, o *link* do formulário hospedado no *googleforms* foi compartilhado em grupos através do aplicativo de mensagens *WhatsApp*. Ele também foi publicado em grupos de moradores de diferentes cidades maranhenses nas redes sociais *Facebook* e *Reddit*. Além disso, também foram publicados anúncios pagos para divulgação na plataforma *Meta*.

Nesse primeiro momento, de disparo on-line, foram obtidas respostas de 22 participantes. Em janeiro de 2025, foram realizadas aplicações presenciais do questionário. Esse processo foi conduzido em dias variados por um período de três semanas.

Os respondentes foram localizados em locais públicos de São Luís: no Estacionamento do projeto Reviver; na Praça Nauro Machado; na Praça Benedito Leite; na Praça João Lisboa; na Avenida Sen. Vitorino Freire; e na Praça Deodoro. Na figura 20 é possível acompanhar onde os locais estão situados.

Figura 20 - Locais de aplicação do questionário



Fonte: Google, 2025.

No formato presencial foram obtidas 20 respostas. A coleta de dados da Etapa 3 da pesquisa forneceu um total de 42 respostas. Desse número, 7 pessoas que haviam participado da *sketch interview* aceitaram participar na nova etapa e fornecer respostas ao questionário.

4.3.3 Análise dos dados quantitativos

Os dados levantados via aplicação de questionário foram analisados por meio de estatística descritiva. Isso em função da possibilidade de sintetizar e organizar uma quantidade maior de dados. Análise na estatística descritiva envolve o cálculo das medidas de tendência central, como a média, a mediana e a moda. Também é constituída pelas medidas de dispersão e amplitude. Dessa forma, ambas as medidas permitem visualizar o comportamento dos dados.

Nesta pesquisa, foram formulados gráficos e histogramas para explicitar a variabilidade e tendência dos dados. Os elementos foram explorados para fornecer um quadro maior sobre o que os dados indicam e sua consequente descrição a respeito do problema da pesquisa. Além disso, foi possível estabelecer relações e comparações entre os dados e estabelecer a interpretação a partir dos resultados obtidos (Gil, 2017).

4.5 Convergência dos dados qualitativos e quantitativos

Por se tratar de uma pesquisa de métodos mistos, este trabalho usa do procedimento de convergência de dados qualitativos e quantitativos para constituir a interpretação e discussão sobre os resultados. Este delineamento é baseado em Creswell e Clark (2017). Segundo os autores, em uma pesquisa de métodos mistos este delineamento permite que o pesquisador compartilhe as descobertas

qualitativas com os resultados estatísticos e quantitativos para entender completamente o problema de pesquisa.

Nesta pesquisa, os resultados foram identificados, contrastados e sintetizados (Creswell e Clark, 2017) em uma tabela de discussão. A intenção foi identificar pontos em que os resultados se relacionam, convergindo ou divergindo. Dessa forma, foi possível estabelecer um entendimento acerca do problema e apontar diretrizes conforme objetivo principal.

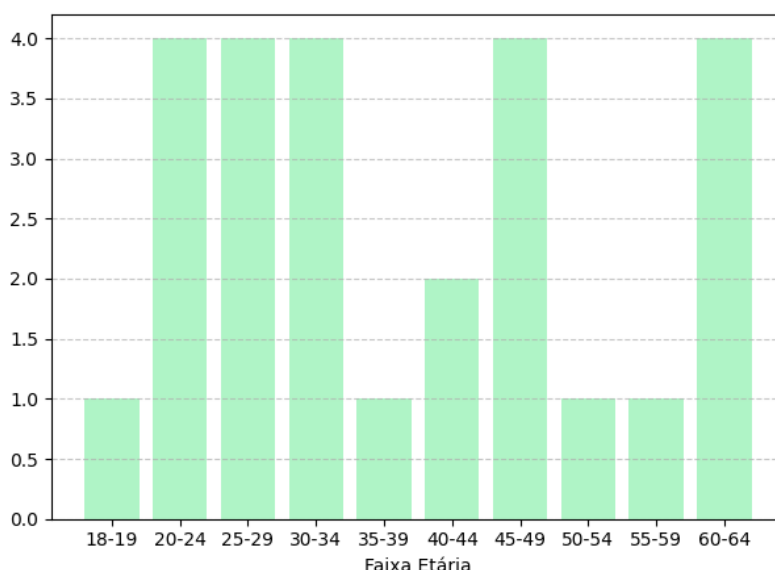
5 RESULTADOS

Este capítulo traz os resultados obtidos a partir dos dados analisados. Ele está dividido em três seções. Na primeira, são apresentados os resultados da *Sketch Interview*. A segunda apresenta os resultados dos questionários. A seção três traz a convergência e discussão desenvolvidas por meio de ambos os resultados.

5.1 *Sketch Interview*

Dado o cerne da pesquisa, os participantes não serão identificados durante a apresentação dos resultados. Entretanto sua faixa etária será apresentada para obter um breve perfil deles. O histograma da figura 21, em seguida, representa as classes das idades dos entrevistados.

Figura 21 - Histograma das classes de idades dos entrevistados



Fonte: elaborado pela autora, 2025.

A média ponderada obtida dos dados em classe é de aproximadamente 38,79 anos. Metade dos participantes, 13 pessoas, têm abaixo de 34 anos e a outra metade está acima dessa idade. Dos 16 entrevistados, 16 se identificaram como do gênero feminino e 10 como do gênero masculino.

5.1.1 Codificação descritiva

A primeira etapa do processo utilizado para analisar os dados obtidos via entrevistas e mapas mentais - a codificação de dados - é a codificação descritiva. Ela aconteceu a partir dos seguintes passos:

- a. Adição dos arquivos individuais da transcrição das entrevistas e dos mapas mentais (.docx e .jpg) no *software* de análise de dados ATLAS.ti;
- b. Leitura criteriosa linha a linha das transcrições entrevista por entrevista e palavras por palavra mapa a mapa;
- c. Mapeamento de temas generalistas frequentes nas falas e mapas dos participantes;
- d. Identificação da ideia central do tema mapeado;
- e. Criação do código - usando verbo flexionado no gerúndio para transmitir a ação da atitude do participante entrevistado;
- f. Releitura dos trechos e expressões dos mapas de acordo com o tema a que pertenciam;
- g. Aplicação do código descritivo criado no trecho e expressão do mapa;
- h. Reconhecimento da frequência de ocorrência de cada código em todo material.

Por fim, foram obtidos 10 códigos descritivos que sintetizam a ideia e atitude dos participantes em suas falas e palavras escolhidas para o mapa. Os CD e suas respectivas ocorrências no material analisado estão listados na tabela 3, a seguir.

Tabela 3 - Códigos descritivos gerados

Códigos Descritivos	Ocorrência
CD - Definindo privacidade	62
CD - Expressando familiaridade	59
CD - Levantando conceitos	44
CD - Questionando a UX	42
CD - Abordando hábitos digitais	30
CD - Identificando riscos	28
CD - Revelando sentimentos	24
CD - Indicando aprendizado	22
CD - Demonstrando falta de conhecimento	16
CD - Explicando por comparações	15

Fonte: elaborado pela autora, 2025.

Diversos trechos de fala, por vezes, apresentaram características de mais de um código. Assim, esses trechos foram rotulados por dois ou até mais códigos. A identificação de mais de um código contribuiu, de certa forma, para o cruzamento de ocorrências entre os códigos.

Além disso, sugere que, em certos aspectos, o que foi dito ou escrito pelo participante possui camadas de significados além daquilo que lhe foi perguntado inicialmente. Após a criação dos dez códigos descritivos, os trechos que pertenciam a cada CD passaram por um novo processo de análise.

5.1.2 Codificação analítica

Na segunda etapa, a codificação analítica, o procedimento adotado foi analisar cada código descritivo para criação de códigos analíticos (CA). A intenção com a criação de uma segunda categoria de codificação era aprofundar aquilo que os participantes já descreviam de forma generalizada em seus relatos. Os códigos analíticos não apenas identificaram como especificaram sobre o que o participante estava falando quando definia a privacidade, por exemplo.

Os passos seguidos para esse processo foram os seguintes:

- a. Seleção das ocorrências de cada Código Descritivo (CD);
- b. Leitura criteriosa das ocorrências pertencentes a um mesmo CD;
- c. Mapeamento dos assuntos específicos mencionados que se repetiam no CD ou extremamente específicos que não se repetiam;
- d. Identificação da categoria do assunto;
- e. Criação do Código Analítico (CA) de acordo com a categoria identificada ou termo extremamente específico usado pelo participante;
- f. Reconhecimento da frequência de ocorrência de cada CA em todas as ocorrências do CD;
- g. Refinamento dos códigos analíticos para verificação de possível duplicidade e exclusão dos códigos cujas síntese se repetia.

A partir do processo de codificação analítica, foram obtidos, em um primeiro momento, 86 códigos analíticos. Após refinamento e verificação da duplicidade da síntese do código, permaneceram 79 códigos analíticos. Eles serão detalhados em seguida no processo de descrição completa dos resultados.

5.1.3 Descrição completa

Esta seção aborda a descrição completa dos códigos analíticos a partir de como eles se distribuem nos códigos descritivos. O passo é nomeado por Creswell

(2014), Gibbs (2009) e Gil (2021) de descrição exaustiva. Ele é fundamental para interpretar os resultados obtidos pela codificação, de acordo com os autores.

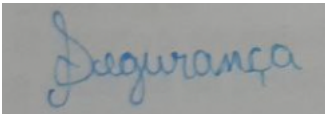
A descrição consiste em um quadro para cada código descritivo contendo os códigos analíticos que pertencem a ele, as ocorrências e o traço. Este último corresponde a amostras de falas dos participantes e expressões do mapa que determinaram a criação do CA.

Palavras ou locuções marcantes aparecem em negrito. As palavras e expressões escritas pelos participantes nos mapas também estão no quadro. Por vezes o trecho apresenta mais de um termo destacado. Isso significa que o mesmo trecho corresponde também a outros códigos analíticos dentro do mesmo código descritivo ou de outros códigos analíticos de códigos descritivos diferentes.

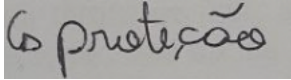
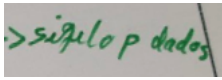
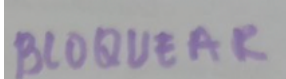
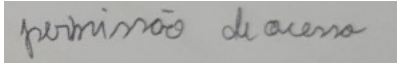
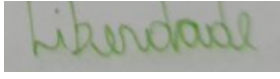
- **CD - Definindo a privacidade**

Este código descritivo aborda a resposta direta dos participantes à primeira pergunta da entrevista. O que faz dele o código descritivo com mais ocorrências. Isso acontece em função das definições atribuídas nos mapas mentais e dos participantes que levantaram mais de uma definição em suas falas. No quadro 10, os 12 códigos analíticos criados para o CD.

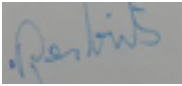
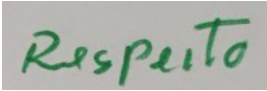
Quadro 10 - Códigos analíticos e traços do CD - Definindo a privacidade

CD - Definindo privacidade	63	Traço
CA - Pessoal Os participantes relacionam privacidade ao pertencimento. Ou seja, algo deles.	19	“Só diz respeito a mim e outros não” (E1 - F - 60 a 64) “Na internet...tipo assim, tem certas coisas que eu quero manter só pra mim...” (E8 - F - 20 a 24) – algo pessoal – (E22 - F - 30 a 34) “A privacidade de dados é a garantia de que os dados que eu fornecer para um site ou plataforma estarão protegidos” (E22 - F 30 a 34)
CA - Segurança Entendem como uma garantia ou segurança que eles têm sobre as próprias informações.	13	“É a garantia de que as informações sensíveis, inseridas em meio digital estarão seguras” (E24 - M - 40 a 44)  (E7 - M - 25 a 29)

Quadro 10 - Códigos analíticos e traços do CD - Definindo a privacidade

CA - Proteção Entendem como a proteção que garante a segurança das suas informações.	11	“Eu penso que seja proteção dos dados que a gente utiliza no ambiente digital” (E3 - M - 25 a 29) “Privacidade é você ter a possibilidade de ter algumas informações suas guardadas, mas você não quer estar ao público no caso, sabe? Seria o contrário” (E12 - F - 20 a 25)
		 (E3 - M - 25 a 29)
CA - Intimidade Entendem como íntimo sobre eles enquanto indivíduos.	10	“E privacidade pra mim é a gente não expor a coisa da gente. Isso, não expor o outro...” (E1 - F - 60 a 64) “Privacidade é ter segurança dos nossos...como posso te dizer... nossos momentos íntimos” (E7 - M - 25 a 29) “Na internet...tipo assim, tem certas coisas que eu quero manter só pra mim...” (E8 - F - 20 a 24)
CA - Confidencial Entendem como informações que eles querem manter secretas ou sigilosas.	11	“Privacidade é algo que tu esconde. Privacidade é uma coisa que tu não quer que outra pessoa queira saber, entendeu?” (E19 - M - 45 a 49)  (E21 - F - 60 a 64)
CA - Não acessível Algo que precisa de permissão para ser acessado, algo que deve ser bloqueado.	7	 (E17 - M - 20 a 24) permissão — (E22 - F - 30 a 34)  (E3 - M - 25 a 29)
CA - Liberdade O ato de ser livre e ter autonomia sobre as próprias ações.	6	“Privacidade pra mim é ter liberdade de fazer o que eu quero no momento que eu quero...” (E4 - F - 60 a 64) “Acho que é como se fosse uma liberdade que a gente tem” (E20 - M - 40 a 44)  (E16 - F - 25 a 29)

Quadro 10 - Códigos analíticos e traços do CD - Definindo a privacidade

CA - Direito Um direito assegurado por lei sobre si mesmos, próprias ações e informações.	5	“Nossa, privacidade... acho que é o direito de manter as minhas... de fazer o que eu quiser com as minhas próprias informações sem interferência dos outros. É o domínio e o direito que eu tenho sobre aquilo que diz respeito a mim. Que hoje, muitas vezes, isso se perde. Acho que é isso” (E13 - F - 30 a 34) “Eu entendo por privacidade... quando meu direito era assegurado de fazer aquilo que eu quero sem interferência de ninguém. Ou seja, é algo que eu faço e que eu não quero, e eu posso ter esse direito de não querer, que uma outra pessoa faça ou saiba do que eu estou fazendo” (E17 - M - 20 a 24) — direito — (E22 - F - 30 a 34)
CA - Inexistente Acreditam que, no contexto atual, a privacidade não existe mais.	4	“sobre privacidade de dados e tals... tipo assim, eu acredito que a gente meio que tipo, não tem” (E14 - F - 25 a 29). “Considero ser um direito que tenho enquanto indivíduo, de ter em sigilo meus dados e informações pessoais. Vez ou outra me pergunto se é possível ter 100% de privacidade digital... Eu suponho que não” (E25 - M - 45 a 49)
CA - Restrito Algo de acesso seletivo.	4	 (E11 - M - 30 a 34) — restrito — (E22 - F - 30 a 34)
CA - Não pode ser invadido Entendem como cordialidade com o próximo.	2	“A privacidade é não invadir, digamos assim. De certa forma, é o espaço do outro” (E15 - M - 20 a 24)
CA - Respeito Entendem como qualidade de caráter sentimental.	2	“Respeito... né? Privacidade é uma coisa assim, nossa, íntima” (E18 - F - 30 a 34)  (E21 - F - 60 a 64)

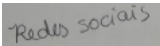
Fonte: elaborado pela autora, 2025.

Os participantes demonstraram entender a privacidade enquanto conceitos mais diretos, como proteção e segurança, por exemplo. Outras classificações remetem a significados menos diretos como não acessível, não pode ser invadido, respeito e liberdade.

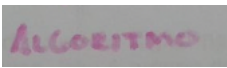
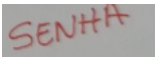
- **CD - Expressando familiaridade**

Neste CD, os participantes abordaram exemplos práticos variados para demonstrar que estavam cientes sobre o tema da entrevista. Para isso usaram termos mais específicos, como algoritmos e base de dados. Mas principalmente, fizeram conexão com redes sociais e demais elementos da internet. Como resultado, foram obtidos os 16 códigos analíticos a seguir (quadro 11).

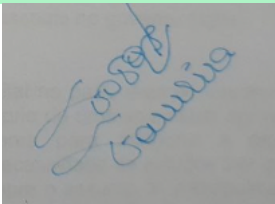
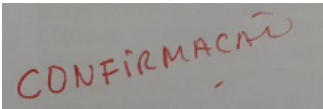
Quadro 11 - Códigos analíticos e traços do CD - Expressando familiaridade

CD - Expressando familiaridade	59	Traço
CA - Redes sociais Citam redes sociais famosas ou o próprio conceito de redes sociais.	14	“Eu quero comprar e o Instagram começa a me mostrar anúncios de empresa de acordo com que eu pesquisei então meio que tá compartilhando uma informação minha que é o interesse meu” (E3 - M - 25 a 29) “Usando o Instagram como exemplo... privacidade para mim no Instagram seria, por exemplo, ele não ter acesso ao meu WhatsApp. Tem também a questão do Facebook, isso tudo, a minha privacidade nos meios digitais” (E16 - F - 25 a 29)
		 (E15 - M - 20 a 24)
CA - Tipos de dados Especificam o tipo de dado ou citam o conceito meus dados pessoais.	11	“Mas aí às vezes não é tudo que eles pedem. Às vezes é uma coisa... a respeito de CPF, eu fico assim [com receio], mas aí eu acabo botando” (E18 - F - 30 a 34) “é só minha. Assim... meus dados, meu endereço, meu número do meu CPF, meu cartão...” (E22 - F - 60 a 64)
		“Tipo assim, o digital hoje em dia faz parte da nossa vida quase 90%. Tem muita coisa que é ligada ao digital” (E7 - M - 25 a 29)
CA - Ambiente digital Contextualizam a privacidade com auxílio do conceito ambiente digital	9	“mas dentro do contexto digital, hoje, isso está muito mais difícil, porque informações sobre nós são solicitadas o tempo inteiro” (E13 - F - 30 a 35)
		“até de quando eu só penso, às vezes eu nem falo, eu só penso e aí já vem um anúncio da coisa e eu fico, meu Deus do céu, até no meu cérebro eles não estão já. Ele vai pegando os dados e faz, enfim...” (E12 - F - 20 a 24)
CA - Coleta de dados Reconhecimento sobre dados pessoais sendo recolhidos de alguma forma.	9	“Eu já vi, mas não desse termo assim. Aí tem aceitar. Quando eu entro no Google. É porque é tipo como eles pedem lá, né? E eu dou. Eu estou ciente de que eles estão coletando lá meus dados” (E17 - F - 30 a 34)
		— coleta de dados (E25 - M - 45 a 49)

Quadro 11 - Códigos analíticos e traços do CD - Expressando familiaridade

CD - Expressando familiaridade	59	Traço
CA - Celular Conectam o uso do celular à privacidade de dados	8	“Eu uso o meu celular, a era digital, como eu estou te dizendo, veio para ajudar, mas também veio para... Aí a gente tem que ter muito cuidado” (E6 - F - 55 a 60)
CA - Ações do usuário Fazem referência às próprias ações pessoais ao se depararem com questões de privacidade	7	“Eu gosto muito de registrar fotos minhas. Minhas solicitação eu não... Eu não aceito. Eu vou procurar quem é... Quem é os amigos deles se tem alguém comigo. Eu sou muito precária [precavida] com isso” (E6 - F - 55 a 60) “Se não aceitar, a gente não tem a página completa de tudo aquilo que a gente está procurando, só aquele produto específico. Aí, quando aceita, aparece várias opções” (E20 - M - 40 a 44) “essa questão dos cookies, né, que eu acho extremamente irritante, todo santo site, você entrar e ter que decidir se aceita ou não” (E13 - F - 30 a 34)
CA - Sites Reconhecem ações dos sites.	7	“os dados são armazenados em bancos e são utilizados pra saber mais de você e principalmente oferecer anúncios e propagandas baseados no seu perfil, nos seus interesses, nas coisas q pesquisa e os sites que visita” (E26 - F - 18 a 19)
CA - Algoritmo Usam o termo algoritmo para desenvolver a ideia.	4	“gente lembra logo da questão do aprendizado dos algoritmos, né, que ficam pegando as nossas informações. Qualquer informação, né?” (E15 - M - 20 a 24)  (E12 - F - 20 a 24) “Outra pessoa não tem acesso aos seus dados, assim, que podem ter uma senha de bloqueio [bloqueio] para a pessoa não conseguir ver outras coisas” (E9 - F - 45 a 49)
CA - Senhas Conectam a ideia ao uso de senhas de proteção	4	 (E17 - M - 20 a 24) “A depender do meio inserido, serve para uma base de dados que tem como uma das finalidades marketing digital” (E24 - M - 40 a 44)
CA - Bancos de dados Síntetizam o assunto à existência de bancos de dados	3	bancos de dados  (E26 - F - 18 a 19)

Quadro 11 - Códigos analíticos e traços do CD - Expressando familiaridade

CD - Expressando familiaridade	59	Traço
CA - Fotos Conectam a ideia da proteção às imagens pessoais	3	 (E6 - F - 50 a 60)
CA - Instituições financeiras Conectam a ideia da proteção aos bancos ou banco digital.	3	<i>“Banco não te manda mensagem, né? E eu sou sempre precária [precavida]. Eu sou muito precária com celular, com meu banco digital”</i> (E6 - F - 50 a 60) <i>“Tem muita coisa que é ligada ao digital, tipo a conta bancária, essas coisas assim, dados pessoais”</i> (E7 - F - 25 a 29) <i>“A gente vai no piloto automático e a gente sabe. Porque tipo assim, que nem câmeras de segurança pra filmar assim na rua, né?”</i> (E14 - F 25 a 29)
CA - Vigilância Conectam a ideia a monitoramento, seja por câmeras de segurança ou dispositivos próprios.	3	<i>“Eu penso assim que tudo o que eu tenho no meu celular ou algo que eu escrevo, que eu guardo ou mando para uma pessoa, fica tudo aqui para mim. Mas eu acho, eu tenho quase certeza que isso não existe no celular, é monitorado 24 horas. Como agora que criaram essa atendente artificial”</i> (E20 - M - 40 a 44)
CA - Computador Conectam o uso do computador à privacidade de dados	2	<i>“autonomia, né? relacionado aos dados... Pode ser movimentação bancária, pode ser redes sociais, até o próprio... utilização tanto de computador como celular”</i> (E11 - M - 30 a 34)
CA - Inteligência artificial Usam o termo inteligência artificial para desenvolver a ideia.	2	<i>“eu tava vendo que agora, né, no WhatsApp o que eu tenho guardado... então eu vi lá que eles tipo, tem inteligência artificial, né?”</i> (E14 - F 25 a 29)
CA - Autenticação Relacionam a necessidade de autenticar e confirmar a veracidade ao fornecimento de dados.	1	 (E17 - M - 20 a 24)

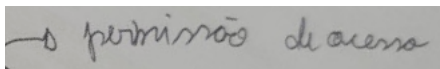
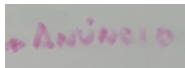
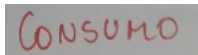
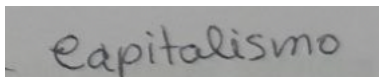
Fonte: elaborado pela autora, 2025.

A ocorrência considerável de citações e exemplos específicos, assim como a variedade de códigos analíticos dentro deste CD sugere que o assunto não é estranho para os participantes. Inclusive sendo o código descritivo com a maior variabilidade de códigos analíticos. Ou seja, estes participantes, em geral, têm consciência sobre as atividades e elementos que permeiam a sua privacidade. Dessa forma, eles foram capazes de descrevê-los e refleti-los.

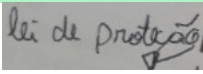
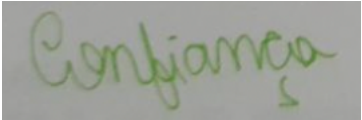
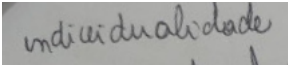
- **CD - Levantando conceitos**

O CD apresenta tópicos mencionados pelos próprios participantes que podem ser discutidos e teorizados de modo mais formal. Esses códigos analíticos, de certo modo, significam que o participante ultrapassou o nível de familiaridade que caracterizava os códigos analíticos de expressão de familiaridade a partir do momento em que suas reflexões envolviam dicotomias e complexidades sociais. Onze códigos analíticos foram formulados para esse CD, conforme o quadro 12.

Quadro 12 - Códigos analíticos e traços do CD - Levantando conceitos

CD - Levantando conceitos	44	Traço
CA - Poder de escolha Reflexão sobre ser condicionado a permitir ou ceder acesso às próprias informações	10	<i>“Ou você aceita ou você não usa. Então não é opção” (E2 - M - 60 a 64)</i> <i>“informações sobre nós são solicitadas o tempo inteiro, a gente, às vezes, só consegue acessar determinados serviços a partir do momento que a gente fornece as nossas próprias informações” (E13 - F - 30 a 34)</i>  (E3 - M - 25 a 29)
CA - Anúncios e propaganda Reflexão sobre dados pessoais serem utilizados como meio para marketing, marketing digital, anúncios, propaganda e publicidade.	6	 (E12 - F - 20 a 24) marketing (E26 - F - 18 a 19)
CA - Consumo e produto Reflexão sobre dados serem apenas produtos frente à realidade capitalista para influenciar a forma de consumir.	6	<i>“Ele vai pegando os dados e faz, enfim, aí eu penso muito nisso, que seria esse repertório de coisas que a gente faz, de coisas que a gente gosta de ouvir como internet e que pode ser utilizado pra vários meios, como esse de público e de conseguir... é vender melhor ou até mostrar uma ideia que cria as bolhas de que a gente fica dentro também um tipo de conteúdo vai sempre vir pra mim” (E12 - F - 20 a 24)</i>  (E13 - F - 30 a 34)  (E15 - M - 20 a 24)
CA - Controle Reflexão sobre a ausência de controle sobre o que acontece com as próprias informações.	6	<i>“A gente não tem mais um controle sobre isso. Às vezes por falta de clareza” (E13 - F - 30 a 34)</i> <i>“Não sei ao certo o que pode ocorrer com meus dados, mas por ora deveria ser usado apenas para aquilo que eu concordo” (E22 - F - 30 a 34)</i>

Quadro 12 - Códigos analíticos e traços do CD - Levantando conceitos

CD - Levantando conceitos	44	Traço
CA - Conformidade Reflexão sobre a privacidade enquanto algo legitimado a partir da lei.	4	 (E3 - M - 25 a 29) — legalidade (E22 - F - 30 a 34)
CA - Direitos e Deveres Reflexão a respeito das implicações para o direito e o dever dos usuários.	4	“Como esses dados são tratados pelas plataformas e inclusive o próprio governo ? Pelas mãos de quantas pessoas meus dados passam também fazem parte do pacote de perguntas . Neste assunto, existe relação de Direitos versus Deveres ?” (E25 - M - 45 a 49)
CA - Proteção Reflexão sobre a proteção não como característica da privacidade, mas conceito interligado ao consentimento.	4	“eu acho que a proteção vem nesse sentido de não... não é nem não utilizar , mas utilizar de acordo com que eu consenti na época que eu toda toda plataforma , tem que ter meu consentimento ” (E3 - M - 25 a 29)
CA - Confiança Reflexão sobre a confiança do titular dos dados e a confiança no operador e controlador dos dados.	3	“isso pode ser interpretado , no meu ponto de vista, como um ato de má fé por parte das empresas que administram os dados ” (E26 - F - 18 a 19)  (E16 - F - 18 a 19)
CA - Individualidade Reflexão sobre a privacidade de dados ser legitimamente fundamental ao direito do indivíduo, do sujeito, do cidadão.	2	 (E3 - M - 25 a 29) — legitimidade (E22 - F - 30 a 34)
CA - Informação Reflexão sobre a importância de informar o cidadão sobre os fins da coleta de dados.	2	informação (E23 - F - 45 a 49) finalidade (E24 - M - 40 a 44)

Fonte: elaborado pela autora, 2025.

Este CD também permitiu uma variabilidade considerável de códigos analíticos. Isso permite inferir que, por vezes, os participantes não só respondiam as perguntas ou reagiam à pauta da entrevista como apresentavam suas próprias ponderações de forma independente ao tentar identificar o que sabiam sobre o assunto.

- **CD - Questionando a UX**

Neste CD, os participantes trouxeram relatos claros sobre suas divergências em relação à interação com as confirmações de consentimento e uso dos cookies. Para eles, a tarefa não é clara, muitas vezes cansativa e frustrante e difícil de entender. Também para eles, tais interfaces não parecem ser confiáveis ou transparentes. O quadro 13 mostra os seis códigos analíticos obtidos.

Quadro 13. Códigos analíticos e traços do CD - Questionando a UX

CD - Questionando a UX	42	Traço
CA - Cansativo para o usuário Argumentam sobre uma experiência insatisfatória uma vez que entendem que são obrigados a concordar para prosseguir.	16	<i>“você querer uma coisa e na hora você ser obrigado a fazer outras que você não sabe nem o que está fazendo, [só] sabe que se você não fizer aquilo ali, não vai”</i> (E2 - M - 60 a 64)
CA - Indução ao consentimento Argumentam que consentimento é condicionado.	12	<i>“Mas eu fico me perguntando se não poderia evitar isso desde antes, esse site precisa de fato rastrear as minhas preferências, dá pra entender onde eu quero chegar?”</i> (E13 - F - 30 a 34)
CA - Não é transparente Argumentam que a experiência fornecida não é clara sobre o que acontece com os dados.	10	<i>“aquilo é chato. Até o momento que tu aperta sem querer, aí já foi, você já consentiu”</i> (E6 - F - 55 a 60)
CA - Não entende o que acontece Experiência não parece ser clara sobre o porquê das ações	6	<i>“e muitos sites nem.. nem oferecem a opção de negar, né? Oferecem só para a gente ler e a gente acaba concordando para não ler, né?”</i> (E15 - M - 20 a 24)
CA - Não parece confiável Experiência não parece segura ou transmite confiança	4	<i>“E isso não é consentimento que você não sabe nem para quê, nem porque nem se vai ser usado ou não”</i> (E2 - M - 60 a 64)
CA - Não sabe o que fazer Experiência não parece ser explicativa e impede o usuário de entender como agir	4	<i>“Quem é que tem acesso a esses dados? Só o pessoal, o pessoal que é quem cuida do site ou qualquer pessoa tem acesso?”</i> (E7 - M - 25 a 29)
		<i>“Por exemplo, esse tipo de botão que você falou. Entende? Mas eu tenho muito medo de clicar em algo errado, não entender”</i> (E4 - F - 60 a 64)
		<i>“Eu tenho medo de apertar qualquer coisa e eles me roubarem. Eu nunca aperto”</i> (E5 - F - 50 a 55)
		<i>“mas eu não sei aonde procurar. Eu não sei o que fazer”</i> (E2 - M - 60 a 64)

Fonte: elaborado pela autora, 2025.

Em geral, os participantes da *sketch interview* não demonstram ter uma experiência do usuário agradável ao interagirem com políticas de privacidade, termos de consentimento e *cookies*. De acordo com os relatos, as ações demandadas são encaradas como irritantes e chatas. Principalmente por comprometerem o uso pleno pois inibem os participantes de prosseguir nas tarefas.

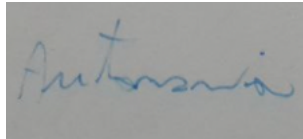
• CD - Abordando hábitos digitais

Este código descritivo faz referência a como os participantes se comportam no ambiente digital ou situações que influenciam suas atitudes nele, conforme o quadro 14. Seus hábitos podem ser orientados desde a sua postura como internautas ativos ou até por serem usuários no piloto automático. Aqui foram desenvolvidos cinco códigos analíticos.

Quadro 14 - Códigos analíticos e traços do CD - Abordando hábitos digitais

CD - Abordando hábitos digitais	30	Traço
CA - Disponibilizar na internet Abordam hábitos relacionados ao uso na internet, envolvendo desde inserir informações ou seu consumo delas.	10	<i>“de ter o direito de, sobre as informações que eu tenho, que eu disponibilizo na internet, o que que eu posso ou não fazer com isso, e que deveria ser a mim”</i> (E13 - F - 30 a 34) <i>“que seria esse repertório de coisas que a gente faz, de coisas que a gente gosta de ouvir na internet e que pode ser utilizado pra vários meios”</i> (E12 - F - 20 a 24)
CA - Falta de atenção Demonstram desatenção ou ignoram ações tipicamente digitais.	7	<i>“Nunca prestei atenção. Por exemplo, esse tipo de botão que você falou”</i> (E4 - F - 60 a 64) [Ler o termo de consentimento] <i>“tadinho? Não, não, não. Quem é esse? Se eu for fazer uma estatística, é de 1 em 1.000.000”</i> (E11 - M - 30 a 34)
CA - Piloto automático Ações estão submetidas ao modo automático da experiência, seja por pressa ou suposição da não necessidade de atenção.	5	<i>“A gente meio que sabe, mas a gente meio que não sabe também, né? A gente vai no piloto automático e a gente sabe”</i> (E14 - F - 25 a 29) <i>“Na pressa para acessar o que preciso, como uma notícia, ou um site qualquer, coloco aceitar ou concordo para otimizar meu tempo”</i> (E22 - F - 30 a 34)
CA - Mediante desafios Hábito digital tem algum caráter desafiador para o usuário. Seja por ser considerado difícil ou não compreensível.	5	<i>“depois clique aqui para continuar... na outra parte eu não sei. Tem muito disso na internet. Tem muita coisa que eu não entendo”</i> (E5 - F - 50 a 55) <i>“Eu preciso de alguma coisa assim de digital. Sempre peço para o meu menino fazer, para a minha filha fazer”</i> (E2 - M - 60 a 64)

Quadro 14 - Códigos analíticos e traços do CD - Abordando hábitos digitais

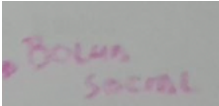
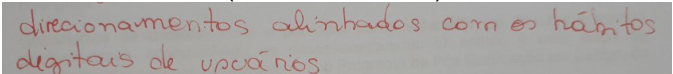
CD - Abordando hábitos digitais	30	Traço
CA - Imposição x autonomia Refletem como o hábito está condicionado à imposição do compartilhamento impactando a autonomia do usuário para acessar os próprios interesses.	5	<i>“Se não aceitar, a gente não tem a página completa de tudo aquilo que a gente está procurando”</i> (E20 - M - 40 a 44)  (E11 - M - 30 a 34)

Fonte: elaborado pela autora, 2025.

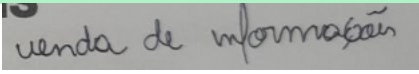
• CD - Identificando riscos

O CD trata de assuntos que podem ser caracterizados como ameaças. Os participantes abordaram temas como crimes, fraudes e vazamentos. De certa forma, as pessoas apontaram para situações que causam preocupação ou desconforto em relação à violação da privacidade dos dados pessoais. No quadro 15, todos os sete códigos analíticos gerados em função desse CD.

Quadro 15. Códigos analíticos e traços do CD - Identificando riscos

CD - Identificando riscos	28	Traço
CA - Violação Identificação do risco está atrelada a forma como os dados seriam obtidos, por meio de violação, <i>hacking</i> .	9	<i>“ah, sei lá, um hacker... alguma coisa minha pra usar meu nome, minha nossa. Eu tenho muito medo disso”</i> (E4 - F - 60 a 64)  (E4 - F - 60 a 64)
CA - Exposição e vazamento Identificação do risco a partir das ameaças que a exposição da vida na internet e redes sociais podem trazer.	7	<i>“não sei, assim, se vazar na internet tem um grande estrago na vida da pessoa, eu acho”</i> (E9 - F - 45 a 49) <i>“ela veio pra destruir... porque tu já pensou, tu tem um dados teu, de repente cai na rede social”</i> (E6 - F - 55 a 60)
CA - Manipulação Identificação do risco a partir da finalidade para qual os dados podem ser usados, como influenciar hábitos e preferências sociais.	5	 (E12 - F - 20 a 24)  (E13 - F - 30 a 34)

Quadro 15. Códigos analíticos e traços do CD - Identificando riscos

CD - Identificando riscos	28	Traço
CA - Comercialização Identificação do risco em função da aquisição financeira e lucro a partir das informações do indivíduo.	4	 (E3 - M - 25 a 29) <i>“Eu acho que pode ser armazenado, né? Tipo um banco de dados e vendido mais ou menos assim vendido. Acho que para alguém em algum espaço do mundo, essas informações são importantes”</i> (E15 - M - 20 a 24)
CA - Crimes Identificação do risco em função do uso de dados para prática de crimes, como golpes e fraudes	4	[se] <i>“outra pessoa pegar ela pode... ela pode roubar o que tiver lá e transferir para a conta dele. Sei lá, pode fazer maldade com a pessoa”</i> (E10 - M - 40 a 44) <i>“vai terminar em consumo ou de alguma forma... ser utilizado para obter algum recurso, seja através de golpes”</i> (E13 - F - 30 a 34)
CA - Desinformação Reconhecimento do risco envolvendo a falta de ciência em relação ao tratamento dos dados.	2	<i>“quase ninguém lê esse... eu acho que ninguém lê. Eu pelo menos nunca li os termos, então não sei. Eu vou estar lá concordando, sem saber o que é, entendeu? Isso é ruim”</i> (E17 - M - 20 a 24)

Fonte: elaborado pela autora, 2025.

• CD - Revelando sentimentos

Neste código descritivo, os participantes falaram expressamente sobre o medo que sentem em relação a possíveis violações dos dados digitais. Em geral, eles demonstraram sentimentos de cunho negativo, como incômodo em relação à obrigação de consentir, ou frustração por não entenderem por completo essa situação. No quadro 16, os quatro códigos analíticos que aprofundam esse CD.

Quadro 16 - Códigos analíticos e traços do CD - Revelando sentimentos

CD - Revelando sentimentos	25	Traço
CA - Insegurança Manifestam receio e inseguranças relacionados a sua experiência, seja no dispositivo ou interface.	13	<i>“Eu tenho medo de apertar qualquer coisa e eles me roubarem. Eu nunca aperto”</i> (E5 - F - 50 a 55) <i>“Eu já ouvi falar, inclusive que que o celular grava, grava informações assim da nossa fala no dia a dia, né? E que a câmera também. Eu já ouvi falar nisso. Eu fico preocupado com essas coisas. Mas eu já ouvi falar. E é isso que eu lembro”</i> (E15 - F - 20 a 24)
CA - Incômodo Manifestam irritação em relação à persistência e à forma como o consentimento é obtido.	9	<i>“aquilo é chato. Até o momento que tu aperta sem querer, aí já foi, você já consentiu”</i> (E6 - F - 55 a 60) <i>“Cookie...é... assim... aí eles seguem insistindo... mesmo que você aceite, eles ficam mandando... é chato demais”</i> (E19 - M - 45 a 49)

Quadro 16 - Códigos analíticos e traços do CD - Revelando sentimentos

CD - Revelando sentimentos	25	Traço
CA - Frustração Manifestam frustração pois identificam ausência de opção e escolha nas suas experiências	5	<i>"Eu só quero, sei lá, ler uma notícia por que ele precisa rastrear os meus hábitos de leitura de notícia para melhorar a minha experiência nesse site, sabe?"</i> (E13 - F - 30 a 34) <i>"Ou você aceita ou você não usa. Então não é opção"</i> (E12 - M - 60 a 64)
CA - Medo Manifestam medo pois a experiência não parece transmitir-lhes segurança	3	<i>"Mas eu tenho muito medo de clicar em algo errado, não entender. Ah, sei lá, um hacker. Alguma coisa minha pra usar meu nome, minha nossa. Eu tenho muito medo disso"</i> (E4 - F - 60 a 64)

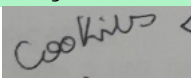
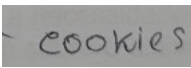
Fonte: elaborado pela autora, 2025.

As ocorrências desses códigos analíticos co-ocorreram em diversos momentos com os códigos analíticos do CD - Questionando a UX. Os participantes não apenas estavam reconhecendo a própria experiência como insatisfatória, mas revelando como se sentem a respeito disso.

• CD - Indicando aprendizado

O CD aborda atitudes dos participantes em relação às informações apresentadas. Alguns problematizaram o tema e outros trouxeram reflexões. Os participantes conseguiram elaborar conclusões próprias a partir do que foi apresentado, ainda que indiretamente. No quadro 17, os cinco códigos analíticos.

Quadro 17 - Códigos analíticos e traços do CD - Indicando aprendizado

CD - Indicando aprendizado	21	Traço
CA - Destaca nova informação Ressaltam qual tópico chamou atenção a partir da entrevista.	13	 (E3 - M - 25 a 29)  (E15 - M - 20 a 24)
CA - Elabora conclusão própria Ressaltam não apenas o tópico, mas conseguem falar a respeito dele.	9	<i>"A proteção de dados deve ser mais segura, visto que há pessoas invadindo sistemas oficiais do governo e "furtando" dados sensíveis dos cadastros para aplicar golpes financeiros"</i> (E23 - F - 45 a 49) <i>"Eu não sabia que tinha ficado disponível para qualquer momento. Que a gente tem acesso a esses termos de uso o tempo inteiro. Pra mim era vir uma vez e tchau tchau"</i> (E3 - M - 25 a 29)

Quadro 17 - Códigos analíticos e traços do CD - Indicando aprendizado

CD - Indicando aprendizado	21	Traço
CA - Problematisa ou reflete Ressaltam o tópico ou assunto em geral a partir de uma proposição sobre o assunto ou predição.	5	<i>“Eu não sabia dessa lei. Eu não sabia. Eu não tinha conhecimento, porque todas as pessoas deveriam saber assim. A gente meio que sabe, mas a gente meio que não sabe também, né?”</i> (E14 - M - 25 a 29)
CA - Reconhece importância das informações Ressaltam positivamente as informações obtidas a partir da entrevista.	5	<i>[percebe que a proteção de dados e privacidade ao navegar e utilizar serviços na internet] “Ainda [está] engatilhando, mas vejo em um futuro próximo termos ótimos resultados quanto à segurança”</i> (E24 - M - 40 a 44) <i>“E não sabia que era para rastreio do site, então achei bem importante essas informações”</i> (E17 - M - 20 a 24) <i>“Foram um pouco difíceis de entender, mas são boas. São informações muito úteis”</i> (E21 - F - 60 a 64)
CA - Prevê mudança de comportamento Citam algum impacto a partir das informações obtidas a partir da entrevista.	1	<i>“Daqui pra frente, quero prestar mais atenção no que eu concordo e disponibilizo meus dados”</i> (E22 - F - 30 a 34)

Fonte: elaborado pela autora, 2025.

Estes códigos analíticos foram elaborados a partir do indicativo de aprendizado de alguns participantes durante o momento I. Mas principalmente a partir do que relataram os participantes que aceitaram colaborar no momento II, realizado semanas depois.

Os cookies foram citados duas vezes em mapas mentais e três vezes em falas por participantes diferentes. A importância da LGPD foi destacada cinco vezes por participantes diferentes. Das informações repassadas aos entrevistados, essas foram as duas mais lembradas no momento II.

• CD - Explicando por comparações.

Ao tentar explicar como percebiam a privacidade, por vezes os entrevistados recorreram a analogias para se fazerem entender. Eles optaram por comparar a privacidade a assuntos como a vida familiar, o casamento, a casa. O quadro 18 mostra os cinco códigos analíticos criados para entender as analogias dos participantes.

Quadro 18 - Códigos analíticos e traços do CD - Explicando por comparações

CD - Explicando por comparações	15	Traço
CA - Casa Associam privacidade ao ambiente casa	5	<i>“Gosto de chegar do meu serviço e para minha casa ter a minha privacidade” (E1 - F - 60 a 64)</i>
CA - Ler mentes Associam o rastreio de informações a adivinhar pensamentos	5	<i>“Uma vez até de quando eu só penso, às vezes eu nem falo, eu só penso e aí já vem um anúncio da coisa e eu fico, meu Deus do céu, até no meu cérebro eles não estão já” (E12 - F - 20 a 25)</i>
CA - Família Associam privacidade à dinâmica familiar	3	<i>“Um exemplo em casa é quando a gente tem nossa privacidade e a gente mora sozinho” (E14 - F - 25 a 29)</i>
CA - Notícias Associam privacidade a acontecimentos reais	3	<i>“Ultimamente a internet está uma coisa assim bombástica. Aqui mesmo aconteceu [cita caso que viralizou]. em minutos estava no mundo todo, Então não foi privado, foi aberto” (E5 - F - 50 a 55)</i>
CA - Casamento Associam privacidade ao casamento	2	<i>“Por exemplo, no caso, eu sou casado. A privacidade no casamento ela não existe. Agora, fora do casamento, ela já existe” (E20 - M - 40 a 44)</i>

Fonte: elaborado pela autora, 2025.

• CD - Demonstrando falta de conhecimento

Durante a entrevista, os participantes expressaram desconhecimento em relação ao assunto algumas vezes. Eles também expressaram alguma incerteza, pontuaram não ter ouvido falar sobre as leis ou saber para que, de fato, servem os *cookies*, por exemplo. Os sete códigos analíticos que compõem o CD aparecem no quadro 19, a seguir.

Quadro 19 - Códigos analíticos e traços do CD - Demonstrando falta de conhecimento

CD - Demonstrando falta de conhecimento	16	Traço
CA - Assume não saber Declaram não saber, entender ou conhecer o assunto e por isso não se acham aptos a desenvolver a resposta	8	<i>“Eu não tô lembrada agora nesse momento” (E1 - F - 60 a 64)</i>
CA - Leis Reconhecem que não tinham conhecimento sobre a LGPD	5	<i>“Não, não entendo... não, porque está fora do meu contexto” (E4 - F - 60 a 64)</i> <i>“eu não sabia que existia uma lei que regulava privacidade e regulava essa proteção de dados” (E15 - M - 20 a 24)</i> <i>“eu não sabia da lei” (E12 - F - 20 a 24)</i>

Quadro 19 - Códigos analíticos e traços do CD - Demonstrando falta de conhecimento

CD - Demonstrando falta de conhecimento	16	Traço
CA - Privacidade de dados digitais Declararam não saber, entender ou conhecer a expressão privacidade de dados digitais	5	<i>“Entendimentos meus são poucos. Pouquíssimos”</i> (E2 - M - 60 a 64)
CA - Cookies Reconhecem que não tinham conhecimento sobre a finalidade dos cookies	2	<i>“Nunca ouvi falar em privacidade de dados digitais”</i> (E10 - M - 40 a 44)
CA - Incerteza Usam expressões de incerteza e não desenvolvem a ideia	2	<i>“Não sabia ainda. Sim, eu pensava que era relacionada a lixo. Quando você navega muito, fica armazenado como se fosse na memória Ram”</i> (E10 - M - 30 a 34)
CA - Não compreende Reconhecem que o assunto não é estranho, mas assumem não entendê-lo.	2	<i>“É no celular, eu acho”</i> (E9 - F - 45 a 49)
CA - Desinteresse Reconhece que não teve interesse de pesquisar sobre a informação anteriormente.	1	<i>“Eu olho muito, Mas também não entendo o que é”</i> (E5 - F - 50 a 54)
		<i>“nunca busquei entender um pouquinho sobre, mas é algo que quando eu leio privacidade de dados digitais eu já tenho uma pequena noção do que se trata”</i> (E17 - M - 20 a 24)

Fonte: elaborado pela autora, 2025.

O código descritivo - demonstrando falta de conhecimento apresenta o menor número de ocorrências. De forma particular, todos os participantes conseguiram falar sobre o assunto e seguir os passos da entrevista.

Curiosamente, algo a se destacar é que, talvez por inibição, os participantes assumiam não saber no início da entrevista. Mas no decorrer dos passos da pauta eles pareciam estar familiarizados com os assuntos. Vide o nível de ocorrências do CD - Expressando familiaridade.

Os entrevistados que aceitaram participar do segundo momento da *sketch interview* relataram que o momento anterior, de sensibilização, contribuiu para ajudá-los a elucidar conceitos que já haviam percebido antes ao navegar na internet. Além disso, eles revelaram estar mais atentos para evitar o hábito de aceitar e concordar automaticamente com a coleta dos seus dados pessoais.

O objetivo desta parte da coleta de dados era cumprir o objetivo específico: conhecer percepções que usuários têm sobre privacidade de dados digitais. A partir dos códigos criados e as suas ocorrências, foi realizada uma síntese dessa percepção dos entrevistados.

Para os participantes da pesquisa, a privacidade de dados digitais é a segurança, a confidencialidade, e a garantia de que as informações deles não devem ser acessadas por qualquer um. E, principalmente um bem pessoal que eles esperam ser protegido

Por fim, pode-se dizer que esse objetivo foi mais do que alcançado. O instrumento *sketch interview*, mesmo com uma amostra pequena, possibilitou conhecer como essas pessoas vêem a privacidade. Ou seja, contribuiu no conhecimento e na resolução do problema de pesquisa.

E foram além. Afinal, por meio do relato dos entrevistados, outros tópicos foram levantados. Como assuntos relacionados à frustração em relação às experiências dos usuários e seus sentimentos. A seguir, os resultados obtidos via aplicação de questionários.

5.2 Questionário

Este instrumento obteve a participação de quarenta e dois respondentes (n=42). A partir da amostra obtida, os achados são descritos em seguida. Eles correspondem ao perfil dos participantes e a forma como as pessoas interagem com a privacidade nas interfaces do governo digital.

5.2.1 O perfil dos respondentes

Esta primeira parte da análise trata do perfil social dos participantes desta etapa da pesquisa. O maior grupo, vinte e duas pessoas, possui formação além da educação básica, divididas entre dez com ensino superior e doze com pós-graduação. A outra parte do grupo, correspondente a vinte pessoas, estudou até diferentes etapas da educação básica.

Desses participantes, dezessete pessoas possuem formação no ensino médio. Sendo esse último o nível de escolaridade com mais frequência entre todos os níveis. Uma pessoa concluiu todo o ensino fundamental (anos finais) e uma pessoa concluiu apenas os anos iniciais.

Um participante da pesquisa revelou não ter terminado o ensino fundamental I, tendo sido alfabetizado de modo incompleto. A tabela 4 corresponde ao quantitativo e variação do nível de escolaridade dos respondentes.

Tabela 4 - Nível de escolaridade dos respondentes

Nível de escolaridade	Frequência	Porcentagem
Não completou o Ensino Fundamental I	1	2,4%
Completou o Ensino Fundamental I	1	2,4%
Completou o Ensino Fundamental II	1	2,4%
Completou o Ensino Médio	17	40,5%
Completou o Ensino Superior	10	23,8%
Possui Pós-Graduação	12	28,6%

Fonte: elaborado pela autora, 2025.

Ainda que a maior parte dos participantes esteja no grupo que possui formação além da educação básica, a amostragem conseguiu alcançar pessoas com nível de escolaridade diferenciados. Isso possibilita a extração de informações de perspectivas heterogêneas. Quanto ao gênero dos participantes da pesquisa, vinte e um respondentes se identificaram com o feminino e vinte e um se identificaram com o masculino.

Quanto à idade, responderam ao questionário pessoas de 18 a 66 anos. A média da idade dos respondentes é de 43,88 anos com desvio padrão [DP] = 12,63, indicando uma dispersão moderada em torno da média. A mediana das idades é de 44 anos, apresentando uma distribuição simétrica. Não há idades extremas representando *outliers*. Portanto, infere-se uma heterogeneidade e uma distribuição equilibrada no intervalo da amostragem.

5.2.2 Resultados do questionário

O objetivo específico da aplicação do questionário é indicar como usuários do governo digital interagem com as políticas de privacidade e com os termos de consentimento. Por isso, foram propostas 35 perguntas (Apêndice F) em 5 etapas.

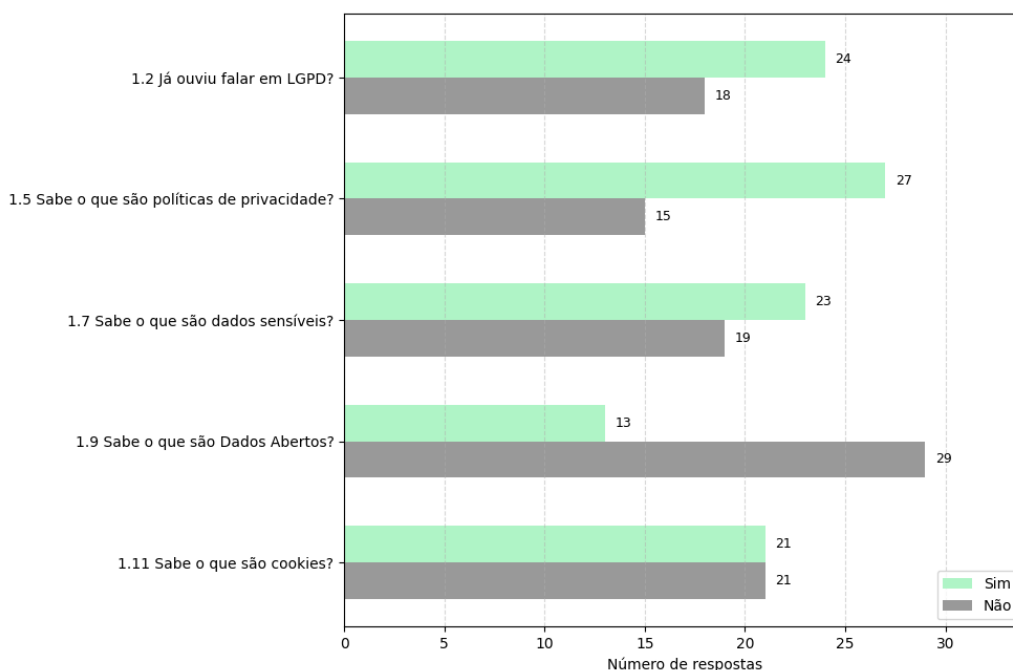
Eles puderam, não apenas apresentar um perfil dessas pessoas, mas indicar elementos que lhes são familiares. Assim como a sua frequência usando serviços de governo digitais e lacunas e pontos de atenção que possam contribuir à pesquisa.

Os primeiros questionamentos apresentados aos respondentes tratavam da sua familiaridade em relação a aspectos das políticas de privacidade apresentadas aos usuários. A eles foi perguntado se já tinham ouvido falar ou sabiam o que era

LGPD: vinte e quatro responderam positivamente; **políticas de privacidade:** vinte e sete disseram sim; **dados sensíveis:** vinte e três confirmaram que sabiam; **dados abertos:** treze disseram saber; e **cookies:** vinte e um afirmaram que sim.

A figura 22 compara as respostas positivas e as negativas em relação a familiaridade dos participantes com os temas.

Figura 22 - Nível de familiaridade dos participantes com os temas (n=42)



Fonte: elaborado pela autora, 2025.

Os números demonstram, em geral, que os respondentes estavam familiarizados com os assuntos LGPD e políticas de privacidade. Entretanto, vinte e nove deles disseram não saber o que são dados abertos. Quando questionados se sabiam da existência do órgão regulamentador da proteção de dados no Brasil, vinte e oito responderam “não”. Entre as quatorze pessoas que responderam sim, sete conseguiram indicar o nome correto.

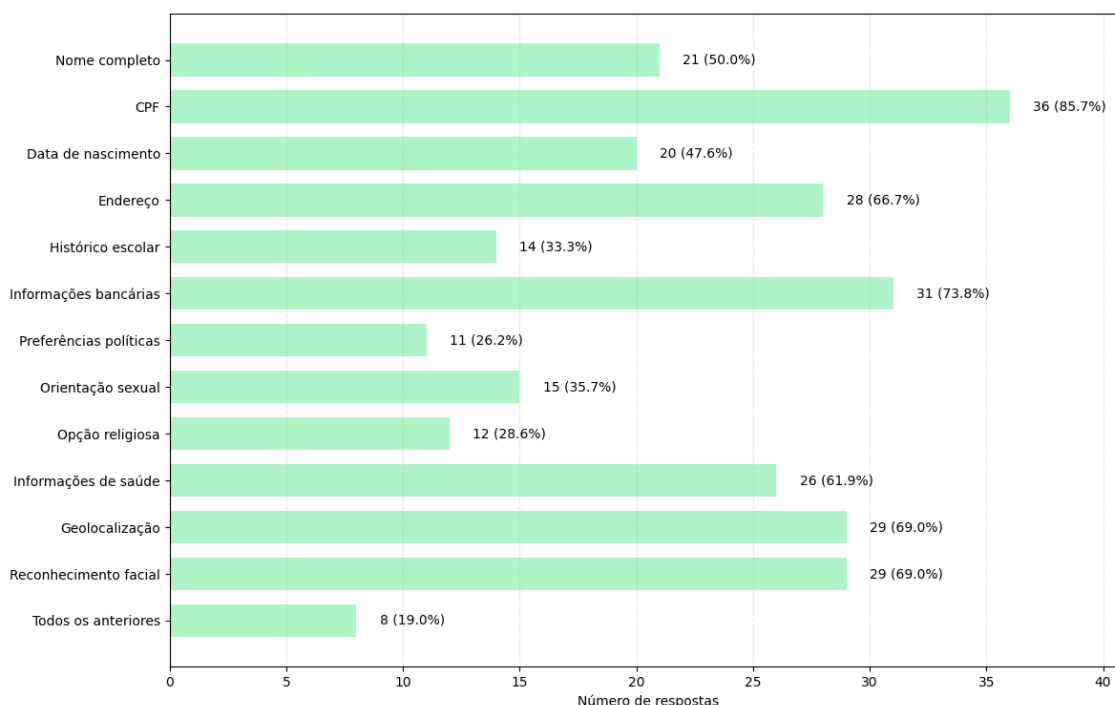
Aos que responderam sim, quando questionados se poderiam explicar o que são políticas de privacidade, classificaram-nas como: leis, políticas públicas, conjuntos de regulamentos, mecanismos de proteção, normas legais, garantias de segurança, confirmação de proteção, acordo entre as partes, etapa de uso em redes sociais e outros. De modo geral, as pessoas que disseram saber, apresentaram com suas palavras definições coerentes com a forma como as políticas de privacidade são apresentadas a elas.

Já em relação aos dados sensíveis, apesar de 54,8% responderem que sabem (n=23), quando confrontados com uma relação com tipos variados de dados, rotularam como dados sensíveis aqueles que são apenas pessoais. Dados pessoais comuns como nome completo, CPF, endereço foram identificados como sensíveis por vinte e um, trinta e seis e vinte e oito participantes, respectivamente. Informações bancárias, outro dado comum, foi apontado por trinta e uma pessoas (73,8% da amostra).

Dados sensíveis como opiniões políticas, opção religiosa e orientação sexual foram classificados por menos da metade dos participantes. São esses tipos de dados que podem implicar situações discriminatórias e de viés algorítmico. Entretanto, o dado sensível “reconhecimento facial” foi apontado por vinte e cinco participantes.

Informações de saúde e genéticas, outro tipo de dado sensível, foi indicado em vinte e seis respostas, mais da metade do total. A figura 23 apresenta a lista completa de tipos de dados relacionados.

Figura 23 - Percepção dos participantes sobre dados sensíveis (n=42)



Fonte: elaborado pela autora, 2025.

Em geral, dos 5 tipos de dados sensíveis disponíveis na lista com 12 opções totais, apenas 2 tipos de dados sensíveis foram indicados por mais de vinte (n=26 e n=29) pessoas. Em contrapartida, os 2 tipos de dados mais votados da lista são CPF

e informações bancárias. Considerando os relatos dos respondentes - durante a aplicação presencial - sugere-se que essa escolha se dê em função da insegurança, que os participantes sentem, em relação a golpes e fraudes atrelados a esse tipo de informação.

A maior parte da amostra (n=29) negou saber o que são dados abertos. Os treze participantes que responderam positivamente indicaram que são tipos de dados que não os expõem e podem ser compartilhados, dados gerais e que não precisam do seu aval para compartilhamento. No geral, informações que podem ser acessadas por todos sem prejuízos ao usuário.

Em relação aos *cookies*, o conhecimento e o desconhecimento quanto ao que são dividiu a amostra. As vinte e uma pessoas que afirmaram saber os definiram em geral como formas, ferramentas, solicitações que *sites*, *apps* e serviços utilizam para gravar, salvar ou armazenar seus dados. Grosso modo, com suas palavras, os respondentes conseguiram formular uma definição congruente com a ação executada pelos *cookies*.

Quando questionados se para eles era importante que seus dados digitais fossem protegidos, todos os quarenta e dois participantes responderam **sim**. Ao justificarem suas respostas eles apontaram questões de:

- segurança (n=5); e
- ameaças por eles consideradas perigosas (n=2).

Eles também citaram:

- crimes virtuais (n=2);
- fraudes (n=4);
- roubo (n=1);
- ação de *hackers* (n=2);
- vazamentos (n=2); e
- golpes (n=10).

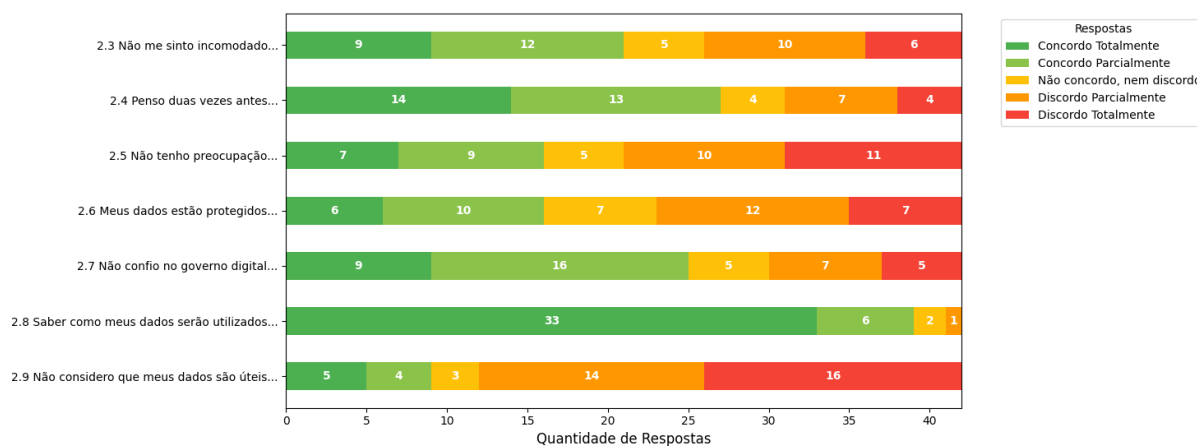
As respostas dos participantes demonstram como a sua percepção de privacidade de dados digitais está conectada, em sua maioria, a temas como segurança e golpes que remetem a preocupações econômicas e financeiras.

Os participantes também responderam a questões propostas em formato de escala de atitudes. Foram fornecidas as seguintes afirmações:

- **2.3** Não me sinto incomodado quando um aplicativo do governo solicita dados pessoais;
- **2.4** Penso duas vezes antes de fornecer minhas informações pessoais em *apps* do governo;
- **2.5** Não tenho preocupação de que serviços do governo possam estar coletando um volume de dados pessoais maior que o necessário;
- **2.6** Meus dados pessoais estão protegidos nos serviços do governo digital;
- **2.7** Não confio no governo digital para proteger os meus dados pessoais;
- **2.8** Estar ciente de como minhas informações pessoais serão utilizadas é muito importante para mim;
- **2.9** Não considero que meus dados pessoais são úteis para a administração pública e para o governo digital.

Eles deveriam avaliar as afirmações quanto ao nível de concordância. As opções eram concordo totalmente; concordo parcialmente; não concordo, nem discordo; discordo parcialmente; discordo totalmente. As respostas dos participantes podem ser visualizadas na figura 24 a seguir.

Figura 24 - Respostas às afirmações apresentadas aos participantes



Fonte: elaborado pela autora, 2025.

A afirmação **2.3** apresenta cinco participantes neutros. Menos da metade, dezesseis, discorda e demonstra sim sentir incômodo quando serviços do governo digital solicitam seus dados. Ainda que isso revele um nível de preocupação aos respondentes, de modo geral - uma vez que metade (n=21) concorde positivamente - esse procedimento é considerado aceitável pelas pessoas.

Em relação à declaração **2.4**, mesmo que quatro pessoas tenham sido neutras e onze discordantes quanto à refletir antes de fornecer seus dados, este é um comportamento real das pessoas, indicada pela concordância de vinte e sete respondentes. Já na declaração **2.5**, dezesseis confirmam concordar que o volume de dados coletados pelo governo não representa preocupação. Entretanto, metade dos participantes (n=10 e n=11) discorda. O que aponta para uma desconfiança dos participantes quanto ao uso das suas informações.

O enunciado **2.6** apresentar o maior número de respostas neutras (n=7) e a menor diferença entre concordância e discordância entre todas as afirmações. Ainda que haja um maior número de pessoas (n=19) discordando da proteção dos seus dados pelo governo, ele não é muito maior do que as pessoas que concordam que há sim proteção. Ainda assim, de acordo com a afirmativa **2.7**, a desconfiança é maior, já que vinte e cinco pessoas concordam que não confiam no governo digital para proteger seus dados.

Trinta e nove pessoas corroboraram com dados de questões anteriores ao concordarem que estar ciente sobre o que será feito com suas informações é muito importante para elas - afirmativa **2.8**. Por fim, quando apresentados à declaração **2.9**, as pessoas discordaram em sua maioria que seus dados pessoais são úteis à administração pública e ao governo digital. Três pessoas se mantiveram neutras e nove pessoas concordaram que seus dados têm utilidade.

Os participantes foram apresentados a duas questões para verificar sua interação com as políticas de privacidade e os termos de consentimento. As perguntas foram as seguintes:

- 2.10 Ao ter contato com políticas de privacidade e termos de consentimento em *sites*, serviços, aplicativos do governo digital (ex.: *app* VIVA PROCON), você costuma?; e
- 2.11 Ao ler políticas de privacidade e termos de consentimento do governo digital (ex.: *app* VIVA PROCON), o que você entende?

Com as respostas obtidas foi possível elaborar uma matriz de interação para verificar a intersecção entre as respostas de cada participante. A tabela 5 condensa os dados da matriz. O eixo y verifica o hábito dos participantes, classificando se eles aceitam os documentos sem ler, se leem parcialmente, a maior parte ou

completamente. Já o eixo x verifica seu nível de compreensão entre não entender, entender pouco, quase tudo ou tudo e confirma seu hábito de não leitura.

Tabela 5 - Matriz da interação dos participantes

	Não leio	Não entendo	Entendo pouco	Entendo quase tudo	Entendo tudo	Total
Aceitar sem ler	11	2	5	1	0	19
Ler parcialmente antes de aceitar	0	2	7	5	1	15
Ler a maior parte antes de aceitar	0	0	0	1	1	2
Ler completamente antes de aceitar	0	0	4	1	1	7
Total	11	4	16	8	3	42

Fonte: elaborado pela autora (2025).

Onze participantes que revelaram **aceitar sem ler**, mantiveram a resposta quanto ao nível de compressão. Já dois participantes que escolheram a mesma opção de hábito optaram por **não entendo** ao avaliar seu nível de compreensão.

Outras cinco pessoas com esse hábito indicaram que em relação à compreensão **entendem pouco**. Uma pessoa, que normalmente **aceita sem ler**, disse **entender quase tudo** dos documentos. O grupo desse hábito em relação à aceitação é formado por dezenove respondentes.

Já em relação ao hábito **ler parcialmente antes de aceitar**, duas pessoas afirmaram que **não entendem**. Sete pessoas afirmaram que **entendem pouco**. Cinco pessoas afirmaram que **entendem quase tudo** e uma pessoa que **entende tudo**.

Como resultado, quinze pessoas têm o hábito de **ler parcialmente antes de aceitar** independente do seu nível de assimilação. Em contraste, apesar de hábitos diferentes em relação à aceitação, quatro pessoas **não entendem** os conteúdos das políticas de privacidade e dos termos de consentimento.

Quanto ao hábito **ler a maior parte antes de aceitar**, uma pessoa disse que **entende quase tudo**. Uma pessoa disse que **entende tudo**. Dessa forma, duas pessoas revelaram que normalmente leem a maior parte antes de aceitar.

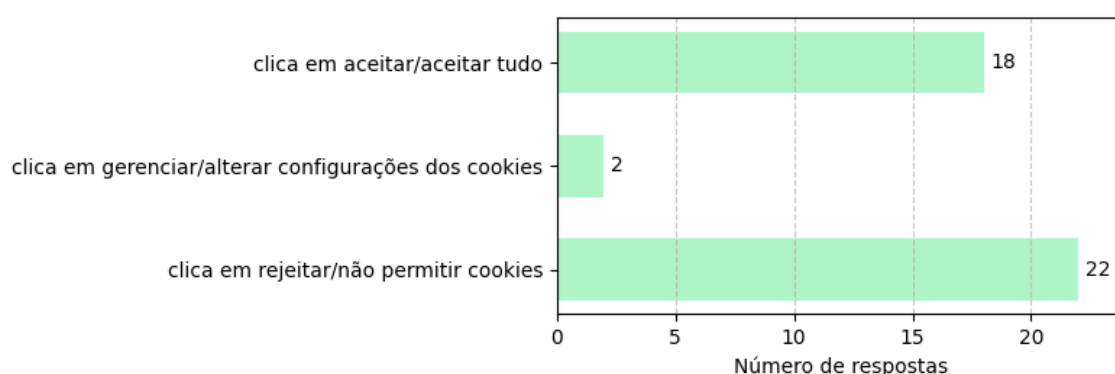
Quatro pessoas mostraram **ler completamente antes de aceitar**, apesar de **entender pouco**. Uma pessoa **entende quase tudo** e um **entende tudo**. No total,

sete pessoas **leem disseram antes de aceitar**, independente do seu nível de compreensão.

Por conseguinte, apesar do seu hábito de ler ou níveis de leitura, um grupo de dezesseis pessoas disseram **entender pouco** as políticas de privacidade e os termos de consentimento. Outro grupo, oito pessoas, disseram **entender quase tudo**. E, por fim, três representam pessoas que disseram **entender tudo**.

Os participantes também foram questionados sobre o seu comportamento de interação ao se depararem com *cookies* nas interfaces de serviços de governo digital. As respostas podem ser visualizadas na figura 25. Vinte e duas pessoas responderam que clicam em rejeitar/não permitir *cookies*. Duas pessoas clicam em gerenciar/alterar configurações dos *cookies*. Dezoito pessoas clicam em aceitar/aceitar tudo.

Figura 25 - Comportamento em relação aos botões de cookies (n=42)



Fonte: elaborado pela autora, 2025.

O grupo de pessoas que **clica em rejeitar/não permitir cookies** (n=22) se manteve equilibrado quanto ao gênero. Onze mulheres e onze homens responderam que escolhem essa opção. A média de idade dessas pessoas é $\approx 41,91$ anos, com desvio padrão [DP] de $\approx 12,94$ anos.

A maioria do grupo possui ensino médio (n=9). Há também pessoas com ensino fundamental (n=2), ensino superior (n=6) e pós-graduação (n=5). No geral, as pessoas que rejeitam ou não permitem os cookies também estão equilibrados quando a escolaridade, pois metade (n=11) concluiu a educação básica e a outra parte (n=11) possui formação além desse nível.

Essas pessoas justificaram a escolha como falta de confiança em relação ao mecanismo. Quatro pessoas citaram que tentam rejeitar, mas alguns *sites* não permitem a continuidade da navegação diante da negativa. Duas pessoas

justificaram que se o *site* impossibilitar o uso após a negativa, eles optam por seguir para outro *site*.

Já uma pessoa comentou que acha a opção rejeitar/não permitir menos complexa que gerenciar os *cookies*. Outras justificativas variaram entre comportamento automático ao clicar, desconhecimento em relação à ação dos *cookies* e incapacidade de explicar a escolha.

Dois participantes disseram que têm o hábito de **gerenciar**, pois nem sempre os *sites* permitem a continuidade da navegação após os *cookies* serem rejeitados. Assim eles podem continuar utilizando o *site*, mas de uma forma que se sintam mais seguros em relação ao mecanismo de rastreo. Esses respondentes se identificaram como do gênero feminino. Elas têm 30 e 40 anos e ensino superior e pós-graduação completos, respectivamente.

O grupo de pessoas que **clica em aceitar/aceitar tudo** (n=18) apresenta diferença quanto ao gênero. Dez homens e oito mulheres responderam escolher essa opção. A média de idade do grupo é de 47 anos, com desvio padrão [DP] de $\approx 11,88$ anos.

O número de pessoas que completaram o ensino médio também é maior (n=8) neste grupo. Assim como há respondentes dos outros níveis de escolaridade, ensino fundamental (n=1), ensino superior (n=3) e pós-graduação (n=6). Os 3 respondentes que possuem ensino superior são homens.

Este grupo também se divide equilibradamente quanto às pessoas que concluíram a educação básica (n=9) e as que cursaram além desse nível (n=9). Os respondentes justificam que o hábito tornou-se automático pela facilidade em sumir com o *pop-up* de *cookies*. Para eles é a solução mais prática e rápida para seguir seu fluxo de navegação através dos *sites*.

Em geral, mais da metade da amostra (n=24) demonstram consciência em relação às ações do mecanismo *cookies*, ainda que no início do questionário, metade deles tenha indicado não saber o que são *cookies*. Para responder a este questionamento, os participantes foram expostos a imagem de uma tela de aceitação de *cookies*. Como mostra a figura 26. Sugere-se que essa visualização possa ter contribuído para que lembrassem do que se tratava.

Figura 26 - *Printscreen* da pergunta ilustrada sobre hábitos em relação aos cookies

2.13 Quanto aos botões como o "aceitar cookies", "aceitar todos os cookies", "permitir todos os cookies" e "rejeitar cookies" (como na imagem ilustrativa), você?

Para melhorar a sua experiência na plataforma e prover serviços personalizados, utilizamos cookies. Ao aceitar, você terá acesso a todas as funcionalidades do site. Se clicar em "Rejeitar Cookies", os cookies que não forem estritamente necessários serão desativados. Para escolher quais quer autorizar, clique em "Gerenciar cookies". Saiba mais em nossa Declaração de Cookies.

Gerenciar cookies Rejeitar cookies Aceitar cookies

☐ clica em aceitar/aceitar tudo

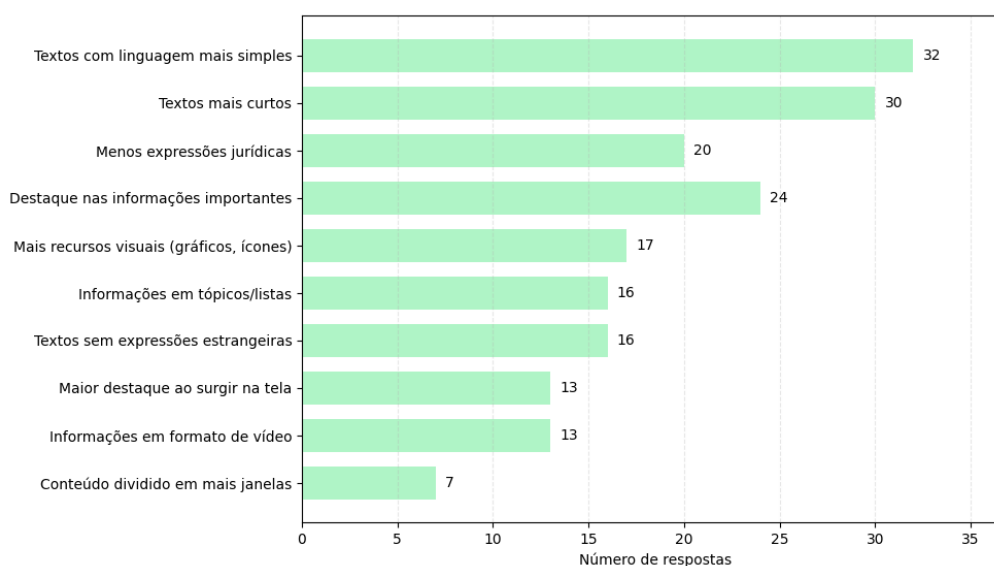
☐ clica em gerenciar/alterar configurações dos cookies

☐ clica em rejeitar/não permitir cookies

Fonte: elaborado pela Autora, 2025.

Por fim, as pessoas que participaram da aplicação do questionário foram convidados a apresentar sugestões para tornar mais amigável a sua interação com as políticas de privacidade e os termos de consentimento. As respostas podem ser visualizadas na figura 27, em seguida. Suas respostas foram escolhidas a partir das opções fornecidas no questionário.

Figura 27 - Sugestões dos respondentes da pesquisa

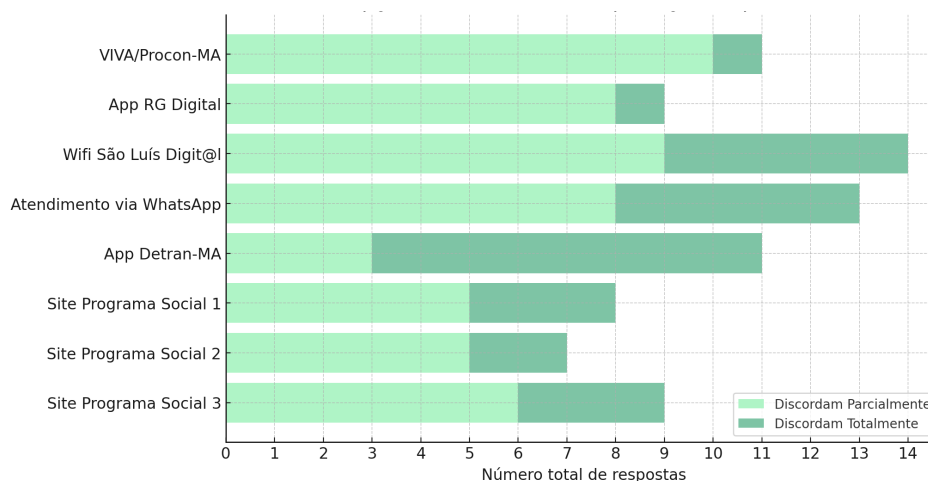


Fonte: elaborado pela autora, 2025.

Os participantes também responderam sobre serviços de governo digital a nível local. Foram listados serviços via aplicativo e *sites* de programas sociais do governo do estado. Canal de atendimento via *WhatsApp* utilizado para contato com instituição pública e login para conexão na rede wifi da prefeitura de São Luís.

O gráfico a seguir (figura 28) demonstra a quantidade de respondentes que discorda, parcialmente ou totalmente, que os serviços listados são claros quanto à proteção da privacidade e dos dados dos usuários.

Figura 28 - Clareza sobre privacidade e proteção de dados em serviços locais



Fonte: elaborado pela autora, 2025.

Em função das iniciativas de governo digital no Estado serem pouco populares e utilizadas pela população, a amostra de respondentes não possuía afinidade com a maioria dos serviços listados. Por isso, optou-se por tabular apenas aqueles que contribuem para o reconhecimento da necessidade de melhorias de acordo com a avaliação desses participantes.

Os resultados obtidos neste capítulo, referentes à análise da *sketch interview* e dos questionários aplicados serão interpretados, discutidos e comparados na seção a seguir.

5.3 Convergência e discussão

A intenção da pesquisa, a partir da sua fundamentação, era focar no contexto e população local. Os participantes eram residentes do estado, de idades e contextos educacionais diferentes. Eles também eram usuários de serviços de governo digital com perfis diferentes. Parte dos participantes já havia utilizado o aplicativo VIVA/Procon-MA para mais de dois serviços diferentes.

Ao considerar as experiências desses usuários através de dois instrumentos diferentes de pesquisa, a *sketch interview* e o questionário, foram obtidos resultados capazes de fornecer orientações para atualizar e melhorar suas experiências com

esses serviços. Para isso eles foram convergidos e integrados a resultados de outras pesquisas de modo a obter os apontamentos necessários.

5.3.1 Diretrizes quanto à privacidade e a proteção de dados pessoais

Durante a análise dos resultados das entrevistas, a percepção é que as pessoas que participaram da pesquisa estão familiarizadas com o assunto. Algumas conseguiram, inclusive, usar termos específicos e elaborar reflexões mais teóricas. Há uma ocorrência diversa de códigos de familiaridade (*Sketch Interview*) e um número maior de respostas positivas, em comparação com as negativas, em relação às perguntas de familiaridade (Questionário).

Entretanto, essa tendência positiva pode ser fruto da predisposição dos participantes em colaborar e tentar alcançar respostas esperadas à pesquisa. Quando confrontados com outros resultados posteriores oriundos dos mesmos instrumentos, verifica-se que vários participantes, demonstram não saber ou ter dificuldade em relação ao assunto (CD - Demonstrando falta de conhecimento; CA - Não entende o que acontece; CA - Não sabe o que fazer; CA - Mediante desafios). Inclusive, confundindo dados sensíveis e dados pessoais comuns.

Esse fato pode ser conectado à necessidade do desenvolvimento de uma cultura educativa sobre a proteção à privacidade de dados. As pessoas em geral sabem que dados pessoais digitais são importantes e podem trazer riscos. Mas associam estes últimos a questões financeiras como golpes e fraudes.

Controle, manipulação, venda de dados e indução ao consentimento foram apontados pela minoria dos participantes. A análise dos resultados mostrou que antes de diretrizes, é preciso aos cidadãos exposição à cultura e educação de proteção de dados. Isso perpassa pelo desenvolvimento de políticas públicas e de governança.

São necessárias ações como campanhas de conscientização e material educativo. Além do estabelecimento de estratégias de comunicação e divulgação de entidades como a ANPD e a própria LGPD. Assim como projetos colaborativos com participação social e vinculação das ações a programas de governo.

O **desenvolvimento de políticas públicas e cultura de proteção e privacidade de dados** é uma diretriz primária. Ela deve estar alinhada a diretrizes específicas para orientar a experiência dos usuários (não apenas aqueles que

utilizam serviço público digital). As diretrizes específicas, no caso desta pesquisa, referem-se a interação com as políticas de privacidade e termos de consentimento.

5.3.2 Diretrizes quanto às políticas de privacidade e termos de consentimento

A partir de agora serão propostas três diretrizes quanto às políticas de privacidade e termos de consentimento. A partir da análise dos resultados da pesquisa foi possível entender a necessidade de uma diretriz mais ampla. Essa se relaciona às políticas públicas e à cultura de privacidade.

A partir dela, são propostas mais três diretrizes: versão resumida e texto integral, relacionada aos documentos com que os usuários de serviços interagem; identificadores de privacidade e segurança, que tornam visíveis os níveis de privacidade e segurança dos serviços; e design ético, comprometido e centrado no usuário, que propõe o compromisso dos profissionais em evitar o uso de *dark patterns* para induzir os usuários. As diretrizes podem ser visualizadas na imagem 29, a seguir.

Figura 29 - Diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital



Fonte: elaborado pela autora, 2025.

- **Versão resumida e texto integral**

Segundo a literatura revisada, a interação de usuários, geralmente internautas experientes, em relação às políticas de privacidade foi por vezes insatisfatória. Isso esteve atrelado à aplicação de *dark patterns* em caixas de diálogos para *cookies* e indução ao consentimento, ao uso de textos complexos e à adoção de jargões jurídicos.

Nesta pesquisa, 45,2% dos respondentes do questionário (n= 19) disseram aceitar as políticas de privacidade ou termos de consentimento sem ler. Outros 42,9% (n=18) aceitam ou aceitam todos os *cookies* porque não conseguiam, não sabiam gerenciar ou argumentaram que negá-los impedia a navegação.

De acordo com a pesquisa Privacidade e Proteção de Dados Pessoais 2023, do Comitê Gestor da Internet no Brasil (CGI.br, 2024), 26% de usuários de internet no Brasil sempre concordam com as políticas sem ler. Outros 32% concordam sem ler quase sempre.

Durante a condução da *sketch interview* os participantes relataram suas insatisfações (CD - Questionando a UX) e o que poderia justificar o índice de pessoas que concordam sem ler (CA - Não é transparente, CA - Não entende o que acontece, CA - Não sabe o que fazer).

Algumas recomendações para essa questão foram pinçadas das sugestões apresentadas aos respondentes do questionário. Textos com linguagem mais simples, textos mais curtos e destaque nas informações mais importantes foram os mais recomendados.

Elas poderiam ser aplicadas através da elaboração de **uma política de privacidade ou um termo de consentimento resumido**. Eles seriam apresentados primeiro à pessoa usuária sendo reescritos em *plain language*. Seriam caracterizados por um tamanho muito menor que concentrasse as três informações mais importantes que foram destacadas e questionadas pelos participantes. São elas o quantitativo dos dados coletados (questão 2.4 do questionário), por qual motivo (questão 2.3 do questionário) e como serão utilizados (questão 2.8 do questionário).

O texto original deveria permanecer como é. Além de continuar sendo disponibilizado integralmente sempre que o usuário precisasse. A versão resumida

também deveria informar sobre a existência do conteúdo integral do documento. Essa ideia pôde ser corroborada pela opinião de dois respondentes do questionário.

Segundo esses participantes, as expressões jurídicas características da versão integral, por exemplo, são necessárias, pois as políticas de privacidade e termos de consentimento não deixam de ser um contrato. Para eles, isso assegura respaldo jurídico para as partes e estabelece os direitos e deveres na relação entre o titular e o controlador dos dados.

• **Identificadores de privacidade e segurança**

Os participantes desta pesquisa identificaram, em sua maioria, riscos ligados a finanças, golpes e fraudes (CD - Identificando riscos; questão 1.13 do questionário) . O desenvolvimento de políticas públicas e cultura de privacidade e proteção de dados é essencial para equilibrar a visão das pessoas quanto aos riscos a que estão verdadeiramente submetidos. Ainda assim, o uso dessas pessoas deve fornecê-las uma experiência que transmita segurança.

Além da versão resumida de políticas de privacidade e termos de consentimento, são recomendados **identificadores de privacidade para os usuários**. Eles são selos que podem contribuir para expor os usuários à jornada dos seus dados. Johansen *et al.* (2021) apresentaram uma proposta semelhante intitulada *privacy labels*, rótulos visuais capazes de orientar os usuários quanto ao nível de privacidade de um produto digital.

Indicadores de privacidade, aliados à apresentação das políticas e termos em versão resumida, podem informar mais rápido e de forma mais simples o que os usuários desejam saber sobre o tipo de consentimento concedido a um serviço. Ou seja, o nível de privacidade e proteção de dados que lhes será assegurada ao usar determinado serviço.

• **Design ético, comprometido e centrado no usuário**

Por parte das instituições cabe a adoção de recomendações de design ético e centrado no usuário. Ou seja, evitando padrões enganosos, especialmente opções únicas ou de pré-seleção de confirmação ou de destaque em opções que induzem ao consentimento.

Isso acontece, pela instrução adequada dos profissionais de design de interação. E principalmente pelo comprometimento das equipes em verificar e evitar o uso desses padrões. A integração do *privacy by design* está conectada ao comprometimento e à ética na atuação desses profissionais, uma vez que a proteção da privacidade do usuário é pilar fundamental do projeto.

A existência de políticas públicas e cultura de privacidade e proteção de dados também pressupõe a existência de canais de denúncia para que usuários possam comunicar problemas de transparência em relação à privacidade dos seus dados (Aguiar, 2024).

5.3.3 Governo digital no Maranhão

A proposta da pesquisa também busca por contribuições para melhoria nos serviços de governo digital da população local. Especialmente no que tange à garantia à privacidade e proteção dos dados dos cidadãos. Entretanto, a partir da aplicação do questionário, sugere-se que a adesão da população a serviços locais ainda é pequena e de difícil investigação desse aspecto.

Por exemplo, não foram encontrados dados estatísticos que pudessem indicar a adesão da população a esses serviços. Ou mesmo números sobre os serviços mais utilizados. Dessa forma, o governo digital no Maranhão se mostra ainda em desenvolvimento. Ou seja, não consolidado enquanto política de Estado.

O que se propõe, a princípio, são investigações recorrentes à medida que surjam novas iniciativas públicas voltadas à prestação de serviços para a população maranhense. Preferencialmente iniciativas que abranjam heterogeneamente serviços para toda a população. Dessa forma, será possível verificar com mais robustez o nível de transparência e a opinião dos usuários sobre tais serviços.

6 CONSIDERAÇÕES FINAIS

Com esta pesquisa foi possível verificar que questões de privacidade e dados não são assuntos tão distantes das pessoas comuns. Elas se preocupam com as próprias informações, mas se vêem em um contexto cada vez mais indutivo. Elas precisam fornecer os próprios dados para fazer das coisas básicas na internet, como ler notícias, até as mais essenciais, como exercer a cidadania por meio do acesso a serviços públicos digitais.

Esta pesquisa tinha como objetivo principal apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital. Por meio dele, verificou-se a necessidade de educar as pessoas antes de apresentá-las a informações como as políticas de privacidade, os termos de consentimento e os *cookies*.

As tarefas que envolvem interagir com esses elementos também precisam ser menos desgastantes. Os textos das políticas e dos termos precisam ser mais curtos e compreensíveis. Outro objetivo da pesquisa era descrever o governo digital brasileiro e como a privacidade e proteção de dados estão posicionadas nele.

O *e-gov* tornou-se fundamental do Estado na prestação de serviços e garantia do exercício da cidadania digital dos brasileiros. Por isso, ele está alinhado à Lei Geral de Proteção de Dados Pessoais. Entretanto, em relação a essa conformidade, de acordo com a literatura revisada, seus usuários não estão isentos à exclusão digital e ao viés algorítmico. E, principalmente a experiências insatisfatórias

A pesquisa pretendia também interseccionar conceitos de design e ergonomia à privacidade, ao consentimento, à proteção de dados pessoais e ao governo digital, e identificar suas contribuições para orientar a comunicação e interação relacionadas a essas questões. Por meio das abordagens relacionadas, as metodologias *privacy by design* e linguagem simples ou cidadã foram verificadas como aliadas fundamentais das abordagens do design na promoção de uma experiência do usuário aprimorada.

Considerando conceitos e trabalhos de HCI, UCD, HC, IxD, Usabilidade e UX, chegou-se a métodos e técnicas que permitissem saber das pessoas usuárias locais formas de incluí-las no processo, para assim chegar às diretrizes. Foram identificados a entrevista, por meio do instrumento *sketch interview*, e o questionário.

Um dos propósitos da pesquisa era conhecer percepções que usuários têm sobre privacidade e proteção de dados pessoais. Verificou-se que eles estão familiarizados em certo ponto com as questões de privacidade. Além disso, conseguiram mapear problemas e experiências insatisfatórias de uso em suas jornadas de usuários.

Ao indicar como usuários do governo digital interagem com as políticas de privacidade e com os termos de consentimento, verificou-se que eles consideram importante serem informados sobre o que é feito com seus dados ainda que mantenham comportamentos como aceitar termos e condições sem ler, justificado pelo pouco entendimento em relação ao conteúdo dos documentos apresentados.

Por fim, ao correlacionar as percepções, interações e a forma como as plataformas apresentam as políticas de privacidade e os termos de consentimento, verificaram-se diretrizes para experiências mais amigáveis dos usuário, como políticas de privacidade e termos de consentimento resumidos e indicadores de privacidade em produtos digitais.

6.1 Limitações da pesquisa

Algumas limitações atravessaram o processo desta pesquisa. O principal, diz respeito ao tamanho das amostras dos participantes. O objetivo era contar com uma amostra da pesquisa quantitativa maior. O *link* de resposta ao formulário foi compartilhado por semanas, mais de uma vez com diversos contatos e em grupos e em redes sociais diferentes. Entretanto, o interesse e a adesão de participantes à pesquisa foi pequeno.

Inferre-se que isso aconteceu por falta de afinidade com o tema da pesquisa, com o tamanho do questionário ou mesmo devido ao caráter voluntário da participação. Ainda mais considerando o caráter voluntário da pesquisa, sem benefícios (item inclusive questionado por respondentes) e conduzida em locais públicos. Com uma amostra maior de pessoas, por exemplo, seria possível verificar se os resultados apresentados permaneceriam os mesmos.

Em relação à pesquisa qualitativa, poucos participantes aceitaram participar do momento II. Sugere-se que isso aconteceu pelo mesmo motivo apresentado em relação ao questionário. Outros participantes dessa etapa não foram encontrados

novamente para participar. Essas pessoas são trabalhadores informais e não estavam no local de trabalho no retorno da pesquisadora para o segundo momento.

6.2 Desdobramentos

Os problemas e reflexões sobre privacidade de dados digitais não são mais emergentes. No início desta pesquisa, em junho de 2023, o contexto que envolvia tecnologia, dados pessoais, grandes companhias e governo era relativamente diferente. A inteligência artificial ainda estava se tornando produto de massa, por exemplo.

No momento da conclusão desta pesquisa, esses fatores estão cada vez mais intrincados e precisam ser colocados em foco quanto ao direcionamento de estudos posteriores. Faz-se necessário uma visão ainda mais crítica e rigorosa a respeito dos direitos dos cidadãos, bem como dos usuários de qualquer serviço digital que disponibilizam seus dados on-line.

Quanto à parte prática, a condução dessa pesquisa sugere alguns desdobramentos para estudos futuros. O primeiro seria a concretização das diretrizes apontadas como produto final deste trabalho. Mais do que guias ou instruções, elas precisam de execução para que o ambiente de interface do usuário com as políticas de privacidade, termos de consentimento e coleta de dados seja mais amigável.

O segundo desdobramento, que na verdade atravessa o primeiro, é a validação das diretrizes apontadas junto aos usuários do governo digital. Afinal, elas serão apenas centradas e pensadas neles se aprovadas pelo público de interesse verdadeiro, o cidadão que utiliza os serviços públicos neste país.

O terceiro desdobramento aparece frente ao governo do estado do Maranhão. Os resultados obtidos sugeriram a necessidade de investigações posteriores concomitantes a necessidade de ampliação na oferta de serviços digitais para a população maranhense. Isso permitiria verificar maior precisão dos dados e percepções sobre a proteção de dados digitais no Estado.

6.3 Lições aprendidas

No início desta pesquisa, objetiva-se discutir as ameaças à privacidade de forma crítica, especialmente do ponto de vista do campo do design. O recorte de

usuários e serviços do governo digital foi incluído nos meses subsequentes a partir das discussões levantadas durante as reuniões de orientação. Isso aconteceu em função da crença da pesquisadora no Estado como instituição capaz e fundamental para salvaguardar os seus cidadãos, principalmente aqueles sujeitos a alguma vulnerabilidade.

O objetivo desta pesquisa, além dos apresentados no início deste documento, era de alguma forma contribuir com essa instituição na proteção da privacidade dos cidadãos. Realizá-los trouxe uma série de aprendizados que estão contidos nesta dissertação e na jornada da pesquisadora. Inicialmente houve o desafio da adaptação e da produção de conhecimento em uma área de pesquisa diferente da de formação da pesquisadora.

Para compreender o tema abordado e relacioná-lo ao recorte escolhido, a pesquisa demandou uma série de revisões na literatura produzidas anteriormente. As lacunas de pesquisa em relação aos temas privacidade - governo digital - design demonstraram a relevância desta proposta, mas também o desafio de conduzi-la. A ausência de produções a nível nacional ou regional se revelou como uma importante lição sobre a condução de uma pesquisa em que maior parte das referências apresentadas advinham de um idioma e de uma cultura diferentes.

O procedimento metodológico pensado para a pesquisa logo teve de ser adaptado a partir dos desempenhos obtidos nos pré-testes realizados. Isso releva a necessidade de, durante a condução da pesquisa, pensar em um procedimento metodológico adaptável. Além de como isso está sujeito às variabilidade de se pesquisar com a participação de seres humanos.

Quando o objetivo geral da pesquisa foi definido, outras diretrizes eram esperadas para o final da pesquisa. Entretanto, a análise dos dados e as respostas dos participantes levaram aos resultados apresentados nesta dissertação. O que revela a necessidade de compreender como uma pesquisa, por vezes, segue uma trajetória diferente da imaginada no seu início a partir dos resultados obtidos dos dados levantados.

REFERÊNCIAS

- AGNER, L. **Ergodesign e arquitetura de informação**: trabalhando com o usuário. 2 ed. Rio de Janeiro: Quartet, 2009.
- AGUIAR, Y. P. C. Design ético em *Black Mirror*. Identificando e discutindo padrões obscuros em IHC. In: SILVEIRA, M. S.; GASPARINI, I. **Práticas de IHC em Sala de Aula**. Porto Alegre: Sociedade Brasileira de Computação, 2024.
- _____. _____. 5 ed., rev e amp. Rio de Janeiro: Ed Senac Rio, 2023.
- ALHARBI, J. A.; Albeshier, A. S.; Wahsheh, H. A. **An Empirical analysis of e-governments' cookie interfaces in 50 countries**. Sustainability 15, 1231. 2023. Disponível em: <https://doi.org/10.3390/su15021231>. Acesso em: 05 jul. 2023.
- ANTONIALLI, D. M.; KIRA, B. **Planejamento urbano do futuro, dados do presente**: a proteção da privacidade no contexto das cidades inteligentes. 2020. Disponível em: <https://doi.org/10.22296/2317-1529.rbeur.202003>. Acesso em: 08 dez. 2023.
- AYLON, O.; TOCH, E. **User-centered privacy-by-design: evaluating the appropriateness of design prototypes**. International Journal of Human Computer Studies, Vol 154, 102641. 2021. Disponível em: <https://doi.org/10.1016/j.ijhcs.2021.102641>. Acesso em: 02 fev. 2024.
- BALBE, R. da S. **Uso de tecnologias de informação e comunicação na gestão pública: exemplos no governo federal**. Revista do Serviço Público, [S. l.], v. 61, n. 2, p. p. 189-209, 2014. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/45>. Acesso em: 13 nov. 2023.
- BARTALI, V.; VELSEN, L. V. **An experiment on data sharing options designs for eHealth interventions**. Internet Interventions 33, 100642. 2023. Disponível em: <https://doi.org/10.1016/j.invent.2023.100642>. Acesso em: 27 nov. 2023.
- BERNARDO, M. do R. M. **Smart Governance em cidades inteligentes europeias**. 2019. Disponível em: <http://hdl.handle.net/10400.2/8943>. Acesso em: 13 nov. 2023.
- BERNI, A.; BORGIANNI, Y. **From the definition of user experience to a framework to classify its applications in design**. 2021. Disponível em: <https://doi.org/10.1017/pds.2021.424>. Acesso em: 16 ago. 2023.
- BOUDON, R. **Métodos em sociologia**. São Paulo: Editora Ática, 1989.
- BOWYER, A.; HOLT, J.; JEFFERIES, J. G.; WILSON, R.; KIRK, D.; SMEDDINCK, J. D. **Human-GDPR interaction: practical experiences of accessing personal data**.

CHI Conference on Human Factors in Computing Systems (CHI '22) Proceedings. 2022. Disponível em: <https://doi.org/10.1145/3491102.3501947>. Acesso em: 23 jun. 2023.

BRASIL - **Carta brasileira para as cidades inteligentes**. 2021b. Disponível em: <https://www.gov.br/cidades/pt-br/acao-a-informacao/acoes-e-programas/desenvolvimento-urbano-e-metropolitano/projeto-andus/carta-brasileira-para-cidades-inteligentes>. Acesso em: 23 out. 2023.

_____ - DECRETO Nº 8777 DE 11 DE MAIO DE 2016. **Institui a Política de Dados Abertos do Poder Executivo federal**. 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 23 out. 2023.

_____ - **Estratégia brasileira para a transformação digital**. 2018. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em: 13 out. 2023.

_____ - **Estratégia brasileira para a transformação digital (E-Digital) Ciclo 2022 - 2026**. 2022. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital>. Acesso em: 24 out. 2023.

_____ - LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. **Lei de acesso à informação**. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 23 out. 2023.

_____ - LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco civil da internet**. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jul. 2023.

_____ - LEI Nº 13.460, DE 26 DE JUNHO DE 2017. **Lei de Proteção ao Usuário do Serviço Público**. 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm. Acesso em: 23 nov. 2023.

_____ - LEI Nº 13.853 DE 08 DE JULHO DE 2019. **Lei geral de proteção de dados pessoais (LGPD)**. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 16 jul. 2023.

_____ - LEI Nº 14.129, DE 29 DE MARÇO DE 2021. **Lei do governo digital**. 2021a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 25 out. 2023.

_____ - **Regiões norte e centro-oeste têm os maiores aumentos de conectividade em 2023**. Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/noticias/regioes-norte-e-centro-oeste-tem-os-maiores-aumentos-de-conectividade-em-2023>. Acesso em 17 abr. 2024.

CAPELLI, C.; Nunes, V.; OLIVEIRA, R. Transparência e transformação digital: o uso da técnica da linguagem simples. In: FRANÇA, T. C. D.; LOUZADA, A. C (Orgs). **Minicursos da VII Escola Regional de Sistemas de Informação (ERSI-RJ 2021)**. Porto Alegre: Sociedade Brasileira de Computação, 2021.

CARDOSO, R. **Design para um mundo complexo**. São Paulo: Cosac Naify, 2012.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 2002.

CAVOUKIAN, A. **Privacy by design: the 7 foundational principles**. 2009. Disponível em: <https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf>. Acesso em: 07 fev. 2023.

CERQUINHO, K. G. **Governo digital no Brasil: o portal gov.br**. Manaus: EDUA, 2017.

CHALHOUB, G.; KRAEMER, M. J.; FLECHAIS, I. **Useful shortcuts: using design heuristics for consent and permission in smart home devices**. International Journal of Human-computer Studies 182, 103177. 2023. Disponível em: <https://doi.org/10.1016/j.ijhcs.2023.103177>. Acesso em: 02 fev. 2024.

CHAMMAS, A.; QUARESMA, M.; MONT'ALVÃO, C. **A Closer look on the user centred design**. Procedia Manufacturing vol 3. 2015. Disponível em: <https://doi.org/10.1016/j.promfg.2015.07.656>. Acessado em: 24 ago. 2023.

CHARMAZ, K. **A construção da teoria fundamentada: um guia prático para análise qualitativa**. Porto Alegre: Artmed, 2009.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br) - **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros : TIC Domicílios 2022**. Núcleo de Informação e Coordenação do Ponto BR, São Paulo: 2023.

_____ - **Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil**. São Paulo: Comitê Gestor da Internet no Brasil, 2022.

- **Privacidade e proteção**

de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2024.

CORDEIRO, R; MONT'ALVÃO, C; QUARESMA, M. **Citizen data-driven design for pandemic monitoring. Strategic Design Research Journal.** Volume 13, number 03, September – December 2020. 342-354. Disponível em: <https://doi.org/10.4013/sdrj.2020.133.04>. Acesso em 27 abr. 2024.

COSTA, G. C. **Analfabetismo resiste no Brasil e no mundo do século 21.** 2019. Disponível em: <https://agenciabrasil.ebc.com.br/educacao/noticia/2019-09/analfabetismo-resiste-no-brasil-e-no-mundo-do-seculo-21>. Acesso em: 25 ago. 2023.

CRESWELL, J. W. **Projeto de pesquisa:** métodos qualitativo, quantitativo e misto. 5. ed. Porto Alegre: Artmed, 2021.

CRESWELL, J. W. **Investigação qualitativa & projeto de pesquisa.** 3. ed. Porto Alegre: Penso, 2014.

CRESWELL, J. W.; CLARK, V. L. P. **Designing and conducting mixed methods research.** Los Angeles: Sage, 2017.

CRISTÓVAM, J. S. da S.; SAIKALI, L. B.; SOUSA, T. P. de. **Governo digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil.** Seqüência Estudos Jurídicos e Políticos, [S. l.], v. 41, n. 84, p. 209–242, 2020. Disponível em: <https://doi.org/10.5007/2177-7055.2020v43n84p209>. Acesso em: 13 nov. 2023.

DINIZ, E. H.; BARBOSA, A. F.; JUNQUEIRA, A. R. B.; PRADO, O. **O governo eletrônico no Brasil:** perspectiva histórica a partir de um modelo estruturado de análise. 2009 Disponível em: <https://doi.org/10.1590/S0034-76122009000100003>. Acesso em: 13 nov. 2023.

DOSS, A. **Cyber privacy.** Dallas: BenBella Books, 2020.

DUARTE, D. E. **Estudos de vigilância.** Rio de Janeiro: CESeC, 2023.

FONSECA, R. A. **A vida mobile no capitalismo de dados:** narrativas de negócios digitais e a constituição do consumidor conectado. São Paulo: Pimenta Cultural, 2020.

FRANCO JR, J. R. de M. Privacidade Digital. In: DAWBOR, L (Org). **Sociedade vigiada.** São Paulo: Autonomia Literária, 2020.

FREITAS, V. P. de; SILVA, L. C. da. **Cidades inteligentes: a busca pela sustentabilidade e o impacto na privacidade.** Revista de Direito da Cidade, [S. l.], v. 12, n. 1, p. 632–651, 2020. DOI: 10.12957/rdc.2020.40588. Disponível em: <https://doi.org/10.12957/rdc.2020.40588>. Acesso em: 08 dez. 2023.

GERVAZONI, A. L. C. **O design de interface como facilitador na comunicação do processo de tratamento de dados digitais dos usuários.** Dissertação (mestrado em Design) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2023.

GIACOMIN, J. **What is human centered design?**. 2014. Disponível em: <https://doi.org/10.2752/175630614X14056185480186>. Acesso em: 16 aug. 2023.

GIBBS, G. **Análise de dados qualitativos.** Porto Alegre: Artmed, 2009.

GIL, A. C. **Como elaborar projetos de pesquisa.** 6. ed. São Paulo: Atlas, 2017.

_____. **Métodos e técnicas de pesquisa social.** 7 ed. São Paulo: Atlas, 2021.

GORICHANAZ, T. **Toward humanity-centered design without hubris.** CHI EA '24: Extended Abstracts. Disponível em: <https://doi.org/10.48550/arXiv.2402.11576>. Acesso em: 02 abr. 2024.

GRAFENSTEIN, M. V.; JAKOBI, T.; STEVENS. **Effective data protection by design through interdisciplinary research methods:** the example of effective purpose specification by applying user-centred ux-design methods. Computer Law & Security Review 46 105722. 2022. Disponível em: <https://doi.org/10.1016/j.clsr.2022.105722> . Acesso em: 25 nov. 2023.

HANADA, L. M.; TAVARES, E.; COSTA, I. De S. A. da. **Going Mobile:** oportunidades, barreiras e fatores críticos de sucesso para iniciativas de M-Government. Revista Gestão & Conexões, [S. l.], v. 9, n. 2, p. 74–93, 2020. Disponível em: <https://doi.org/10.13071/regec.2317-5087.2020.9.2.27649.74-93>. Acesso em: 13 nov. 2023.

HÖÖK, K.; LÖWGREN, J. **Characterizing Interaction Design by its ideals:** a discipline in transition. Volume 7, Issue 1, Pages 24-40. 2021. Disponível em: <https://doi.org/10.1016/j.sheji.2020.12.001>. Acesso em: 29 mar. 2024.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. **Pesquisa nacional por amostra de domicílios contínua:** acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2022. 2023. Disponível em: <https://>

biblioteca.ibge.gov.br/visualizacao/livros/liv102040_informativo.pdf. Acesso em: 13 nov. 2023.

JOHANSEN, J.; PEDERSEN, T.; FISCHER-HÜBNER, S.; JOHANSEN, C.; SCHNEIDER, G. ROOSENDAAL, A.; ZWINGELBERG, H.; SIVESIND, J.; NOLL, J. **A Multidisciplinary definition of privacy labels: the story of princess privacy and the seven helpers.** Inf. Comput. Secur., 30, 452-469. 2020. Disponível em <https://doi.org/10.48550/arXiv.2012.01813>. Acesso em: 23 jun. 2023.

KITCHIN, R. **Getting smarter about smart cities:** Improving data privacy and data security. Dublin: Data Protection Unit, Department of the Taoiseach, 2016.

KITKOWSKA, A.; SHULMAN, Y.; MARTUCCI, L. A.; WÄSTLUND, E. **Designing for privacy: exploring the influence of affect and individual characteristics on users' interactions with privacy policies.** Computers & Security, vol 134, 103468. 2023. Disponível em: <https://doi.org/10.1016/j.cose.2023.103468>. Acesso em: 02 fev. 2024.

KREBS, L. M.; DEWITTE, P.; GEERTS, D.; VERBERT, K.; RODRIGUEZ, O. L. A.; AUSLOOS, J. NAUDTS, L. **Tell me what you know:** GDPR implications on designing transparency and accountability for news recommender systems. CHI'19 Extended Abstracts. 2019. Disponível em: <https://doi.org/10.1145/3290607.3312808>. Acesso em: 23 jun. 2023.

KREMER, B. **Racismo algorítmico.** Rio de Janeiro: CESeC, 2023.

KREUZ, L. R. C.; VIANA, A. C. A. **4a Revolução industrial e governo digital:** exame de experiências implementadas no Brasil. Revista Eurolatinoamericana de Derecho Administrativo, Santa Fe, vol. 5, n. 2, p. 267-286, jul./dic., 2018. Disponível em: <https://doi.org/10.14409/redoeda.v5i2.9092>. Acesso em: 13 nov. 2023.

KUANG, C.; FABRICANT, R. **Fácil de usar:** como os segredos do design user friendly estão mudando o modo como vivemos, trabalhamos e nos divertimos. São Paulo: Alta Books, 2022.

LAKATOS, E. M.; MARCONI, M. D. A. **Técnicas de pesquisa.** São Paulo: Atlas, 2002.

_____. **Fundamentos de metodologia científica.** São Paulo: Atlas, 2003.

_____. **Metodologia científica.** São Paulo: Atlas, 2010.

LAVILLE, C.; DIONNE, J. **A Construção do Saber**: manual de metodologia da pesquisa em ciências humanas. Porto Alegre: Artmed; Belo Horizonte: Editora UFMG, 1999.

LE MOS, A.; ARAÚJO, N. V. **Cidadão Sensor e Cidade Inteligente**: Análise dos Aplicativos Móveis da Bahia. Revista Famecos, Porto Alegre, v. 25, n. 3, p. 1-19, setembro, outubro, novembro e dezembro de 2018: ID28708. DOI: <http://dx.doi.org/10.15448/1980-3729.2018.3.28708>. Acesso em: 13 nov. 2023.

LIALINA, O. Turing complete user. 2012. In: LIALINA, O. **Turing complete user**: resisting alienation in Human Computer Interaction. Berlin: Arthistoricum.net, Heidelberg University Library, 2021.

_____. Rich user experience. 2014. In: LIALINA, O. **Turing complete user**: resisting alienation in Human Computer Interaction. Berlin: Arthistoricum.net, Heidelberg University Library, 2021.

_____. Once again: the doorknob. 2018. In: LIALINA, O. **Turing complete user**: resisting alienation in Human Computer Interaction. Berlin: Arthistoricum.net, Heidelberg University Library, 2021.

LÖFGREN, Karl; WEBSTER, C William R. **The value of Big Data in government**: The case of 'smart cities'. Big Data & Society, 7(1). 2020. Disponível em: <https://doi.org/10.1177/2053951720912775>. Acesso em: 18 dez. 2023.

MACHULETZ, D.; BÖHM, R. **Multiple purposes, multiple problems**: a user study of consent dialogs after GDPR. Proceedings on Privacy Enhancing Technologies (2): 481-498. 2020. Disponível em: <https://doi.org/10.48550/arXiv.1908.10048>. Acesso em: 23 jun. 2023.

MAFRA, W. A. A privacidade como direito fundamental da pessoa humana. In: DAWBOR, L (Org). **Sociedade vigiada**. São Paulo: Autonomia Literária, 2020.

MARTINUZZO, J. A. **Governo eletrônico no Brasil**: paradigmas políticos da gênese. IP - Informatica Publica, Belo Horizonte, v.9, n.2, p.15-28, Dez 2007. Disponível em: http://www.pbh.gov.br/informaticapublica/ANO9_N2_PDF/governo-eletronico-brasil.pdf. Acesso em: 13 nov. 2023.

MATHEUS, R.; JANSSEN, M.; JANOWSKI, T. **Design principles for creating digital transparency in government**. 2021. Disponível em: <https://doi.org/10.1016/j.giq.2020.101550>. Acesso em: 25 nov. 2023.

- MATOS NETO, E. O. **Governo móvel no Brasil**: uma análise do estado da arte no desenvolvimento de aplicativos móveis por instituições do setor público brasileiro. Tese (doutorado em Comunicação) - Universidade Federal da Bahia, Salvador, 2020.
- MANZINI, E. **Design: quando todos fazem design**: uma introdução ao design para inovação social. São Leopoldo: Editora UNISINOS, 2017.
- McNEIL, J. **Lurking**: how a person became a user. Nova York: MCD Farrar, Straus and Giroux, 2020.
- MINAYO, M. C. de S. **Pesquisa social**: teoria, método e criatividade. 21. ed. Petrópolis: Editora Vozes, 2002.
- MONT'ALVÃO, C.; MORAES, A. **Ergonomia**: conceitos e aplicações. Rio de Janeiro: 2AB, 2010.
- MONT'ALVÃO, C. **Linguagem cidadã e design da informação**: aproximações. Actas de Diseño, Vol 16, Issue 37, p64. 2021. Disponível em: <https://doi.org/10.18682/add.vi37>. Acesso em: 23 jun. 2023.
- MORAES, A. **Ergonomia, Ergodesign e usabilidade**: algumas histórias, precursores : divergências e convergências. Ergodesign & HCI, v. 1, n. 1, p. 1-9. 2013 Disponível em: <http://dx.doi.org/10.22570/ergodesignhci.v1i1.41>. Acesso em: 09 mar. 2023.
- MORAIS, E. M. de; LOPER, A. A. **Interação humano-computador**. Londrina: UNOPAR, 2014.
- MOREIRA, H.; CALEFFE, L. G. **Metodologia da pesquisa para o professor pesquisador**. 2. ed. Rio de Janeiro: Lamparina, 2008.
- NETTO, V. A. A importância de regulamentar e proteger os dados pessoais. In: DAWBOR, L. (Org). **Sociedade vigiada**. São Paulo: Autonomia Literária, 2020.
- NIELSEN, J. **10 Usability Heuristics for User Interface Design**. 1990. Disponível em: <https://www.nngroup.com/articles/ten-usability-heuristics/>. Acesso em: 07 fev. 2023.
- NORMAN, D. A. **O design do dia a dia**. São Paulo: Anfiteatro, 2018.
- _____. **Design for a better world**: meaningful, sustainable, humanity centered. Cambridge: The MIT Press, 2023.
- OLIVEIRA, F. C. de M. B.; OLIVEIRA, F. A. de M. B. **Interação Humano Computador**. Fortaleza: Ed UECE, 2015.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Peer Review OCDE Skills**: revisão do governo digital do Brasil rumo à transformação digital do setor público - conclusões preliminares. 2018. Disponível em: <http://repositorio.enap.gov.br/handle/1/3627>. Acesso em: 13 nov. 2023.

PARINI, F.; PEGORARO, L. **O Direito à privacidade e à imagem nas cidades inteligentes**. Revista da Faculdade de Direito da FMP, v. 16, n. 2, p. 159 - 178, 16 dez. 2021. Disponível em: <https://doi.org/https://doi.org/10.53929/rfdf.v16i2.233>. Acesso em: 08 dez. 2023.

PIRES, H. F. de M. P. **Impactos da Linguagem Simples na compreensibilidade da informação em governo eletrônico**: o caso de um benefício do INSS. Dissertação (mestrado em Design) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2021.

PORTO, A. G.; FREES, C.; DORIA, F.; CAMPOLARGO, M. **O Futuro é das chics**: como construir agora as cidades humanas, inteligentes, criativas e sustentáveis. Brasília: IBCIHS, 2020.

PRIVACY INTERNATIONAL. **RELATÓRIO DA SOCIEDADE CIVIL 41ª Sessão da Revisão Periódica Universal**: Brasil Uma submissão realizada por Privacy International e Derechos Digitales. 2022. Disponível em: <https://www.derechosdigitales.org/wp-content/uploads/PT-UPR-41a-Session-Brasil-updated.pdf>. Acesso em: 23 jan. 2024.

PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho. 2. ed. Novo Hamburgo: Feevale, 2013.

REIA, J.; BELLI, L. **Smart Cities no Brasil**: regulação, tecnologia e direitos. Belo Horizonte: Casa do Direito, 2021.

RENNÓ, R. **Smart cities e big data**: o cidadão produtor de dados. URBS. Revista de Estudios Urbanos y Ciencias Sociales. Volumen 6, número 2, páginas 13-24. 2016. Disponível em: <http://hdl.handle.net/10835/4777>. Acesso em: 12 dez. 2023.

REZENDE, L. V. R.; CRUZ-RIASCOS, S. A.; RODRIGUES, A. C. T. **Dados abertos em cidades inteligentes**: uma análise da fronteira entre acesso e privacidade. 2019. Disponível em: <http://hdl.handle.net/10760/38639>. Acesso em: 08 dez. 2023.

RIVANDEIRA, J. E.; SILVA, J. S.; COLOMO-PALACIOS, R.; RODRIGUES, A.; BOAVIDA, F. **User-centric privacy preserving models for a new era of the**

internet of things. Journal of Network and Computer Applications, vol 217, 103695. 2023. Disponível em: <https://doi.org/10.1016/j.jnca.2023.103695>. Acesso em: 02 fev. 2024.

RODRIGUES, A. D'. M. V. **“O Direito à Smart City”**: desafios da integração das tecnologias digitais e da coesão socio-espacial. 2021. Dissertação (Mestrado em Geografia Humana: Globalização Sociedade e Território) - Universidade de Lisboa, Lisboa, 2021.

ROGERS, Y.; SHARP, H.; PREECE, J. **Design de Interação**: além da interação homem-computador. São Paulo: Bookman, 2005.

ROGERS, Y.; DOURISH, P.; OLIVIER, P.; BRERETON, M.; FORLIZZI, J. **The dark Side of Interaction Design**. CHI'20 Extended Abstracts. 2020. Disponível em: <https://doi.org/10.1145/3334480.3381070>. Acesso em: 29 mar. 2024.

ROMANI, G. F.; PINOCHET, L. H. C.; PARDIM, V. I.; SOUZA, C. A. de. **A segurança como fator-chave para a cidade inteligente, a confiança dos cidadãos e o uso de tecnologias**. Rev. Adm. Pública 57 (2). 2023. Disponível em: <https://doi.org/10.1590/0034-761220220145>. Acesso em: 08 dez. 2023.

SANTOS, A. dos; DAROS, C.; DUDERSTADT, A.; OLIVEIRA, A. A.; SCHULENBURG, R.; QUINTAS, R. K. Revisão bibliográfica sistemática. in: SANTOS, A. dos. (Org). **Seleção do método de pesquisa: guia para pós-graduandos em design e áreas afins**. Curitiba: Insight, 2018.

SÃO LUÍS. **Plano São Luís inteligente**. 2023. Disponível em: <https://saoluis.ma.gov.br/saoluisinteligente>. Acesso em: 13 dez. 2023.

SAURA, J. R.; RIBEIRO-SORIANO, D.; PALACIOS-MARQUÉS, D. **Assessing behavioral data science privacy issues in government artificial intelligence deployment**. 2022. Disponível em: <https://doi.org/10.1016/j.giq.2022.101679>. Acessado em: 02 fev. 2024.

SCHLEMMER, A.; PADOVANI, S. **Mapeamento sobre a experiência prévia com design centrado no usuário (DCU) de desenvolvedores de sistemas e-gov**. Ergodesign & HCI v. 9, n. 2, p. 67-86. 2021. Disponível em: <http://dx.doi.org/10.22570/ergodesignhci.v9i2.1585>. Acesso em: 02 abr. 2024.

SCHWARTZMAN, S. **Pesquisa acadêmica, pesquisa básica e pesquisa aplicada em duas comunidades científicas**. 1979. Disponível em: http://www.schwartzman.org.br/simon/acad_ap.htm. Acesso em: 17 mar. 2023.

SILVA, G. A. da. **Uma perspectiva crítica para as políticas públicas de inclusão digital no Brasil**: estudo de caso sobre não-usos e não-usuários de internet. 2020. Dissertação (Mestrado em Tecnologia e Sociedade) - Universidade Tecnológica Federal do Paraná, Curitiba, 2020.

SILVA, M. da; BERNARDINI, J. V.; BERNARDINI, F.; MACIEL, C. **Requisitos de privacidade para aplicações de crowdsourcing no contexto das cidades inteligentes**. 2019. Disponível em: <https://doi.org/10.5753/ihc.2019.8432>. Acesso em: 08 dez. 2023.

SILVA, V. H. S. Em 2021, **28 milhões de pessoas no Brasil não usaram a internet, diz IBGE. 2022**. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/09/16/em-2021-28-milhoes-de-pessoas-no-brasil-nao-usaram-a-internet-diz-ibge.ghtml>. Acesso em: 25 ago. 2023.

SOUZA, M. S. de; RIBEIRO, D. M. M. **Mensuração de desempenho em Smart Government**: análise da Estratégia de Governança Digital do Governo Federal do Brasil. CONF-IRM 2021 Proceedings. 11. 2021. Disponível em: <https://aisel.aisnet.org/confirm2021/11>. Acesso em: 13 nov. 2023.

VAZ, J. C. Administração pública e governança eletrônica: possibilidades e desafios para a tecnologia. 2002. In: **Governo Eletrônico - os desafios da participação cidadã**. Fortaleza: Fundação Konrad Adenauer, 2002.

VÉLIZ, C. **Privacidade é poder**. São Paulo: Editora Contracorrente, 2021.

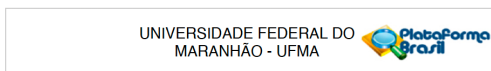
VIANA, A. C. A. **Transformação digital na administração pública**: do governo eletrônico ao governo digital. Revista Eurolatinoamericana de Derecho Administrativo, Santa Fe, vol. 8, n. 1, p. 115-136, ene. /jun. 2021. DOI 10.14409/redoeda.v8i1.103303. Acesso em: 13 nov. 2023.

WEIGL, L.; BARBEREAU, T.; FRIDGEN, G. **The construction of self-sovereign identity: extending the interpretative flexibility of technology**. Government Information Quarterly, vol 40, issue 4, 101873. 2023. Disponível em: <https://doi.org/10.1016/j.giq.2023.101873>. Acesso em: 02 fev. 2024.

ZUBOFF, S. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F.; CARDOSO, B.; KANASHIRO, M.; GUILHON, L.; MELGAÇO, L (Orgs). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018.

APÊNDICES

Apêndice A. Parecer do Comitê de Ética



PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: PROTEÇÃO DE DADOS E DA PRIVACIDADE NO GOVERNO DIGITAL

Pesquisador: FABIANA FRANCA SILVA

Área Temática:

Versão: 1

CAAE: 82857224.1.0000.5087

Instituição Proponente: Universidade Federal do Maranhão

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 7.239.705

Apresentação do Projeto:

Desenho:

A metodologia de pesquisa adotada utiliza uma combinação de métodos mistos a ser realizada em quatro etapas. Quanto à sua natureza, ela é classificada como aplicada, devido ao seu objetivo em "gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos" (Prodanov; Freitas, 2013, p. 51). Assim como pelo seu enfoque nas questões e compreensão da privacidade no governo digital face à LGPD para

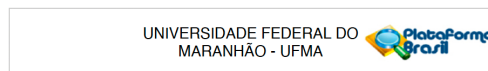
construção de um ambiente mais seguro. Em relação aos objetivos, a pesquisa apresenta caráter descritivo. A partir do intento de descrever "características de determinada população ou fenômeno" (Gil, 2008, p. 42). Sendo isso o entendimento da população de interesse a respeito das políticas de privacidade.

Resumo: A eficiência da prestação de serviços on-line está diretamente relacionada à quantidade e qualidade de dados que esses obtêm dos seus usuários. Nesse contexto, as ameaças à privacidade se tornam ainda mais reais, reverberando em diretrizes como a Lei Geral de Proteção de Dados

Pessoais brasileira, a LGPD. Contudo, a forma como as políticas de privacidade e os termos de

Endereço: Avenida dos Portugueses, 1966 CEB Velho Cidade Universitária Dom Delgado
Bairro: Bacanga **CEP:** 65.080-805
UF: MA **Município:** SAO LUIS
Telefone: (98)3272-8708 **E-mail:** cepufma@ufma.br

Página 01 de 07



Continuação do Parecer: 7.239.705

consentimento, determinados pela LGPD, são apresentados aos cidadãos são complexas, comprometendo a usabilidade das interfaces que as expõem aos cidadãos. Dessa forma, sob a ótica do design, como objetivo principal, busca-se apontar diretrizes mais amigáveis e centradas nos cidadãos para garantia da privacidade e proteção aos dados pessoais no governo digital. Esta pesquisa justifica-se pela importância do e-gov para o exercício da cidadania do indivíduo, sendo seu uso uma forma de inclusão digital e inovação pública. Além de propor o Design como um mediador que aponte caminhos para um acesso consciente e saudável dos usuários. Com esse propósito, foram realizadas pesquisas bibliográfica e documental a fim de construir um referencial que consubstancie a justificativa da pesquisa. Serão usados procedimentos metodológicos como entrevista acompanhada de desenho e a aplicação de questionário. Por fim, espera-se que esta pesquisa, além de contribuir cientificamente com o campo do design, devido ao seu viés interdisciplinar, possa cooperar com os cidadãos que utilizam os serviços do governo digital para que seu direito à privacidade seja assegurado e garantido.

Introdução:

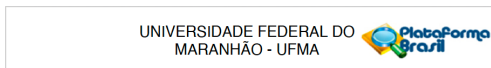
As facilidades trazidas pela era da informação são evidentes e indispensáveis em várias esferas da sociedade. Foram naturalizadas, não só em iniciativas privadas, mas também na administração pública, em sua prestação de serviços à população. No Estado, esse cenário é visto na consolidação do governo digital, uma estrutura que propõe sua desburocratização e modernização, aproximando-o do cidadão (Brasil, 2021).

O governo digital é a evolução do governo eletrônico, cuja principal característica era a automatização de processos e documentos impulsionado pela evolução tecnológica e pela globalização (OCDE, 2018). Essa transformação foi norteada por diferentes fases da web e aplicação das Tecnologias da Informação e Comunicação (TICs), recursos tecnológicos usados para mediar e automatizar a comunicação e a informação

(Cristóvam et al., 2020). Atualmente a estrutura pública digital propõe a autonomia do cidadão, assim como sua inclusão digital, na obtenção de serviços e políticas públicas (Brasil, 2021a).

Endereço: Avenida dos Portugueses, 1966 CEB Velho Cidade Universitária Dom Delgado
Bairro: Bacanga **CEP:** 65.080-805
UF: MA **Município:** SAO LUIS
Telefone: (98)3272-8708 **E-mail:** cepufma@ufma.br

Página 02 de 07



Continuação do Parecer: 7.239.705

Além disso, os artefatos do dia a dia também se tornaram conectáveis à internet, um conceito conhecido por Internet das Coisas (IoT) (Kreuz; Viana, 2019). Assim como as cidades convertem-se em inteligentes, recorrendo à aplicação de TICs e IoTs aos elementos do ambiente na busca por soluções para melhorar a qualidade de vida dos seus cidadãos. O objetivo é apresentar uma gestão mais transparente e eficiente (Reis; Bell, 2021).

Dessa forma, a rede conecta não apenas máquinas, mas ambientes, pessoas e organizações. Para que sejam eficientes, os serviços precisam de informações dos usuários, dados pessoais que são obtidos da rede. Assim é possível aprimorar

ações e personalizar ainda mais os serviços prestados. Coletar, tratar e armazenar dados mostra-se uma prática comercial e política a depender dos interesses de quem os detém e utiliza. Isso estabelece uma realidade de capitalismo de dados (Zuboff, 2018), em que o lucro sobre as informações a despeito do consentimento e compreensão afeta sistemas, empresas e governos.

A produção de dados digitais atualmente é inevitável. Diante dos interesses econômicos relacionados a eles, a privacidade, um direito fundamental e subjetivo, precisa ser considerada nos serviços que envolvam dados pessoais (Véliz, 2021). Tal contexto

alavanca regulamentações que fiscalizem e garantam a preservação da privacidade dos cidadãos diante do sistema de coleta de dados. A Lei Geral de Proteção de Dados brasileira (LGPD), Lei nº 13.709/2018, zela para que os cidadãos sejam informados desde o princípio que seus dados estão sendo coletados, como estão sendo e que

tratamento receberão pelos operadores das entidades coletoras (Brasil, 2020). A LGPD é visualizada, de forma prática, pela presença de pop-ups de aceitação e gerenciamento de cookies, caixas de diálogo e links que levam ao

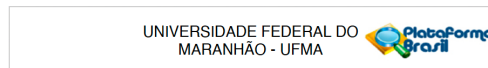
texto das políticas de privacidade e dos termos de consentimento em sites, plataformas e aplicativos. O que é apresentado aos usuários nessas telas é o que é determinado nos parágrafos e incisos da LGPD, embora em formas complexas. São recorrentes as expressões jurídicas para

explicar o objetivo e etapas de documentos e ações. Segundo a pesquisa Privacidade e Proteção de Dados Pessoais 2021, do Comitê Gestor da Internet no Brasil (2022), quanto à leitura de políticas de

privacidade nas telas de sites e aplicativos no país, 81% dos usuários de internet não as lêem

Endereço: Avenida dos Portugueses, 1966 CEB Velho Cidade Universitária Dom Delgado
Bairro: Bacanga **CEP:** 65.080-805
UF: MA **Município:** SAO LUIS
Telefone: (98)3272-8708 **E-mail:** cepufma@ufma.br

Página 03 de 07



Continuação do Parecer: 7.239.705

integralmente por serem muito longas e 69% por

considerarem-nas difíceis de entender.

Metodologia Proposta:

Esta pesquisa é desenvolvida em quatro etapas. A primeira consiste em pesquisa bibliográfica e documental, onde serão realizadas revisões sistemáticas e narrativas a partir da literatura existente a fim de constituir o referencial teórico do trabalho.

Na segunda etapa, o objetivo é conhecer percepções que usuários têm sobre privacidade e proteção de dados pessoais a partir da realização de Entrevista acompanhada de desenho, ou Sketch Interview. Como público de interesse, serão recrutados dois grupos de pelo menos 10 pessoas cada.

Um grupo composto por usuários frequentes do app VIVA PROCONMA, pessoas que já tenham utilizado pelo menos dois serviços diferentes do aplicativo. O outro grupo será

formado por usuários não frequentes do app VIVA PROCONMA, pessoas que já tenham utilizado ou não ao menos um serviço do app VIVA

PROCONMA. Ambos participarão apenas após assinatura do Termo de Consentimento Livre e Esclarecido (TCLE). Nesta pesquisa, a sketch

interview será operada em dois momentos. No primeiro, ela seguirá a seguinte ordem: **ETAPA A:** breve abordagem oralizada explicativa sobre o contexto, além da distribuição de papel sulfite, canetas coloridas e notas autoadesivas; **ETAPA B:** Entrevista e Produção do desenho pelos

participantes; **ETAPA C:** Explicação verbal do participante sobre seu desenho; **ETAPA D:** Aproximação, com a sensibilização oralizada a respeito

das políticas de privacidade, dos termos de consentimento, das caixas de diálogo e da LGPD de forma sintetizada; **ETAPA E:** Conclusão da produção do desenho pelo participante. Haverá um intervalo de duas semanas e após esse período será

cumprido o segundo momento da entrevista. Esse, consiste na **ETAPA F:** Retorno. Nela, o participante poderá rever a sua produção e

confrontar isso com as experiências que teve nas últimas duas semanas após ser sensibilizado a respeito das políticas de privacidade, dos termos de consentimento, das caixas de diálogos e da

LGPD. Já na terceira etapa, para indicar como usuários do governo digital interagem com as políticas de privacidade e com os termos de

Endereço: Avenida dos Portugueses, 1966 CEB Velho Cidade Universitária Dom Delgado
Bairro: Bacanga **CEP:** 65.080-805
UF: MA **Município:** SAO LUIS
Telefone: (98)3272-8708 **E-mail:** cepufma@ufma.br

Página 04 de 07

UNIVERSIDADE FEDERAL DO
MARANHÃO - UFMA



Continuação do Parecer: 7.239.705

consentimento, serão aplicados questionários on-line e presencialmente. Na quarta e última etapa será realizada a análise dos dados obtidos. O objetivo é correlacionar as percepções e interações e a forma como as plataformas apresentam as políticas de privacidade para entender os caminhos de abordagem da privacidade e da proteção de dados.

Metodologia de Análise de Dados:

As entrevistas serão analisadas por meio triangulação dos dados: informações recebidas a partir do desenho, respostas ou mudanças de pensamento após a etapa de aproximação e explicações dados pelos entrevistados a respeito do próprio desenho. Além disso, também haverá análise das falas das entrevistas via codificação seletiva de dados, por meio de software de análise. Por fim, as entrevistas serão analisadas via tabulação de dados.

Desfecho Primário:

Apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital.

Tamanho da Amostra no Brasil 70

Objetivo da Pesquisa:

Sob a ótica do design e a partir da proposta de desburocratização, acessibilidade, emancipação e letramento digital o objetivo geral deste trabalho é:

Apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital.

Avaliação dos Riscos e Benefícios:

Riscos:

Os riscos serão mínimos aos participantes desta pesquisa, relacionados ao desconforto emocional frente à resposta do questionário e das entrevistas relacionados à temática proteção de dados pessoais e da privacidade no governo digital. Os riscos serão minimizados através de esclarecimentos prévios sobre a pesquisa e pela aplicação de pré-testes. Além disso, a garantia do anonimato será assegurada.

Benefícios:

O participante não receberá qualquer remuneração. A participação nesse estudo contribuirá para os debates acerca da proteção da privacidade e

Endereço: Avenida dos Portugueses, 1966 CEB Velho Cidade Universitária Dom Delgado
Bairro: Bacanga **CEP:** 65.080-805
UF: MA **Município:** SAO LUIS
Telefone: (98)3272-8708 **E-mail:** cepufma@ufma.br

UNIVERSIDADE FEDERAL DO
MARANHÃO - UFMA



Continuação do Parecer: 7.239.705

de dados pessoais com o intuito de conscientizar os cidadãos sobre o assunto. Os benefícios não são diretos e imediatos.

Comentários e Considerações sobre a Pesquisa:

A investigação tem relevância acadêmica.

Considerações sobre os Termos de apresentação obrigatória:

O TCLE está redigido adequadamente e de acordo com a Resolução CNS n. 466/12.

Recomendações:

Não há recomendações.

Conclusões ou Pendências e Lista de Inadequações:

Não há pendências.

Considerações Finais a critério do CEP:

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMACOES_BASICAS_DO_PROJETO_2378197.pdf	27/08/2024 12:01:43		Aceito
Folha de Rosto	folhaDeRosto_assinado2.pdf	27/08/2024 12:00:55	FABIANA FRANCA SILVA	Aceito
Outros	declaracao_local_de_coleta_de_dados.pdf	26/08/2024 07:13:10	FABIANA FRANCA SILVA	Aceito
Projeto Detalhado / Brochura Investigador	PROJETO_comite_etica_privacidadegov digital.pdf	26/07/2024 11:48:23	FABIANA FRANCA SILVA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	QUESTIONARIO_ONLINE_TCLE.pdf	25/07/2024 19:35:57	FABIANA FRANCA SILVA	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	Entrevista_TCLE.pdf	25/07/2024 19:35:42	FABIANA FRANCA SILVA	Aceito
Orçamento	ORCAMENTO_comite_etica.pdf	25/07/2024 19:32:21	FABIANA FRANCA SILVA	Aceito
Cronograma	CRONOGRAMA_pesquisa_comite_etica.pdf	25/07/2024 19:30:38	FABIANA FRANCA SILVA	Aceito

Situação do Parecer:

Endereço: Avenida dos Portugueses, 1966 CEB Velho Cidade Universitária Dom Delgado
Bairro: Bacanga **CEP:** 65.080-805
UF: MA **Município:** SAO LUIS
Telefone: (98)3272-8708 **E-mail:** cepufma@ufma.br

Página 06 de 07

UNIVERSIDADE FEDERAL DO
MARANHÃO - UFMA



Continuação do Parecer: 7.239.705

Aprovado

Necessita Apreciação da CONEP:

Não

SAO LUIS, 21 de Novembro de 2024

Assinado por:
Emanuel Pércles Salvador
(Coordenador(a))

Apêndice B. TCLE *Sketch Interview*

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Título da pesquisa: Proteção de dados pessoais e da privacidade no governo digital

Nome da pesquisadora responsável: Fabiana França Silva

Nome da orientadora da pesquisa: Prof^a Dr^a Cláudia Renata Mont'Alvão Bastos Rodrigues

Gostaríamos de convidar você a participar como voluntária (o) de uma entrevista semiestruturada acompanhada de desenho/esquema. O estudo é uma etapa da dissertação que estamos desenvolvendo no Programa de Pós Graduação em Design, da Universidade Federal do Maranhão (UFMA).

OBJETIVO

O objetivo do estudo é apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital.

JUSTIFICATIVA

É crescente o uso de iniciativas de governo digital no país, visando oferecer serviços públicos de forma mais fácil e prática. Isso é próprio de uma sociedade em rede. Nela, dados dos cidadãos servem como indicadores para melhorar a atuação da administração pública. Dessa forma, se revela a necessidade de estudos que contribuam para a conhecer o que os cidadãos entendem sobre o assunto, e, principalmente, para colaborar na proteção da privacidade e dos dados pessoais para que eles acessem tais serviços do governo digital com segurança e tenham seu direito à privacidade assegurado.

PROCEDIMENTOS METODOLÓGICOS

Para a realização desta etapa da pesquisa será realizada uma entrevista semiestruturada, acompanhada de desenho/esquema, com produção de um mapa mental. De forma presencial, em local de sua preferência, podendo ser também por meio remoto, *Whatsapp* ou plataforma de videoconferência, como o *Zoom* ou *Google Meet* por meio de dois encontros com um intervalo de duas semanas entre cada um.

A pesquisadora a) apresentará a pesquisa e os objetivos da sua realização; b) seguirá um roteiro com questionamentos referentes ao seu entendimento sobre privacidade e proteção de dados; c) convidará o participante a produzir um mapa mental que ilustre as suas ideias; d) explicará sobre LGPD, consentimento, políticas de privacidade e termos de consentimento, e caixas de diálogo utilizando a interface do aplicativo VIVA PROCON/MA e convidará o participante a concluir o mapa mental após as informações repassadas; e após um intervalo de duas semanas e) pedirá que o participante reveja seu mapa mental e respostas entre o primeiro e segundo momento da entrevista.

A entrevista será gravada por meio de áudio, para posterior transcrição e melhor análise das informações obtidas.

RISCOS

Os riscos aos participantes desta pesquisa são mínimos. Eles estão relacionados a desconforto emocional frente à resposta da entrevista relacionado à temática proteção de dados pessoais e da privacidade no governo digital. Os riscos serão minimizados através de esclarecimentos prévios sobre a pesquisa. Além disso, a garantia do anonimato é assegurada.

BENEFÍCIOS

Você não receberá qualquer remuneração. A participação nesse estudo contribuirá para os debates acerca da proteção da privacidade e de dados pessoais com o intuito de conscientizar os cidadãos sobre o assunto. Os benefícios não são diretos e imediatos.

CUSTOS

Você não terá qualquer custo para participar do estudo.

CONFIDENCIALIDADE DO ESTUDO

Os resultados desta pesquisa serão utilizados somente para fins científicos. O registro de sua participação será mantido confidencialmente. Nas publicações e/ou relatórios resultantes deste trabalho a identificação dos participantes não será revelada. Apenas o seu mapa mental será utilizado como forma de ilustrar os resultados da pesquisa. Seu nome, imagem e voz não aparecerão em nenhuma publicação sobre a pesquisa. Todo material de registro em áudio, vídeo ou fotografia será tratado como confidencial e restrito para uso acadêmico.

PARTICIPAÇÃO VOLUNTÁRIA

A sua participação é voluntária. O(A) Sr(a). tem plena liberdade de recusar-se a participar ou retirar seu consentimento, em qualquer fase da pesquisa, sem penalização alguma. A recusa em participar não acarretará qualquer penalidade ou modificação da forma em que é atendido pelo pesquisador.

ESCLARECIMENTOS

O(A) Sr(a). receberá uma via do Termo de Consentimento Livre e Esclarecido. O(A) Sr(a). pode entrar em contato com a pesquisadora responsável a qualquer tempo para informação adicional no e-mail fabiana.fs@discente.ufma.br. O(A) Sr(a). também pode entrar em contato com o Comitê de Ética em Pesquisa da UFMA, Endereço O CEP/UFMA está localizado no Prédio CEB Velho, em frente ao Auditório Sérgio Ferretti. E-mail:

cepufma@ufma.br. Telefone: 3272- 8708. E com a Comissão Nacional de Ética em Pesquisa (CONEP), quando pertinente.

Um Comitê de Ética em Pesquisa é um grupo não remunerado formado por diferentes profissionais e membros da sociedade que avaliam um estudo para julgar se ele é ético e garantir a proteção dos participantes

Caso aceite o convite de participar desta pesquisa, solicitamos sua rubrica em todas as suas páginas e sua assinatura ao seu término.

Este TCLE é apresentado em duas vias, sendo uma cópia pertencente ao pesquisador responsável e a outra ao participante de pesquisa.

CONSENTIMENTO PÓS-INFORMAÇÃO

Assinatura do participante

Assinatura da pesquisadora

São Luís _____ de _____ de _____.

Apêndice C. Pauta da entrevista

ETAPA A. Breve abordagem explicativa sobre o contexto

Com usuários frequentes do *app* VIVA PROCON MA

Pesquisadora: Olá.

Esta entrevista se trata de uma pesquisa de mestrado em design da Universidade Federal do Maranhão.

A partir de agora as nossas falas serão gravadas para que possam ser transcritas e utilizadas para construir a pesquisa, conforme o seu consentimento.

Pesquisadora: Atualmente os governos federal, estadual e municipal oferecem *sites* e aplicativos para que a população tenha acesso aos seus serviços. Um deles é o do VIVA PROCON, do Governo do Maranhão, do qual você é usuário. Minha intenção é saber como você, ao utilizar serviços assim, que representam o governo digital, percebe a privacidade, e também as suas opiniões e sentimentos.

Com usuários não-frequentes do *app* VIVA PROCON MA

Pesquisadora: Olá.

Esta entrevista se trata de uma pesquisa de mestrado em design da Universidade Federal do Maranhão.

A partir de agora as nossas falas serão gravadas para que possam ser transcritas e utilizadas para construir a pesquisa, conforme o seu consentimento.

Pesquisadora: Atualmente os governos federal, estadual e municipal oferecem *sites* e aplicativos para que a população tenha acesso aos seus serviços. Como o *app* do VIVA PROCON Maranhão, por exemplo. Minha intenção é saber como você, ao utilizar serviços assim, que representam o governo digital, percebe a privacidade, e também as suas opiniões e sentimentos.

Pesquisadora: Sinta-se livre para responder da forma que for melhor para você. Não há certo ou errado, o objetivo é conhecer a sua opinião.

1) O que você entende como privacidade? e privacidade de dados digitais?

2) Você sabe o que pode ser feito com esses seus dados digitais?

Entrega dos Materiais

Serão disponibilizados 1 folha de papel e canetas coloridas.

ETAPA B. Produção do mapa mental pelo participante

Pesquisadora: Gostaria que você escrevesse no mapa mental as palavras que vem a sua mente quando você pensa sobre isso.

ETAPA C. Explicação verbal do participante sobre o seu mapa mental

Pesquisadora: Agora gostaria que você me explicasse quais palavras escolheu e o por quê.

ETAPA D. Aproximação e conclusão do mapa mental pelo participante

Entrega do texto dos cartões para o participante ou leitura com a pesquisadora.

Pesquisadora: Gostaria de apresentar a você alguns conceitos relacionados à privacidade e proteção de dados.

Pesquisadora: Eu gostaria que você refletisse se essas informações tiveram algum impacto em você, no que produziu antes e nas suas ideias e expectativas sobre esse assunto daqui para frente.

Pesquisadora: Gostaria de saber se você deseja complementar o mapa mental com mais ideias, ou fazer outro comentário.

INTERVALO ENTRE MOMENTO I E II

ETAPA F. Retorno

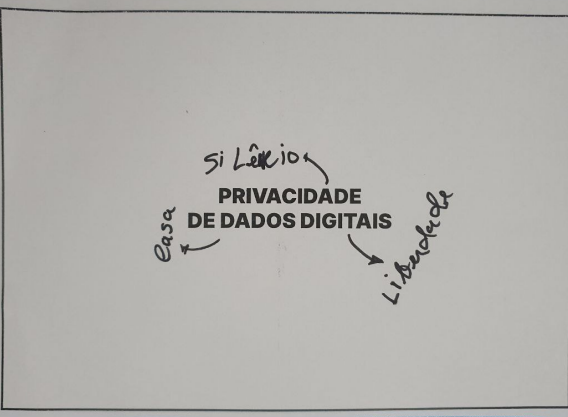
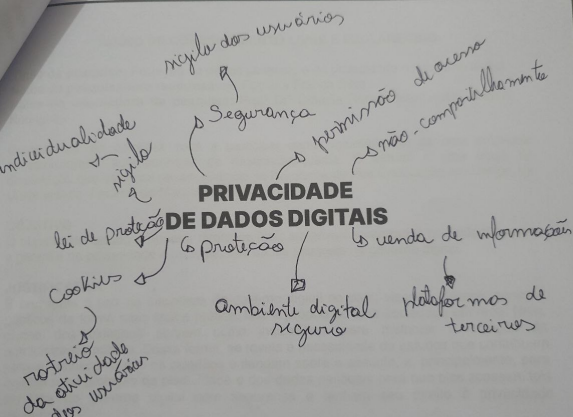
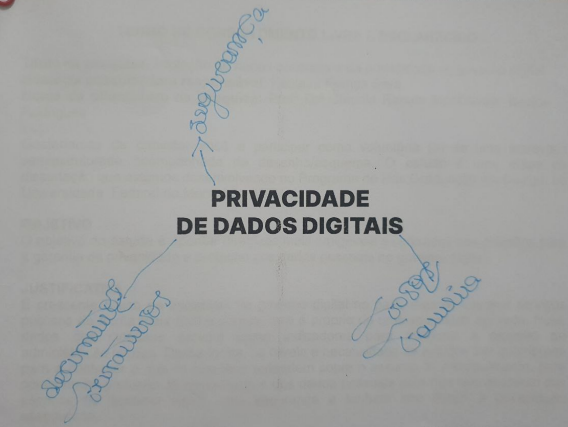
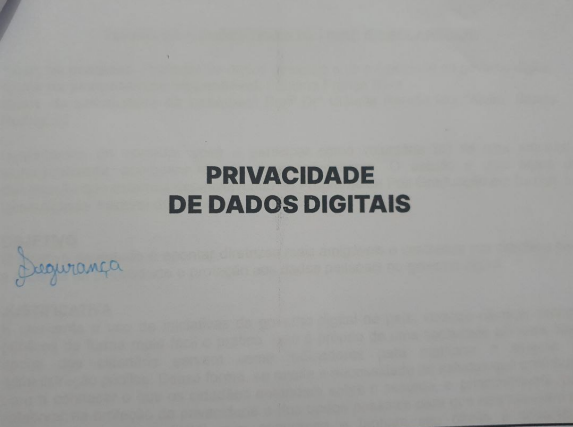
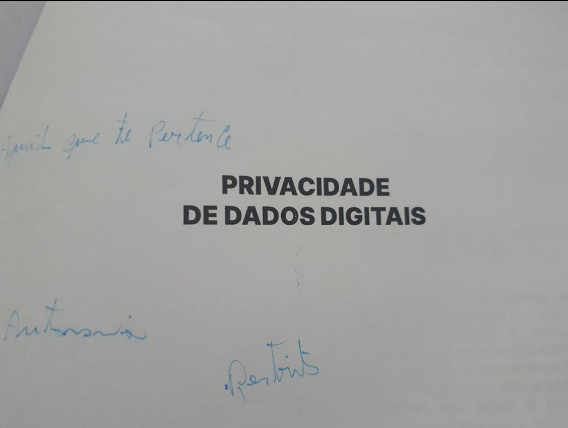
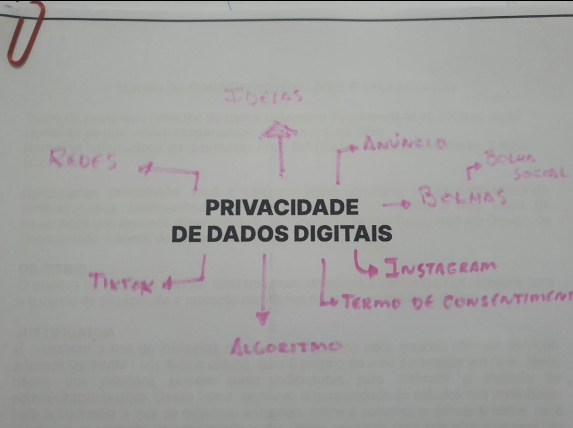
Pesquisadora: No nosso reencontro, aqui está o mapa mental que você produziu. Gostaria que você olhasse para ele e lembrasse dos últimos dias, depois da nossa primeira conversa.

Você gostaria de acrescentar algo?

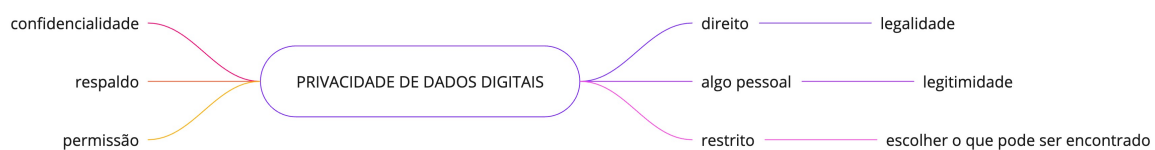
O que mudou para você em relação às políticas de privacidade, ao consentimento e ao governo digital?

Há alguma coisa que você gostaria de sugerir ou comentar sobre as políticas de privacidade e termos de consentimento do seu ponto de vista de cidadão?

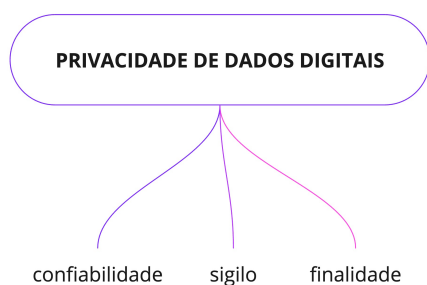
Apêndice D. Mapas mentais produzidos pelos participantes

	
E1 - F - 60 a 64	E3 - M - 25 a 29
	
E6 - F - 55 a 60	E7 - M - 25 a 29
	
E11 - M - 30 a 34	E12 - F - 20 a 24

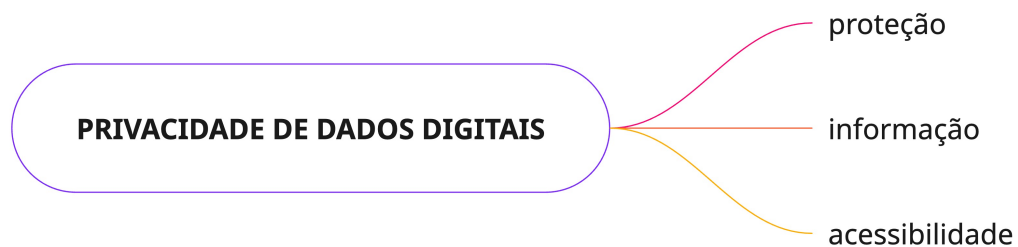
Consumo Propaganda direcionamentos alinhados com os hábitos digitais de usuários Rastreamento de informações, hábitos. PRIVACIDADE DE DADOS DIGITAIS	Redes sociais algoritmo Invasão cookies Capitalismo PRIVACIDADE DE DADOS DIGITAIS
E13 - F - 30 a 34	E15 - M - 20 a 24
PRIVACIDADE DE DADOS DIGITAIS Confiança liberdade	BLOQUEAR CONFIRMAÇÃO SENHA PRIVACIDADE DE DADOS DIGITAIS
E16 - F - 25 a 29	E17 - M - 20 a 24
sigilo p dados Respeito Só uma pessoa pode saber não pode ser violada PRIVACIDADE DE DADOS DIGITAIS	bancos de dados marketing privacidade de dados digitais informações pessoais
E21 - F - 60 a 64	E26 - F - 18 a 19



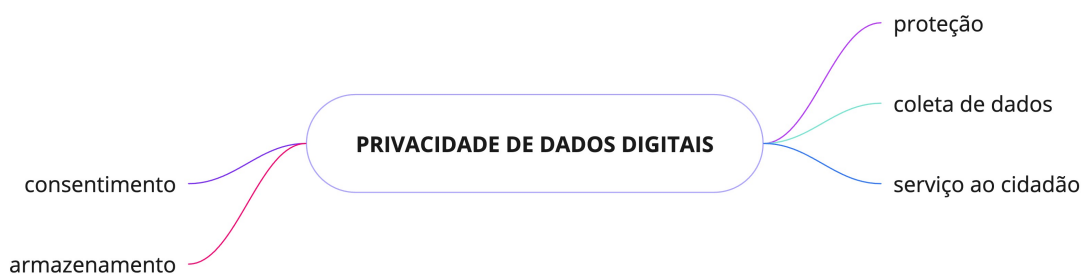
E22 - F - 30 a 34



E23 - M - 40 a 44



E24 - F - 45 a 49



E25 - M - 45 a 49

Apêndice E. TCLE Questionário

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Título da pesquisa: Proteção de dados pessoais e da privacidade no governo digital

Nome da pesquisadora responsável: Fabiana França Silva

Nome da orientadora da pesquisa: Prof^a Dr^a Cláudia Renata Mont'Alvão Bastos Rodrigues

Gostaríamos de convidar você a participar como voluntária (o) de um questionário. O estudo é uma etapa da dissertação que estamos desenvolvendo no Programa de Pós Graduação em Design, da Universidade Federal do Maranhão (UFMA).

OBJETIVO

O objetivo do estudo é apontar diretrizes mais amigáveis e centradas nos cidadãos para a garantia da privacidade e proteção aos dados pessoais no governo digital.

JUSTIFICATIVA

É crescente o uso de iniciativas de governo digital no país, visando oferecer serviços públicos de forma mais fácil e prática. Isso é próprio de uma sociedade em rede. Nela, dados dos cidadãos servem como indicadores para melhorar a atuação da administração pública. Dessa forma, se revela a necessidade de estudos que contribuam para a conhecer o que os cidadãos entendem sobre o assunto, e, principalmente, para colaborar na proteção da privacidade e dos dados pessoais para que eles acessem tais serviços do governo digital com segurança e tenham seu direito à privacidade assegurado.

PROCEDIMENTOS METODOLÓGICOS

Para a realização desta etapa da pesquisa, você preencherá este formulário on-line que foi pré-estruturado sobre o tema elencado no título da dissertação.

RISCOS

Os riscos aos participantes desta pesquisa são mínimos. Eles estão relacionados a desconforto emocional frente à resposta da entrevista relacionado à temática proteção de dados pessoais e da privacidade no governo digital. Os riscos serão minimizados através de esclarecimentos prévios sobre a pesquisa. Além disso, a garantia do anonimato é assegurada.

BENEFÍCIOS

Você não receberá qualquer remuneração. A participação nesse estudo contribuirá para os debates acerca da proteção da privacidade e de dados pessoais com o intuito de conscientizar os cidadãos sobre o assunto. Os benefícios não são diretos e imediatos.

CUSTOS

Você não terá qualquer custo para participar do estudo.

CONFIDENCIALIDADE DO ESTUDO

Os resultados desta pesquisa serão utilizados somente para fins científicos. O registro de sua participação será mantido confidencialmente. Nas publicações e/ou relatórios resultantes deste trabalho a identificação dos participantes não será revelada. Seu nome, endereço de email ou quaisquer dados digitais que o identificam e individualizam não aparecerão em nenhuma publicação sobre a pesquisa.

PARTICIPAÇÃO VOLUNTÁRIA

A sua participação é voluntária. O(A) Sr(a). tem plena liberdade de recusar-se a participar ou retirar seu consentimento, em qualquer fase da pesquisa, sem penalização alguma. A recusa em participar não acarretará qualquer penalidade ou modificação à forma em que é atendido pelo pesquisador.

CONSENTIMENTO PÓS-INFORMAÇÃO

Ao prosseguir você confirma o aceite de participação nesta pesquisa.

Apêndice F. Questionário

0.1 Você já utilizou o aplicativo VIVA PROCON/MA?

- ☐ Não
☐ Sim, já utilizei para 1 serviço
☐ Sim, já utilizei para mais de 2 serviços diferentes

0.2 Você é funcionário ou recebe benefícios do governo?

- ☐ Sim ☐ Não

0.3 Quando você precisa de algum serviço público, de que forma você o acessa?

0.4 Com qual frequência você utiliza serviços, sites ou aplicativos de governo digital (como VIVA PROCON, Gov.br, Carteira de Trabalho, Meu SUS Digital)?

- | | |
|---------------------------------------|--|
| ☐ Não utilizo | ☐ Mensalmente |
| ☐ Diariamente | ☐ Eventualmente (a cada três ou seis meses) |
| ☐ Semanalmente | ☐ Raramente (uma vez ao ano) |

1.2 Você já ouviu falar sobre a LGPD?

- ☐ Sim ☐ Não

1.3 Você sabe se existe algum órgão que regulamenta a proteção de dados no Brasil?

- ☐ Sim ☐ Não

1.4 Se sim, qual o nome do órgão? _____

1.5 Você sabe o que são políticas de privacidade?

- ☐ Sim ☐ Não

1.6 Se sim, compartilhe o que você sabe: _____

1.7 Você sabe o que são dados sensíveis?

- ☐ Sim ☐ Não

1.8 Da lista abaixo, quais você acha que são dados sensíveis?

- | | |
|--|---|
| ☐ Nome completo | ☐ Preferências políticas |
| ☐ CPF | ☐ Opção religiosa |
| ☐ Data de nascimento | ☐ Informações de saúde, genética e biométrica |
| ☐ Endereço | ☐ Geolocalização (sua localização no momento de acessar o sistema) |
| ☐ Histórico escolar | ☐ Imagem do seu rosto |
| ☐ Informações bancárias | ☐ Todos |
| ☐ Preferências sexuais | |

1.9 Você sabe o que são Dados Abertos?

- ☐ Sim ☐ Não

1.10 Se sim, compartilhe aqui: _____

1.11 Você sabe o que são cookies?

- ☐ Sim ☐ Não

1.12 Se sim, explique a seguir: _____

1.13 Para você, é importante que seus dados digitais sejam protegidos?

☐ Sim ☐ Não

1.14 Por que você acha isso? _____

2.1 Você já deve ter percebido que precisa concordar com textos sobre a privacidade ANTES de acessar um site, serviço, app do governo digital. Você entende por quê?

☐ Sim ☐ Não

2.2 Se você respondeu sim, explique a seguir: _____

2.3 “Não me sinto incomodado quando um aplicativo do governo solicita dados pessoais”. Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.4 “Penso duas vezes antes de fornecer minhas informações pessoais em apps do governo”. Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.5 “Não tenho preocupação de que serviços do governo possam estar coletando um volume maior que o necessário dos meus dados pessoais”. Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.6 “Meus dados pessoais estão protegidos nos serviços do governo digital”.

Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.7 “Não confio no governo digital para proteger os meus dados pessoais”. Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.8 “Estar ciente de que maneira meus dados pessoais serão utilizados é muito importante para mim”. Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.9 “Não considero que meus dados pessoais sejam úteis para a administração pública e para o governo digital”. Em relação a afirmação, escolha 1 opção:

☐ concordo totalmente ☐ concordo parcialmente ☐ não concordo, nem discordo ☐ discordo parcialmente ☐ discordo totalmente

2.10 Ao ter contato com políticas de privacidade e termos de consentimento em sites, serviços, aplicativos do governo digital (ex.: app VIVA PROCON), você costuma?

Escolha 1 opção:

- ☐ aceitar sem ler
 ☐ ler parcialmente antes de aceitar
 ☐ ler a maior parte antes de aceitar
 ☐ ler completamente antes de aceitar

2.11 Ao ler políticas de privacidade e termos de consentimento do governo digital

(ex.: app VIVA PROCON), **o que você entende?** Marque 1 opção:

- ☐ não leio
 ☐ não entendo
 ☐ entendo pouco
 ☐ entendo quase tudo
 ☐ entendo tudo

2.12 Em relação à clareza quanto à proteção dos seus dados digitais, como você avalia essas iniciativas de governo digital no Maranhão?

VIVA Procon

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

APP RG digital

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

Rede wifi São Luís Digit@l

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

Central de atendimento virtual/WhatsApp (ex: marcação de consultas ou exames na rede estadual/municipal)

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

APP Detran Maranhão

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

Site de cadastro para participação do programa Transporte Universitário

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

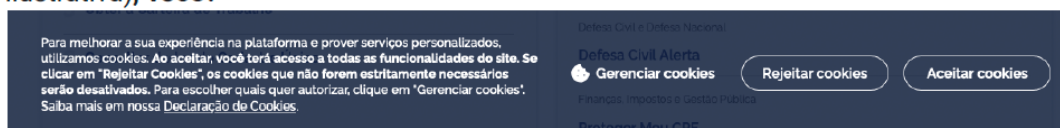
Site de cadastro para participação do programa Mais Renda

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

Site de cadastro para matrículas e rematrículas nas escolas da rede pública

- ☐ concordo totalmente
 ☐ concordo parcialmente
 ☐ não concordo, nem discordo
 ☐ discordo parcialmente
 ☐ discordo totalmente

2.13 Quanto aos botões como o "aceitar cookies" (ou "aceitar todos os cookies", "permitir todos os cookies"), "gerenciar cookies" e "rejeitar cookies" (como na imagem ilustrativa), você?



- ☐ () clica em aceitar/aceitar tudo
- ☐ () clica em gerenciar/alterar configurações dos cookies
- ☐ () clica em rejeitar/não permitir cookies

2.14 Gostaria que você explicasse a sua opção na questão anterior:

2.15 Quais as suas sugestões para a forma de apresentação das políticas de privacidade e os termos de consentimento em sites, app, serviços do governo digital (ex.: app VIVA PROCON)? Marque quantas opções você quiser.

- ☐ () Textos com linguagem mais simples (com palavras mais conhecidas e familiares)
- ☐ () Textos mais curtos
- ☐ () Textos com menos ou sem expressões jurídicas
- ☐ () Informações com menos conteúdo, mas dividido em uma quantidade maior de janelas
- ☐ () Mais recursos visuais (como gráfico, desenho, ícone, imagem)
- ☐ () Maior destaque ao surgirem na tela
- ☐ () Destaque nas informações mais importantes (usando recursos como negrito, palavras maiores, por exemplo)
- ☐ () Textos sem expressões estrangeiras (em língua inglesa, por exemplo)
- ☐ () Informações em formato de vídeo
- ☐ () Informações em formato de tópicos ou lista

3.1 Qual a sua idade? _____

3.2 Com qual gênero você se identifica? _____

3.3 Qual o seu nível de escolaridade?

- ☐ () Não completei o Ensino Fundamental I
- ☐ () Ensino Fundamental I/Primário completo
- ☐ () Ensino Fundamental II/Ginásio completo
- ☐ () Ensino Médio/2º grau completo
- ☐ () Ensino Técnico completo
- ☐ () Ensino Superior completo
- ☐ () Pós-graduação completo