PODER EXECUTIVO
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Marcos Antônio Soares Maia

Identificando Ameaças à Privacidade em Redes Sociais Online

Manaus
Setembro de 2024

Marcos Antônio Soares Maia

Identificando Ameaças à Privacidade em Redes Sociais Online

Dissertação apresentada ao Programa de Pós- Graduação em Informática de Computação da Universidade Federal do Amazonas do Instituto como requisito parcial para ob- tenção do grau de Mestre em Informática.

ORIENTADOR: PROF. DR. EDUARDO LUZEIRO FEITOSA

COORIENTADOR: PROF. DR. ANDREY ANTÔNIO DE OLIVEIRA RODRIGUES

Manaus
Setembro de 2024

Ficha Catalográfica

Elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

M217i Maia, Marcos Antonio Soares
Identificando Ameaças à Privacidade em Redes Sociais Online / Marcos Antonio Soares Maia. - 2024.
66 f. : il., color. ; 31 cm.

Orientador(a): Eduardo Luzeiro Feitosa.
Coorientador(a): Andrey Antônio Oliveira Rodrigues.
Dissertação (mestrado) - Universidade Federal do Amazonas, Programa de Pós-Graduação em Informática, Manaus, 2024.

1. Risco de privacidade em redes sociais online . 2. Ameaças de privacidade. 3. Ativos de Informação. 4. Segurança em Redes Sociais Online. 5. Exposição de dados. I. Feitosa, Eduardo Luzeiro. II. Rodrigues, Andrey Antônio Oliveira. III. Universidade Federal do Amazonas. Programa de Pós-Graduação em Informática. IV. Título

---

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Programa de Pós-Graduação em Informática

FOLHA DE APROVAÇÃO

"IDENTIFICANDO AMEAÇAS A PRIVACIDADE EM REDES SOCIAIS ONLINE"

MARCOS ANTÔNIO SOARES MAIA

DISSERTAÇÃO DE MESTRADO DEFENDIDA E APROVADA PELA BANCA EXAMINADORA CONSTITUÍDA PELOS PROFESSORES:

Prof. Dr. Eduardo Luzeiro Feitosa - PRESIDENTE

Prof. Dr. Eduardo James Pereira Souto - MEMBRO INTERNO

Prof. Dr. César Augusto Viana Melo - MEMBRO INTERNO

MANAUS, 09 de setembro de 2024.

Documento assinado eletronicamente por **Eduardo Luzeiro Feitosa**, **Professor do Magistério Superior**, em 03/10/2024, às 17:51, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Eduardo James Pereira Souto**, **Professor do Magistério Superior**, em 22/10/2024, às 08:00, conforme

horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **César Augusto Viana Melo**, **Professor do Magistério Superior**, em 22/10/2024, às 13:21, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2224236** e o código CRC **E61EF262**.

Avenida General Rodrigo Octávio, 6200 - Bairro Coroado I Campus Universitário Senador Arthur Virgílio Filho, Setor Norte - Telefone: (92) 3305-1181 / Ramal 1193
CEP 69080-900, Manaus/AM, coordenadorppgi@icomp.ufam.edu.br

Agradecimentos

Primeiramente, agradeço a Deus, pela força, sabedoria e determinação ao longo de toda a jornada acadêmica. Sem Sua orientação e bênçãos, este trabalho não seria possível. Quero expressar minha profunda gratidão ao meu orientador, professor Eduardo Luzeiro Feitosa, por nunca me abandonar durante esta jornada desafiadora e transformadora. Eduardo, sua orientação constante, paciência e dedicação foram pilares fundamentais para a concretização deste trabalho. Eduardo, obrigado por acreditar em mim, por ser um mentor exemplar e por transformar desafios em oportunidades de aprendizado. Este trabalho é tanto meu quanto seu, fruto de uma parceria baseada em confiança, respeito e colaboração.

Agradeço a minha mãe, Sílvia Pereira Maia, pelo amor incondicional, apoio contínuo e incentivo em cada etapa da minha vida. Você é a minha inspiração e motivo de perseverança. Agradeço aos meus irmão João Soares Maia e Mateus Maia Soares por estarem comigo nessa jornada.

Aos membros da banca, pela disponibilidade e pelas contribuições valiosas que enriqueceram este trabalho. Agradeço aos meus amigos de curso, professor Euler, Neto, pela parceria, apoio mútuo e pelas incontáveis discussões e trocas de conhecimento que tornaram este percurso mais leve e enriquecedor. Aos meus amigos que fiz no mestrado em especial Rafael Castilho e Larissa Andrade que me deram muito apoio e incentivo.

Também agradeço a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho. Seu apoio, carinho e incentivo foram essenciais para que eu pudesse alcançar este objetivo. Esta conquista é tanto minha quanto de todos vocês.

Por fim, destaco que o presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, e foi parcialmente financiado pela Fundação de Amparo à Pesquisa do Estado do Amazonas – FAPEAM – por meio do projeto POSGRAD.

Resumo

Com mais da metade da população mundial presente em plataformas de Redes Sociais Online (RSOs), o compartilhamento de informações pode trazer consequências negativas, especialmente quando essas informações atingem um público indesejado. Apesar de existirem medidas como configurações de privacidade e pontuações de risco, essas soluções frequentemente falham em identificar e avaliar ameaças mais abrangentes à privacidade, que não se limitam apenas ao conteúdo postado, mas também à forma como os dados são expostos nas RSOs. Essas ameaças incluem clonagem de perfil, *cyberstalking* e rastreamento de localização, resultando de falhas nos controles de privacidade, que não são detectadas por soluções focadas apenas na visibilidade das postagens. Este estudo propôs a criação de uma árvore de ameaças à privacidade em publicações de RSOs, através da identificação sistemática dessas ameaças e da análise das informações, privadas ou públicas, que podem expor a privacidade dos usuários. Como resultado, a pesquisa identificou e apresentou oito ameaças principais que podem comprometer a privacidade dos usuários, tanto em seus perfis quanto em suas postagens.

Palavras-chave: Risco de privacidade em redes sociais online, Ameaças de privacidade, Ativos de Informação.

Abstract

With more than half of the world's population present on Online Social Networking (OSN) platforms, sharing information can have negative consequences, especially when this information reaches an unintended audience. Despite the existence of measures such as privacy settings and risk assessment, these solutions often fail to identify and assess broader threats to privacy, which are not limited to just the content posted, but also to how data is exposed on OSNs. These threats include profile cloning, cyberstalking, and location tracking, resulting in breaches of privacy controls that are not blocked by solutions focused solely on the visibility of posts. This study proposed the creation of a privacy threat tree in RSOs posts, through the systematic identification of these threats and the analysis of information, private or public, that may expose users' privacy. As a result, the joint research presented eight main threats that may compromise users' privacy, both in their profiles and in their posts.

Keywords: Privacy risk in online social networks, Privacy threats, Threats privacy concerns.

Lista de Figuras

1.1 Metodologia utilizada nesta pesquisa, baseada no ciclo de DSR 5

3.1 Exemplos de postagens em redes sociais com divulgação de ativos de informação 15
3.2 Foto do perfil de um usuário do Twitter 15
3.3 Exemplo de postagens no Twitter de Barack Obama 16

4.1 Em quais redes sociais você tem uma conta ? 22
4.2 Em quais redes sociais você tem uma conta ? 23
4.3 Ameaça à Reputação 24
4.4 Roubo de Identidade 26
4.5 Cyberstalking 27
4.6 Espionagem ou Monitoramento 28
4.7 Gravação não Autorizada 30
4.8 Clonagem de Perfil 31
4.9 Rastreamento e Inferência de Dados 33
4.10 Reconhecimento Facial 34
4.11 Cateterização das Ameaças 36

5.1 Ameaça a Reputação - Especialistas 37
5.2 Análise de dados - Roubo de Identidade 38
5.3 Cyberstalking 39
5.4 Espionagem - Especialistas 40
5.5 Gravação não autorizada 17- Especialistas 41
5.6 Clonagem de Perfil - Especialistas 42
5.7 Rastreamento e Inferência de Dados 43
5.8 Reconhecimento Facial 44
5.9 Categorização dos Ativos de Informação 46

Lista de Tabelas

1 **Termos e String de busca em inglês** 8
2 **Termos e string de busca em português** 8
3 **Artigos selecionados no 2° filtro na IEEE e Scopus** 10

4 **Principais ameaças à privacidade identificadas no trabalho de (Rodrigues, 2022).** 18
5 Interpretação do Coeficiente Alfa de Kappa 21

6 Valores de KAPPA para Ameaças a Reputação 25
7 Valores de KAPPA para Roubo de Identidade 26
8 Valores de KAPPA para Cyberstalking 28
9 Valores de KAPPA para Espionagem ou Monitoramento 29
10 Valores de KAPPA para Gravação não autorizada 30
11 Valores de KAPPA para Clonagem de perfil 32
12 Valores de KAPPA para Rastreamento e Inferência 33
13 Valores de KAPPA para Reconhecimento Facial 34
14 **Kappa Médio de todas as Ameaças** 35

15 Valores de KAPPA para Ameaça a Reputação 38
16 Valores de KAPPA para Cyberstalking 39
17 Valores de KAPPA para Espionagem ou Monitoramento 40
18 Valores de KAPPA para Gravação não Autorizada 41
19 Valores de KAPPA para Clonagem de Perfil 42
20 Valores de KAPPA para Rastreamento e Inferência de Dados 43
21 Valores de KAPPA para Reconhecimento Facial 44
22 **Kappa Médio de todas as Ameaças** 45

Sumário

1.1 Contexto 12
1.2 Problema 13
1.3 Objetivos 14
1.4 Método de Pesquisa 14
1.5 Estrutura do Documento 15
2.1 Mapeamento Sistemático da Literatura 17
2.1.1 Estratégia de Pesquisa 17
2.1.2 Artigos selecionados após a condução do MSL 19
2.2 Trabalhos Relacionados 19
2.3 Discussão 23
3.1 Ativos de Informação e Ameaças à privacidade 24
3.1.1 Ativos de Informação 24
3.1.2 Ameaças à Privacidade 26
3.2 Estudo Exploratório 27
3.2.1 Questionário 28
3.2.2 Participantes 30
3.2.3 Nível de Confiança 30
4.1 Análise das Respostas 33
4.1.1 Ameaça à reputação 34
4.1.2 Roubo de Identidade 35
4.1.3 Cyberstalking 37
4.1.4 Espionagem ou Monitoramento 38
4.1.5 Gravação não Autorizada 39
4.1.6 Clonagem de Perfil 41
4.1.7 Rastreamento e Inferência de Dados 42
4.1.8 Reconhecimento Facial 43
4.2 Discussão dos Resultados 45
5.1 Análise das Respostas 47
5.1.1 Ameaça à reputação 47
5.1.2 Roubo de Identidade 48
5.1.3 Cyberstalking 49
5.1.4 Espionagem ou Monitoramento 50
5.1.5 Gravação não Autorizada 51
5.1.6 Clonagem de Perfil 51
5.1.7 Rastreamento e Inferência de Dados 53
5.1.8 Reconhecimento Facial 53
5.2 Discussão dos Resultados 55
5.3 Considerações Finais 57
6.1 Limitações 58
6.2 Trabalhos Futuros 59
Referências Bibliográficas 61

Capítulo 1

Introdução

1.1 Contexto

As Redes Sociais Online (RSOs) estão cada vez mais presente no cotidiano da sociedade. Um exemplo disso é o número elevado de novos usuários que as utilizam para trabalhar, entretenimento, relacionamentos ou outras finalidades. Dados recentes revelam que mais da metade da população mundial utiliza plataformas de RSOs (Demartini and Ciriaco, 2024). De fato, as RSOs criam um espaço livre para ideias e opiniões, permitindo uma gama de interatividade entre grupos e encurtando a comunicação com outras pessoas, facilitando a conversação com demais usuários.

Tipicamente, em uma RSO, cada usuário tem um perfil que geralmente contém informações pessoais, fotos e atividades recentes. Nelas, os usuários podem estabelecer conexões ou "amizades" com outros usuários, formando uma rede de contatos. Suas atividades, como postagens, atualizações ou compartilhamentos, são exibidas em um *feed* de notícias para que outros possam ver e interagir, seja curtindo, comentando ou e enviando mensagens. Por fim, algumas RSOs também permitem a criação e participação em grupos ou comunidades com interesses específicos.

No entanto, essa interatividade pode trazer sérias consequências quando informações privadas chegam a um público não desejado. Embora muitas vezes não saibam, os usuários são os principais responsáveis pelo vazamento de suas informações pessoais. A exposição de informações pessoais pode levar a problemas de privacidade como fraude, assédio, discriminação e até mesmo violência. A privacidade, no âmbito de RSO, refere-se ao direito dos usuários de manter dados pessoais e atividades protegidas contra acesso, divulgação ou interferência não autorizados (Rodrigues, 2022). Em outras palavras, o usuário deve ter a capacidade de controlar quais detalhes são divulgadas, para quem, quando e sob quais circunstâncias.

É por isso que adotar abordagens que assegurem a segurança e privacidade dos usuários torna-se crucial (Marin, 2020; Lima, 2022). Para ajudar os usuários a compreenderem os potenciais riscos de privacidade relacionados aos seus perfis, postagens e interações com outros participantes, ferramentas, avaliações, métodos e técnicas vem sendo propostas (Petkos et al., 2015; Sramka, 2015; Chen et al., 2018; Al-Asmari and Saleh, 2019b; Smith and Brown, 2022).

Dentre essas soluções, as que avaliam o nível de risco de privacidade através do uso de métricas e cálculos são as mais abundantes (Liu and Terzi, 2010; Domingo-Ferrer, 2010; Gundecha et al., 2011; Nepali and Wang, 2013; Zeng et al., 2014; Laleh et al., 2015; Aghasian et al., 2017; Chen et al., 2018; Han et al., 2019; Alemany et al., 2019). Entretanto, tais soluções não identificam ou

avaliam como ocorrem as ameaças nas RSOs. De acordo com Taylor et al. (2023), entender as ameaças é essencial para capacitar os usuários a tomarem decisões, protegerem sua privacidade e segurança digital, e promoverem práticas responsáveis nas RSOs. Em outras palavras, avaliar as ameaças à privacidade ajuda a conscientizar os usuários sobre o potencial uso indevido de seus dados e a adotar práticas que protejam suas informações pessoais. Assim, a colaboração entre desenvolvedores, especialistas em segurança digital e usuários é crucial para enfrentar esses desafios e promover um ambiente online mais seguro (das Mercês Silva et al., 2021).

Mas identificar ameaças de privacidade em RSOs é uma tarefa complexa e desafiadora. Fatores como a evolução constante das ameaças, questões éticas e legais, dificuldades na integração de dados e limitações tecnológicas contribuem para essa dificuldade, tornando a identificação de ameaças um campo em constante evolução e repleto de obstáculos (Chatti Iorio, 2018; Chakraborty et al., 2022; Taylor et al., 2023).

1.2 Problema

A proteção da privacidade dos usuários em RSOs tornou-se uma questão crítica, especialmente à luz de regulamentos rigorosos como o GDPR na União Europeia e a LGPD no Brasil.

Manter a privacidade dos dados dos usuários é de extrema importância, conforme o *Regulamento Geral de Proteção de Dados* (GDPR) da União Europeia, que em seu Artigo 5(1)(f) estabelece que os dados pessoais devem ser tratados com segurança adequada, prevenindo acessos não autorizados ou ilícitos gdp (2016). De maneira semelhante, a *Lei Geral de Proteção de Dados* (LGPD) do Brasil também define, no Artigo 6, que a segurança dos dados pessoais deve ser garantida por meio de medidas técnicas e administrativas aptas a proteger os dados contra acessos indevidos lgp (2020).

Embora as plataformas de RSOs ofereçam mecanismos de configuração de privacidade para seus usuários, como a opção de controlar a visibilidade de uma postagem, os usuários frequentemente enfrentam riscos de vazamento de privacidade (De and Dey, 2017). Isso porque eles compartilham detalhes excessivos sobre sua rotina, vida familiar, pertences e interesses. Essa falta de conscientização dos usuários, ao publicar informações, leva a experiências negativas de privacidade, resultando, em alguns casos, no abandono da RSO. Por exemplo, usuários com perfis totalmente públicos disponibilizam informações pessoais para qualquer pessoa, incluindo perseguidores (*stalkers*), *spammers* e *hackers*, possa usar essas informações para ganho pessoal (Joyee De and Imine, 2019a). Histórias reais de vazamentos de informações confidenciais ocorrem com frequência.

O problema reside no fato de que existem ameaças à privacidade, como clonagem de perfil, monitoramento de atividades, *cyberstalking* e rastreamento de localização, às quais os usuários se expõem ao divulgar seus dados privados em uma RSO. Por exemplo, é possível inferir com alta precisão a localização do usuário a partir de conteúdos disponibilizados publicamente (Rodrigues, 2022). Enquanto muitas soluções atuais focam na avaliação quantitativa de riscos de privacidade, elas frequentemente negligenciam a identificação e análise das ameaças reais, limitando a eficácia na proteção do usuário

Em geral, as pesquisas relacionadas a privacidade em RSO avaliam os riscos analisando mensagens, amigos em comum e publicações (privadas ou públicas), por meio de métricas e pontuações, seu alcance e sua importância. Entretanto, eles não consideram a ameaça propriamente dita *(cyberstalking, espionagem ou monitoramento)*. Em nossa visão, a análise das ameaças à privacidade em RSOs permite entender como os usuários podem proteger seus dados pessoais (nome, endereço de e-mail, número de telefone, localização, interesses e atividades online, por exemplo) . Assim, como podemos avaliar e compreender efetivamente essas ameaças de

privacidade e as informações expostas em RSOs?

Esta pesquisa propõe uma compreensão das ameaças de privacidade com base nas informações expostas dos usuários em RSOs e os resultados obtidos podem ser usados para desenvolver ferramentas e recursos que ajudem os usuários a proteger sua privacidade e para orientar o desenvolvimento de políticas e práticas de privacidade para RSOs.

1.3 Objetivos

O objetivo desta pesquisa é explorar a relação entre as informações sensíveis divulgadas por usuários e as ameaças à privacidade em Redes Sociais Online (RSOs). Por meio de um estudo exploratório, que envolve a aplicação de formulários de pesquisa, busca-se entender como os usuários percebem os riscos à sua privacidade e identificar quais informações sensíveis podem ser associadas a diferentes tipos de ameaças. A pesquisa também visa desenvolver uma árvore de ameaças para ilustrar essa relação e orientar futuras práticas de mitigação.

Para alcançar esse objetivo geral, os seguintes objetivos específicos foram estabelecidos:

- Identificar e classificar os tipos de informações sensíveis que os usuários expõem em RSOs, categorizando-as como ativos de informação.
- Classificar as ameaças relacionadas às informações divulgadas pelos usuários, categorizando-as de acordo com as ameaças específicas das RSOs.
- Elaborar uma árvore de ameaças que relacione informações sensíveis a ameaças específicas em RSOs, proporcionando uma compreensão clara dos riscos envolvidos.

1.4 Método de Pesquisa

A pesquisa conduzida nesta pesquisa foi caracterizada como exploratória-descritiva e adotou uma abordagem qualitativa e quantitativa. A metodologia tem como fundamentação o ciclo de *Design Science Research* (DSR) (Wieringa, 2014), um paradigma que estabelece as etapas de uma pesquisa para resolver um problema por meio da criação de um artefato, avaliando o que foi projetado e comunicando os resultados obtidos no contexto da pesquisa. A saída do DSR podem ser constructos, modelos, métodos, instanciações e melhores teorias.

A Figura 1.1 representa a metodologia baseada no ciclo de DSR.

- Investigação do Problema - Por meio de uma revisão sistemática da literatura, foram aplicados critérios específicos para identificar tanto soluções generalistas quanto específicas voltadas à detecção de riscos. O mapeamento considerou publicações dos últimos cinco anos em bases de dados como Scopus e IEEE Xplore, com o objetivo de identificar lacunas e oportunidades de melhoria nas abordagens existentes
- Solução Proposta– Após as observações e análises realizadas através do mapeamento sistemático da literatura, foi desenvolvido um estudo para alcançar uma solução para as ameaças abordadas nesta pesquisa. Baseando-se em uma metodologia que integra técnicas de aprendizado de máquina com métodos tradicionais de análise de risco, oferecendo uma melhoria significativa em relação aos trabalhos recentes, especialmente na precisão da detecção precoce de ameaças.
- Estudo de Viabilidade - Um estudo de viabilidade foi conduzido através de um questionário de pesquisa com o objetivo de identificar as ameaças. Esse estudo seguiu para dois estágios, (primeiro estudo e segundo estudo) e resultou na publicação parcial de um artigo.

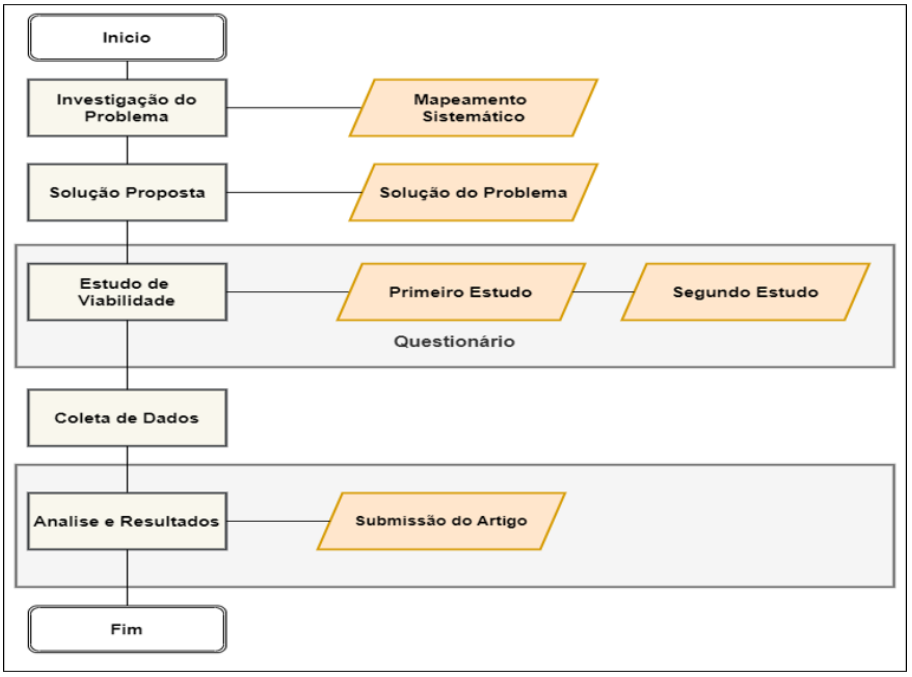

Figura 1.1: Metodologia utilizada nesta pesquisa, baseada no ciclo de DSR.

- Coleta de Dados - Após os resultados do estudo de viabilidade, os dados foram coletados para obter uma melhor precisão na solução e identificação das ameaças.
- Analise e Resultados - A conclusão destacará os estudos realizados, incluindo os pontos positivos e negativos, para ressaltar os resultados obtidos na pesquisa.
- Recomendações - Após a conclusão, serão feitas recomendações e indicados trabalhos futuros visando a melhoria da proposta da pesquisa.

1.5 Estrutura do Documento

Esta dissertação de mestrado é composta por seis capítulos. O Capítulo 1 aborda a Introdução, seguida pela Justificativa e pela Problemática do projeto, bem como pelos Objetivos. Os capítulos subsequentes desenvolvem o conteúdo conforme a estrutura proposta.

- **Capítulo 2** – Mapeamento Sistemático e trabalhos relacionados, cujo propósito foi identificar as ameaças e os métodos de avaliação que aprimoram a privacidade no âmbito das RSOs.
- **Capítulo 3** – Solução Proposta: Esta seção apresenta a solução encontrada para a pesquisa e descreve o passo a passo para alcançar o objetivo.
- **Capítulo 4** – Análise do Questionário: Esta seção abriga as considerações finais, destacando as contribuições significativas do trabalho. Além disso, apresenta perspectivas futuras que podem ser exploradas como continuação ou expansão do escopo deste estudo.

- **Capítulo 5** – Avaliação das ameaças de privacidade nas RSOs: Identificar potenciais riscos que os usuários podem enfrentar ao compartilhar informações pessoais online.
- **Capítulo 6** – Considerações Finais e Trabalhos Futuros: contém as considerações finais, contribuições do trabalho, além de apresentar as perspectivas futuras .

Capítulo 2

MSL e Trabalhos Relacionados

Neste capítulo apresenta a condução e os resultados de um mapeamento sistemático das ameaças de privacidade em redes sociais online (RSO) .

2.1 Mapeamento Sistemático da Literatura

A execução do Mapeamento Sistemático da Literatura (MSL) foi baseado no guia apresentado em (Kitchenham and Charters, 2007), por meio de gênero, de acordo com o paradigma GQM (*Goal-Question-Metric*) (Basili and Rombach, 1988), com o objetivo de **Analisar** as ameaças de privacidade em RSOs, **Com o propósito de** caracterizá-las, **Do ponto de vista dos** pesquisadores e **No contexto de** fontes primárias disponíveis no mecanismo de busca da Scopus e IEEE.

A questão de pesquisa investigada neste mapeamento foi a seguinte: "Como as soluções existentes tratam e mitigam as ameaças à privacidade em RSOs, conforme relatado na literatura científica ?".

2.1.1 Estratégia de Pesquisa

A pesquisa foi realizada empregando as bibliotecas digitais IEEE[1] e Scopus[2], através de seus mecanismos de busca avançada. Os idiomas escolhidos para busca foram o Inglês e o Português, assim como os termos utilizados na pesquisa (palavras-chave). Com a finalidade de melhorar e estruturar a busca na bibliotecas, foi utilizado o PICOC (*Population, Intervention, Comparison, Outcome e Context*) (Keele et al., 2007).

- **Population (P)**: Redes Sociais Online.
- **Intervention (I)**: Tecnologias para projeto e avaliação das ameaças de privacidade em RSOs.
- **Comparison (C)**: Não se aplica, pois, o objetivo não é fazer uma comparação entre tecnologias, mas caracterizá-las.
- **Outcome (O)**: A melhoria de privacidade dos artefatos construídos.

[1]https://ieeexplore.ieee.org/Xplore/home.jsp
[2]http://www.scopus.com/home.url

- **Context (C)**: Redes Sociais Online usadas para comunicação pessoal e compartilhamento de dados. Quais ?

As string de busca em inglês e português são apresentadas nas Tabelas 1 e 2. Os termos estão agrupados em população, intervenção e resultados.

Tabela 1: **Termos e String de busca em inglês.**

String de busca em inglês		
População	(“Privacy risk assessment” AND “social media” or “online social media” or “social media”)	AND
Intervenção	(“tool” OR “graphs” OR “inspection” OR “aspect” OR “heuristics”)	AND
Resultados	(“privacy risk” OR “privacy assessment in online social networks” OR “threats in online social networks” OR “threat assessment in online social networks” OR “privacy methods on social networks”)	

Fonte: Próprio Autor.

Tabela 2: **Termos e string de busca em português.**

String de busca em português		
População	("avaliação dos riscos de privacidade"E ("mídia social"ou "mídia social online"ou "redes sociais")	AND
Intervenção	("ferramenta"OU "gráficos"OU "inspeção"OU "aspecto"OU "heurística")	AND
Resultados	(("risco de privacidade"OU "análise dos riscos de privacidade"OU "avaliação de ameaças em redes sociais online"OU "avaliação de risco"OU "métodos de privacidade em redes sociais")	

Fonte: Próprio Autor.

Cada artigo identificado na MSL foi avaliado segundo os seguintes critérios de inclusão e exclusão:

- **CI1**: Publicações que apresentam tecnologias que projetam e/ou avaliam a privacidade de redes sociais online;
- **CI2**: Publicações onde são apresentadas ferramentas que apoiam tecnologias que projetam e/ou avaliam a privacidade de redes sociais online;
- **CI3**: Publicações onde são descritos estudos experimentais de tecnologias que projetam e/ou avaliam a privacidade de redes sociais online;
- **CI4**: Publicações que discutam aspectos relacionados a tecnologias que projetam e/ou avaliam a privacidade de redes sociais online;
- **CI5**: ações de trabalhos anteriores;

Critérios para exclusão de artigos

- **CE1**: Não serão selecionadas publicações que não atendam aos critérios acima;

- **CE2**: Não serão selecionadas publicações que não tenham disponibilidade de conteúdo para leitura e análise dos dados, eventos pagos, (especialmente em casos, onde os estudos são pagos ou não disponibilizados pela máquina de busca).
- **CE3**: Não serão selecionadas publicações que descrevam e/ou apresentem "keynote speech", anais, tutoriais, cursos, workshops e similares.

No processo de seleção preliminar (1º filtro), o pesquisador avaliou o título e o resumo de cada artigo de acordo com os critérios de inclusão e exclusão.

2.1.2 Artigos selecionados após a condução do MSL

Na biblioteca digital **IEEE**, houve um retorno de 239 artigos utilizando a string de busca. Dos artigos retornados, 65 foram selecionados no primeiro filtro com os seus respectivos critérios de inclusão. Utilizando a biblioteca digital **Scopus**, houve um retorno de 143 artigos utilizando a string de busca e os artigos retornados, 46 foram selecionados no primeiro filtro com os seus respectivos critérios de inclusão. Dos 65 artigos que passaram no 1° filtro da IEEE, 17 passaram no 2° filtro e dos 46 do 1º Filtro da Scopus, 06 artigos passaram para o 2° filtro após a leitura parcial.

Os artigos aceitos estão listados na Tabela 3.

2.2 Trabalhos Relacionados

Esta seção apresenta os trabalhos relacionados identificados na MSL que respondem a questão de pesquisa.

Liu and Terzi (2010) desenvolveram um método para medir e avaliar a privacidade dos usuários em redes sociais. O conceito de "score de privacidade" foi introduzido como uma métrica que reflete o risco associado à exposição de informações pessoais. Apesar das contribuições significativas, o estudo não leva em conta as interações sociais e contextuais complexas que podem afetar a privacidade. Por exemplo, a confiança entre amigos e a sensibilidade de diferentes tipos de informação podem variar amplamente.

Jin et al. (2013) realizaram uma análise do comportamento do usuário que beneficia outros em RSOs. Os autores analisaram diferentes aspectos do uso das redes sociais, incluindo a interação social, a disseminação de informações e a privacidade. A incorporação de mais tipos de dados comportamentais e a melhoria da escalabilidade do modelo para lidar com redes sociais ainda maiores. No entanto O modelo proposto pode ser computacionalmente intensivo, dificultando sua aplicação em larga escala.

Nepali and Wang (2013) desenvolveram um modelo capaz de monitorar a privacidade dos usuários em redes sociais e fornecer um *ranking* de privacidade com base nas configurações e comportamentos dos usuários. No entanto, como qualquer modelo teórico, enfrenta limitações, especialmente no que diz respeito à aplicação prática em redes sociais reais, generalização, complexidade computacional, variedade de dados, complexidade das interações sociais, comportamento dinâmico dos usuários e a subjetividade da privacidade.

Zeng et al. (2014) desenvolveram um modelo de avaliação da privacidade que leva em conta o nível de confiança entre os usuários de uma rede social. A ideia é que a confiança mútua entre os usuários pode influenciar significativamente a exposição e a proteção das informações pessoais. Apesar das contribuições, o modelo não é diretamente aplicável a todas as redes sociais, dado

Tabela 3: **Artigos selecionados no 2° filtro na IEEE e Scopus**

Nº	Autores / Ano	Título da pesquisa	CI
01	Zhang, Z., Ren F., Zhang J. , Sen Su, Yang Yan, Qian Wei, Li Sun , Guozhen Zhu, and Congying Guo (2023)	When Behavior Analysis Meets Social Network Alignment.	CI1
02	Aslihan Banu Cengiz, Guler Kalem, Pinar Sarisaray Boluk, (2022)	The Effect of Social Media User Behaviors on Security and Privacy Threats	CI1
03	Razan Saleh Almogbel, Ali Abddulaziz Alkhalifah, (2022)	User Behavior in Social Networks Toward Privacy and Trust: Literature Review	CI1
04	Dimitrios Amanatidis, Ifigeneia Mylona, Michael Dossis, (2022)	Social Media and Consumer Behaviour: Exploratory Factor Analysis	CI1
05	Daniel Mican, Dan-Andrei Sitar-Tăut, (2022)	User Behavior on Online Social Networks: Relationships among Social Activities and Satisfaction	CI1
06	Puneet Pushkar, Usha Mittal, (2022)	User Behavior Analysis based on their Social-Media Interaction	CI1
07	Shu-Hsien Liao, Retno Widowati, Chieh-Ju Cheng, (2021)	Investigating Taiwan Instagram users' behaviors for social media and social commerce development	CI4
08	Chen, J. He, L. Cai, L. E Pan, J. (2020)	Disclose More and Risk Less: Privacy Preserving Online Social Network Data Sharing.	CI4
09	L Ö. Çoban, A. İnan and S. A. Özel(2020)	Privacy Risk Analysis for Facebook Users.	CI2
10	Jaafar Idrais, Yassine El Moudene, Abderrahim Sabour, (2019)	Characterizing user behavior in Online Social Networks: Study of seasonal changes in the Moroccan community on Facebook	CI1
11	X. Han, H. Huang and L. Wang (2019)	F-PAD: Private Attribute Disclosure Risk Estimation in Online Social NetworksDisclose More and Risk Less: Privacy Preserving Online Social Network Data Sharing.	CI1
12	J. Alemany, E. Del Val, J. M. Alberola and A. Garćia-Forne (2019)	Metrics for Privacy Assessment When Sharing Information in Online SocialNetworks.	CI2
13	H. A. Al-Asmari e M. S. Saleh(2019)	A Conceptual Framework for Measuring Personal Privacy Risks in Facebook Online Social Network.	CI1
14	Aghasian E., Garg S., Gao L., Yu And J S. (2017)	Montgomery Scoring Users' Privacy Disclosure Across Multiple Online Social Networks.	CI1
15	G. Petkos, S. Papadopoulos and Y. Kompatsiaris (2015)	PScore: A Framework for Enhancing Privacy Awareness in Online Social Networks.	CI1
16	Sramka M. (2015)	Evaluating Privacy Risks In Social Networks From The User's Perspective.	CI1
17	Laleh N., Carminati B. E Ferrari E., (2015)	Graph Based Local Risk Estimation in Large Scale Online Social Networks.	CI4
18	Zeng Y., Sun Y., Xing L. E Vokkarane V. (2014)	Trust-aware privacy Evaluation in online social networks.	CI2
19	Nepali, R. K And Wang, Y. (2013)	SONET A Social Network Model for Privacy Monitoring and Ranking	CI1
20	Long Jin, Yang Chen, Tianyi Wang, Pan Hu, (2013)	Understanding User Behavior in Online Social Networks: A Survey	CI1
21	Gundecha P.; Barbier G., E Liu H., (2011).	Exploiting Vulnerability to Secure User Privacy on Social Networking Site.	CI1
22	Domingo-Ferrer, J. (2010)	Rational privacy disclosure in social networks. Modeling decisions for artificial intelligence.	CI3
23	K. Liu and E. Terzi,(2009)	A Framework for Enhancing Privacy Awareness in Online Social Networks.	CI1

Fonte: Próprio Autor.

que diferentes plataformas possuem diferentes dinâmicas de confiança e políticas de privacidade. Além disso, o modelo não leva em conta todos os fatores que afetam a privacidade, como a divulgação involuntária de informações por amigos ou a exploração de dados por terceiros. Laleh et al. (2015) desenvolveram uma métrica de risco chamada "fator de risco local", com base na observação de que usuários mal-intencionados em RSOs, e um método para estimar os riscos de privacidade em redes sociais de grande escala, utilizando uma abordagem baseada em grafos. O foco do trabalho foi a identificação de riscos locais que um usuário específico pode enfrentar ao compartilhar informações em sua rede social. Embora o artigo apresente avanços na estimativa de riscos de privacidade em redes sociais, a interpretação dos riscos identificados é complexa e exigi conhecimento especializado.

Petkos et al. (2015) desenvolveram um *framework* chamado **PScore**, afim de aumentar a conscientização dos usuários sobre questões de privacidade em RSOs. O *framework* assume que os usuários responderão positivamente as suas sugestões e ajustarão suas configurações de privacidade. No entanto, isso nem sempre é ou será verdade, limitando a atuação da solução. O trabalho de Aghasian et al. (2017) abordou usuários de RSO que postam suas informações confidenciais e expõem sua situação social e financeira. A metologia proposta visou ajudar os usuários a entender melhor os riscos de privacidade associados ao compartilhamento de informações em múltiplas redes. Contudo, o trabalho não considerou a diversidade de dados entre diferentes redes sociais pode tornar desafiador criar uma pontuação uniforme e comparável. Usuários de sites de redes sociais online, sem saber, divulgam suas informações confidenciais que agravam a situação social e riscos financeiros. Para evitar a perda de informações e a exposição da privacidade, os usuários precisam encontrar maneiras de quantificar seu nível de privacidade com base em seus dados de rede social online. Não há explícito o critério para medir a dificuldade de extração de dados, que é, portanto, um problema aberto para investigação dos riscos de privacidade.

Chen et al. (2018) criaram uma métrica de privacidade que investiga o compartilhamento de dados da RSO, detectando quais os riscos ao publicar uma mensagem. A pesquisa indicou que quanto mais informações no seu perfil de um usuário (endereço, e-mail, contato e telefone pessoal), maiores serão as chances de uma futura invasão. Com isso, os autores afirmam que mais 59% dos usuários não têm controle da sua privacidade e o restante representavam usuários que não divulgavam tantos conteúdos na rede.

Na pesquisa de Han et al. (2019), os autores afirmaram que ao mensurar medidas de riscos é possível detectar atividades sociais online das pessoas. Os resultados revelaram grupos com mais riscos de violações em sua RSO, estimado em 61%, pois ao divulgar em larga escala, o risco de visualização de seu perfil se torna maior, podendo ocasionar perseguições de *cyberstalking*.

Al-Asmari and Saleh (2019b) propuseram um *framework* conceitual para medir os riscos de privacidade pessoal no Facebook. O *framework* permite a avaliação sistemática dos riscos de privacidade enfrentados pelos usuários do Facebook, considerando diferentes tipos de informações pessoais que podem ser compartilhadas na plataforma. Por ser um *framework* conceitual, faltam dados detalhados ou experimentos práticos para validar a eficácia e a aplicabilidade do modelo na prática.

Alemany et al. (2019) focaram em criar um conjunto de medidas que permitisse aos usuários e pesquisadores entenderem melhor os riscos associados à divulgação de informações pessoais nessas plataformas. As métricas desenvolvidas são aplicáveis a um conjunto específico de plataformas de redes sociais ou contextos de compartilhamento de informações. Sua generalização para diferentes plataformas e cenários pode ser limitada. Também a interpretação das métricas pode ser subjetiva e variar entre diferentes grupos de usuários e culturas, exigindo uma abordagem flexível na aplicação das medidas.

O estudo de Çoban et al. (2020) avaliou o comportamento dos usuários e o risco de privaci-

dade para usuários do Facebook, enfatizando a importância da conscientização sobre o que é compartilhado em redes sociais online. Os pesquisadores coletaram dados de 1.200 usuários e revelaram que quanto maior o número de visualizações em informações como postagens normais ou localizações, maior é o risco de privacidade associado. Cerca de 67% dos usuários avaliados compartilharam informações pessoais, aumentando assim o risco de violação de sua privacidade nas redes sociais.

A pesquisa de Mican et al. (2020) analisou o comportamento dos usuários em RSOs e validou a hipótese de que as atividades nessas plataformas estão diretamente ligadas ao nível de satisfação do usuário. Descobriram que quanto mais os usuários publicam e comentam, maior é seu nível de satisfação, mas também observaram que à medida que os usuários atribuem maior importância às redes sociais, sua satisfação tende a diminuir. Este estudo contribui significativamente para a compreensão das correlações entre atividades nas redes sociais, adicionando novos dados à literatura existente.

Pushkar and Mittal (2022) revisaram várias técnicas para analisar o comportamento do usuário nas interações das RSOs e apontaram limitações, como a escassez de estudos abrangentes sobre a avaliação do comportamento do usuário nessas redes. Os pesquisadores também observaram que os resultados não representam precisamente todas as situações e suas consequências, uma vez que os dados detalhados sobre as classificações de redes sociais em relação aos riscos nem sempre estão disponíveis ao público. Portanto, existem desafios em obter uma imagem completa e precisa dessas dinâmicas de comportamento do usuário.

O trabalho de Amanatidis et al. (2022) concentrou-se na avaliação dos riscos de privacidade, análise do comportamento do usuário e na realização de redução de dimensionalidade. O principal objetivo do estudo foi investigar a relação entre privacidade, confiança e como esses fatores impactam o comportamento dos usuários nas redes sociais. Ele proporciona uma visão detalhada e abrangente dos conceitos e métodos relacionados à proteção da privacidade e ao fortalecimento da confiança dos usuários em redes sociais comportamentais.

O estudo de Almogbel and Alkhalifah (2022) analisou e sintetizou as pesquisas existentes sobre como os usuários se comportam em relação à privacidade e confiança nas redes sociais online. Os autores incluíram a investigação de fatores que influenciam as decisões dos usuários ao compartilhar informações pessoais e ao interagir com outros usuários nas plataformas de mídia social. Diferentes tipos de comportamento foram discutidos, incluindo estratégias de gestão de privacidade, compartilhamento seletivo de informações e níveis de confiança em diferentes tipos de conexões sociais (amigos, familiares, estranhos). Os resultados dos estudos individuais podem variar significativamente dependendo das amostras, metodologias e contextos estudados, limitando a generalização para diferentes grupos demográficos ou culturais.

O estudo de Cengiz et al. (2022) ofereceu uma análise importante sobre como os comportamentos dos usuários de mídias sociais impactam as ameaças à segurança e privacidade. Apesar de suas limitações, incluindo amostra limitada, dados autodeclarados, foco em plataformas específicas, rápida evolução das redes sociais e complexidade dos riscos, o estudo fornece informações para melhorar a segurança e proteger a privacidade dos usuários online. Este estudo foi desenvolvido para investigar o efeito dos comportamentos dos usuários de mídia social em seu nível de vulnerabilidade em termos de segurança e privacidade. O estudo foi conduzido por métodos de pesquisa, que foram aplicados a usuários de mídia social em dois países - Turquia e Iraque.

2.3 Discussão

Dentre os estudos apresentados neste capítulo, fica claro que os usuários frequentemente desempenham o papel de facilitadores no vazamento de informações. Desta forma, grande parte dos trabalhos consideram o risco de privacidade como uma função que envolve elementos do perfil e postagens dos usuários, o que inclui informações como nome real, e-mail, cidade natal, número de telefone, status de relacionamento, orientação sexual, nome de perfil, entre outros. A contribuição de cada um desses itens para a avaliação total do risco depende de sua sensibilidade e da visibilidade permitida pelas configurações de privacidade do usuário.

Por outro lado, os trabalhos não exploraram às ameaças, uma vez que as análise se concentra exclusivamente nas informações. Nada é dito sobre as ameaças e quais informações estão relacionados a elas. É com base nessas análises que identificamos a oportunidade de desenvolver um novo modelo de avaliação de riscos de privacidade em RSOs voltadas para as ameaças.

Capítulo 3

Solução Proposta

Este capítulo apresenta o estudo exploratório proposto com usuários de RSOs e baseado na aplicação de um questionário. De acordo com Malhotra et al. (2020), um questionário se configura como um método de coleta de dados de uma amostra populacional, com o propósito de investigar determinado assunto. O foco foi identificar a relação entre ativos de informação e ameaças à privacidade, tanto em postagens quanto perfil de usuários em RSO, visando estabelecer formalmente, de acordo com o conhecimento dos participantes, quais ativos estão relacionados com qual ameaça.

Para tanto, primeiramente, abordamos os conceitos de ativo de informação e ameaça de privacidade e, posteriormente, explicamos o estudo exploratório.

3.1 Ativos de Informação e Ameaças à privacidade

De acordo com a ISO 27002 (ABNT, 2013), um **ativo de informação** é qualquer informação que seja valiosa para uma organização. Essa informação pode ser tangível ou intangível, e pode estar em qualquer formato, incluindo documentos, dados, sistemas, software, processos e pessoas. Já uma **ameaça de privacidade** é entendida como um evento indesejável potencial ou real que pode causar danos ao usuário na forma de divulgação, exposição e uso indevido de dados privados (Laorden et al., 2010; Rathore et al., 2017b; Joyee De and Imine, 2019b).

3.1.1 Ativos de Informação

Em uma RSO, um ativo de informação pode ser definido como uma informação relacionado ao usuário, que possui um valor pessoal. Nesta pesquisa, um ativo representa uma informação ou atributo pessoal do usuário que possua valor e tenha implicações em suà privacidade, e por isso deva ser protegido contra possíveis ameaças. Exemplos de ativos incluem número de identificação (RG), número de cadastro de pessoa física (CPF), nome, fotos, vídeos, localização, entre outros.

Para facilitar a identificação dos ativos em RSO, Rodrigues (2022) categorizou os ativos de acordo com a forma como aparecem em: (1) **Dados textuais**, seja no formato de arquivos ou texto livre; (2) **Dados multimídia**, como fotos, áudios ou vídeos; e (3) **Dados geográficos**, geralmente referentes à geolocalização.

Com o objetivo de melhorar a compreensão sobre os ativos de informação, a Figura 3.1 ilustra alguns tipos de ativos disponibilizados (intencionalmente ou não) em RSOs. Um ponto

importante a ser destacado é que existem ativos que não são diretamente compartilhados pelos usuários, mas são coletados ou gerados pela própria plataforma.

Figura 3.1: Exemplos de postagens em redes sociais com divulgação de ativos de informação. Na imagem (a), exposição por terceiros do endereço (rua e bairro) e do número de identificação (RG) do usuário. Na imagem (b), exposição por terceiros do nome, CPF, CNPJ e foto do usuário. Por fim, na imagem (c) dados sobre o perfil de um usuário.

É importante destacar que nesta pesquisa, entendemos que os ativos de informação podem ser coletados tanto do perfil do usuário quanto de suas postagens. A Figura 3.2 ilustra os ativos do perfil de um usuário no Twitter (agora X).

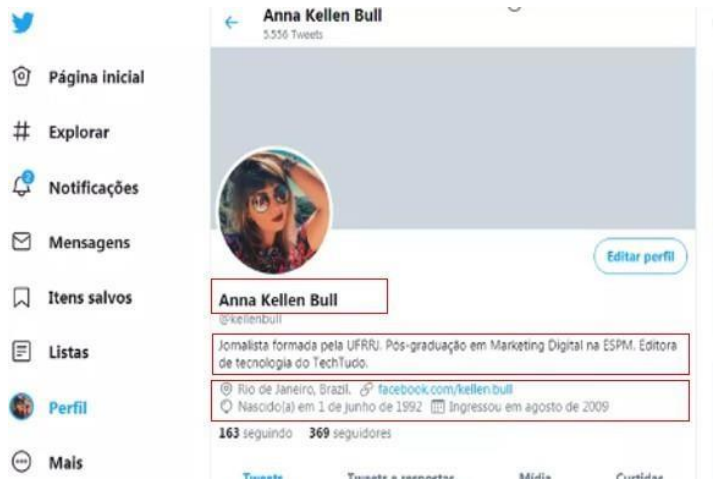

Figura 3.2: Foto do perfil de um usuário do Twitter.

Nota-se, na Figura 3.2, a presença de cinco (5) ativos de informação: **nome** (Anna Kellen Bull), **biografia curta**, **cidade** onde mora, **data de nascimento** e **data de ingresso** na RSO.

Já a Figura 3.3 ilustra três (3) postagens feitas pelo ex-presidente dos Estados Unidos da América, Barack Obama, em sua conta no Twitter. A primeira, e mais central, representa uma

foto (imagem) dele com sua esposa. A segunda é a imagem de uma postagem textual. A terceira também é uma postagem textual acompanhada de um vídeo.

Figura 3.3: Exemplo de postagens no Twitter de Barack Obama.

Os ativos identificados na Figura 3.3 são: (1) uma **imagem**, que pode ser afetada por ameaças de rastreamento e inferência de informações, clonagem de perfil e espionagem ou monitoramento; (2) um **texto** de uma postagem parabenizando um time de futebol americano, que pode ser tirado de contexto e empregado em uma ameaça à reputação e (3) uma postagem com **texto** e **vídeo**, pode sofrer riscos como *cyberstalking* e espionagem ou monitoramento.

3.1.2 Ameaças à Privacidade

Embora o conceito de ativos de informação seja relativamente simples e de fácil percepção, o conceito de ameaças à privacidade é mais complexo. Recentemente, Rodrigues (2022) conduziu uma MSL a fim de identificar as ameaças à privacidade as quais os usuários de RSO estão expostos. Ele identificou mais de 30 ameaças à privacidade descritas na literatura. Ao analisá-las, observou que várias eram de natureza igual ou semelhante, apresentando nomenclaturas diferentes, mas com significados similares. Além disso, outras estavam relacionadas à segurança de sistemas e não estavam diretamente vinculadas à privacidade dos dados do usuário. Como resultado, Rodrigues (2022) categorizou um conjunto de ameaças da seguinte forma:

- **Cyberstalking** - Uso da RSO para assediar ou perseguir um indivíduo, ou um grupo de indivíduos, com comportamento indesejado ou ameaçador, imposto repetidamente.
- **Divulgação de Informação** - Refere-se à descoberta e divulgação não autorizada de informações privadas. O compartilhamento dessas informações pode causar implicações negativas para a vida do usuário, como emprego dos seus dados para fins diversos, como campanhas políticas, marketing e anúncios indesejados.

- **Clonagem de perfil** - Um agente malicioso pode utilizar os dados compartilhados por um determinado usuário e clonar o seu perfil, sem que a RSO ou a própria vítima percebam a clonagem. Com isso, o agente malicioso cria uma identidade falsa para fazer os amigos da vítima acreditarem no novo perfil (falso). Com esse perfil criado, o agente malicioso poderá entrar em contato com a lista de amigos da vítima e enviar links para capturar dados privados.
- **Inferência ou rastreamento** - É a coleta e combinação de dados para gerar ou descobrir informações pessoais do usuário que não estão diretamente compartilhadas em seus perfis nas RSOs, mas podem ser inferidas usando diferentes técnicas computacionais. Tal atividade é realizada por provedores de RSO, que rastreiam e analisam as atividades online do usuário (como navegação diária e preferências de compras, por exemplo) por meio de diversas técnicas de aprendizagem de máquina. Como resultado, as RSOs constroem perfis completos do usuário com o objetivo de vender produtos ou rastrear o seu comportamento.
- **Ameaça à reputação** - Um agente malicioso ou uma entidade maliciosa pode obter acesso a informações pessoais e explorá-las para prejudicar à privacidade do usuário. Assim, os usuários podem se tornar vítimas de manipulação e distorção de dados. Vale destacar que existem diversas ferramentas disponíveis para manipular e distorcer diversos dados.
- **Reconhecimento facial** Identificar o rosto de alguém em uma foto ou vídeo e cruzar referências com outros dados pode ser usado para expor informações pessoais do usuário. Algoritmos, quando combinados com outras tecnologias, possibilitam encontrar usuários com uma boa precisão, sem o consentimento destes. Segundo o jornal *New York Times*, a empresa Clearview AI criou um banco de dados com mais de três bilhões de imagens de usuários das redes sociais online, como Facebook e YouTube.
- **Espionagem** - É um tipo de monitoramento que permite, em tempo real, a coleta e o processamento de diversas atividades do usuário de RSOs, principalmente atividades de perfil e relacionamentos com outros indivíduos.
- **Gravação não autorizada** - Muitas RSOs fornecem serviços de *chat* e videochamadas, proporcionando mais interação entre seus usuários. No entanto, informações pessoais podem ser divulgadas ou coletadas, uma vez que qualquer participante pode facilmente realizar uma gravação não autorizada para posteriormente chantagear o outro participante (vítima). Além disso, um participante pode distorcer os dados da chamada e exibi-los inadequadamente.
- **Roubo de identidade** - É um tipo de ameaça em que um agente malicioso obtém acesso ilegal a conta do usuário da RSO para capturar dados privados. Diferentes técnicas podem ser aplicadas por um atacante para realizar um roubo de identidade. Por exemplo, um atacante pode enviar links para obter informações confidenciais, como senhas e códigos de autenticação. De posse desses dados, poderá obter acesso a conta do usuário na RSO e todo seu registro de atividades e dados pessoais.

A Tabela 4 enumera as ameaças elencadas por (Rodrigues, 2022).

3.2 Estudo Exploratório

Uma vez definidas as ameaças à privacidade, notamos que era preciso identificar os ativos de informação da RSOs. Analisando os trabalhos da literatura, incluindo Rodrigues (2022), não foi

Tabela 4: **Principais ameaças à privacidade identificadas no trabalho de (Rodrigues, 2022).**

Ameaças	Sinônimos	Referências
Cyberstalking	*Stalking* e *digital stalking*	(Sramka, 2012), (Fogues et al., 2015), (Aktypi et al., 2017), (De and Imine, 2018b)
Divulgação de informação	Disseminação, divulgação de conteúdo, divulgação de identidade e uso indevido de dados	(Casas et al., 2015), (Zeng et al., 2015), (Aktypi et al., 2017), (Rathore et al., 2017a), (Bioglio et al., 2019)
Clonagem de perfil	Perfil falso e Perfil clonado	(Mahmood, 2012), (Jaafor and Birregah, 2015), (Aktypi et al., 2017), (Rathore et al., 2017a), (Abid et al., 2018)
Inferência ou Rastreamento	Extração de informações, rastreamento de atividades, mineração de dados e criação de perfil	(Laorden et al., 2010), (Watanabe et al., 2011), (Wang and Nepali, 2015), (Dong and Zhou, 2016), (Abid et al., 2018)
Ameaça à reputação	Discriminação, constrangimento, ataques Sybil e manipulação de dados	(Aktypi et al., 2017), (Rathore et al., 2017a)
Reconhecimento facial	Recuperação de imagens e marcação de fotos	(Laorden et al., 2010), (Kavianpour et al., 2011), (Kumar et al., 2017)
Espionagem	Espionagem corporativa e monitoramento	(Aktypi et al., 2017)
Gravação não autorizada	Risco de videochamadas e videochamadas em grupo	(Rathore et al., 2017a)
Roubo de identidade	Phishing, invasão de conta e descoberta de atributos ocultos	(Tucker et al., 2015), (De and Imine, 2018a),(De and Imine, 2018b), (Al-Asmari and Saleh, 2019a)

possível identificar qualquer tipo de relação entre os ativos e as ameaças. Em outras palavras, a exposição de quais ativos pode caracterizar uma determinada ameaça. Assim, decidiu-se elaborar um formulário de pesquisa.

O **objetivo** foi de identificar os ativos de informação de um RSO que podem comprometer à privacidade dos usuários ao estarem relacionados com uma determinada ameaça. Para tanto, os **participantes**, usuários de RSO, responderam, sob sua perspectiva após acesso a material introdutório sobre o assunto, quais os ativos de informação podem estar relacionados a determinadas ameaças de privacidade, por meio da exposição de suas informações de perfil ou postagens.

Optamos por realizar uma pesquisa de opinião porque, de acordo com Malhotra et al. (2020), tais pesquisas proporcionam a identificação de aspectos relevantes. Neste trabalho, a pesquisa de opinião se configura como um método de coleta de dados de uma amostra populacional, com o propósito de investigar o conhecimento de ameaças em RSO.

3.2.1 Questionário

O questionário aplicado neste estudo foi elaborado em língua portuguesa e montado para ser respondido de forma simples e direta, utilizando a plataforma Google Formulários. O período de coleta de dados ocorreu de 05 de outubro a 05 de novembro de 2023. A estrutura do questionário foi dividida em duas etapas distintas. A primeira concentrou-se na caracterização dos participantes, perguntando sobre sua formação (área de TI ou não), idade, RSOs que possui e frequência de acesso.

A segunda parte abordou, de forma direta, as oito perguntas relacionadas as ameaças à privacidade. O formato das perguntas foi sempre o mesmo:

Exemplo:

- **Quais dos ativos listados abaixo você considera que podem ser comprometidos em uma ameaça à reputação ?**.
- Nome (Nome completo, Nome e sobrenome, nome abreviado)
- Apelido
- Identificação (RG, CPF, certificado militar, carteira funcional, entre outros)
- Data de Nascimento
- Idade
- Sexo
- Endereço atual (textual)
- Endereço(s) anteriore(s) (textual)
- Telefone(s) (Celular/Fixo)
- E-mail(s)
- Imagem do perfil
- Foto(s)
- Vídeo(s)
- Áudio(s)
- Biografia
- Escolaridade (Fundamental, médio, superior)
- Ano de Formação (Fundamental, Médio, superior)
- Religião
- Emprego atual
- Endereço do emprego (textual)
- Emprego(s) anterior(es)
- Cargo
- Localização (Onde está no momento, onde visitou) - (não textual)
- Status de relacionamento
- Dados de familiares
- Dados de amigos
- Informações sobre hobbies (Esportes, leitura, culinária, passeios, viagens, jogos, música, trabalho voluntário, dança, entre outros)
- Condição de saúde (Tratamentos, doenças, idas a hospitais, entre outros)

Assim, para cada ameaça, os participantes precisavam marcar os ativos que acreditavam estar relacionados com aquela ameaça.

Como forma de auxiliar os participantes, antes do preenchimento do questionários, todos precisavam visualizar um material sobre ameaças e sobre ativos de informação. Vale destacar que é o mesmo material encontrado no trabalho de (Rodrigues, 2022)[1].

3.2.2 Participantes

Este estudo exploratório foi aplicado em dois tipos de participantes. O primeiro, denominado **público em geral**, usuários de RSO, ligados ou não a área de computação. O público em geral representa uma ampla variedade de perspectivas, experiências e opiniões. Os participantes do público em geral foram convidados através de e-mail e grupos de Whatsapp. No total, obtivemos 273 respostas.

O segundo grupo de participantes foi formado especialistas na área de segurança da informação, indivíduos com conhecimento técnico e experiência específica na área de estudo em questão. Isso permite uma análise mais Eles foram convidados através de e-mail, grupos de WhatsApp e Linkedln. No total, obtivemos o aceite de 17 especialistas.

A escolha por esse dois públicos de participantes se justifica da seguinte forma:

- **Validação e Confiança:** A avaliação por especialistas garante a validade e confiabilidade dos dados, tendo em vista que possuem conhecimento aprofundado, o que permite identificar falhas, erros ou lacunas na pesquisa. Já a avaliação do público geral proporciona uma perspectiva mais ampla e diversificada de percepções.

- **Aprimoramento**: A avaliação por especialistas e do público em geral pode fornecer *feedback* valioso sobre a o processo de coleta dos dados.

- **Legitimidade e Aceitação**: A inclusão de diversas perspectivas aumenta a legitimidade dos dados e promove a aceitação das conclusões por parte da comunidade científica, das partes interessadas e do público em geral.

3.2.3 Nível de Confiança

O cálculo do nível de confiança é fundamental em pesquisa porque fornece uma medida da incerteza associada aos resultados obtidos a partir de uma amostra da população. Neste trabalho empregamos o Alfa de Kappa para avaliar o nível de confiança.

3.2.3.1 Kappa de Fleiss

O valor de Kappa de Fleiss é uma medida estatística utilizada para avaliar a concordância ou acordo entre dois ou mais avaliadores quando eles classificam ou categorizam itens de interesse. Ele é amplamente utilizado em várias áreas, incluindo pesquisa médica, ciências sociais, psicologia, epidemiologia, entre outras.

O valor do coeficiente de Kappa de Fleiss varia de -1 a 1, onde: (i) im valor próximo de 1 indica uma concordância quase perfeita entre os avaliadores; (ii) um valor próximo de 0 indica concordância apenas ao acaso; e (iii) um valor negativo indica concordância menos do que a esperada ao acaso, o que significa que os avaliadores discordam mais do que concordam.

[1]https://drive.google.com/drive/folders/1SyoSAqPBOnrmZLvo1pf5GQj5q9NztwgYoy 1qtrCMIRfGrV-Deo8cOsteVHTrt5XEhbSyqEkHt

O cálculo do Kappa de Fleiss envolve a construção de uma tabela de contagem que mostra quantas vezes cada avaliador categorizou os itens em cada categoria. A fórmula leva em conta tanto a proporção observada quanto a proporção esperada de concordância.

A fórmula geral para o cálculo do coeficiente de Kappa de Fleiss é dada por:

$$\kappa = \frac{P_o - {}_eP}{1 - P_e} \tag{3.1}$$

Onde:

- Po é a proporção observada de concordância entre os revisores.
- Pe é a proporção esperada de concordância ao acaso, calculada com base nas proporções marginais de concordância para cada categoria.

Tabela 5: Interpretação do Coeficiente Alfa de Kappa

Alfa de Kappa	**Interpretação**
< 0,00	Concordância nenhuma
Menor que 0,20	Concordância baixa
0,21 - 0,40	Concordância mínima
0,41 - 0,60	Concordância fraca
0,61 - 0,80	Concordância forte
Maior que 0,80	Concordância quase perfeita

Capítulo 4

Primeiro Estudo

Para validar o questionário, decidimos aplicá-lo com o público em geral, usuários de RSO, ligados ou não a área de computação. Os participantes foram convidados através de e-mail e grupos de Whatsapp. No total, obtivemos 273 respostas.

O processo de resposta ao questionário foi o seguinte. Após aceitarem contribuir com o estudo, os participantes assinaram um Termo de Consentimento Livre e Esclarecido (TCLE), disponível em **Relacionando Ameaças de Privacidade e Informações Expostas em Redes Sociais Online** . Após o TCLE, receberam acesso ao dois catálogos de informação. Um sobre ameaças à privacidade em RSO - o mesmo aplicado no trabalho de (Rodrigues, 2022) - e outro sobre ativos de informação em RSO. Ambos os catálogos, que estão disponíveis tanto no formulário de pesquisa quanto via Drive do Google, desempenharam o papel de identificar e categorizar as ameaças à privacidade em RSOs, permitindo esclarecer quais dúvidas ou dificuldades que os participantes tivessem na identificação dos ativos de informação relacionados a determinada ameaça. Vale destacar que os participarem eram convidados a acessar o conteúdo dos catálogos, não obrigados.

Em seguida, respondiam as oito (8) perguntas do formulário sobre as ameaças, marcando os itens que julgavam mais prováveis de ocorrer para cada uma das ameaças.

Figura 4.1: Em quais redes sociais você tem uma conta ?

Antes de apresentar as respostas, é preciso caracterizar os participantes. Começando pela idade, segmentamos os participantes em grupos específicos 4.1. O grupo 01 foi formado por usuários com idades entre 16 e 20 anos, totalizando 98 participantes (35,9% do total). O grupo 02 foi formado por usuários com idades entre 21 e 28 anos, totalizando 86 pessoas e compreendendo 31,5% dos participantes. O grupo 03 foi composto por 45 participantes entre 29 e 35 anos, representando 16,5% do total. O grupo 04 foi composto por 29 participantes entre

36 e 45 anos, representando 10,6% do total. Por fim, o grupo 05, constituído de participantes com mais de 46 anos, possuiu 15 pessoas, o que representa 5,5% dos participantes.

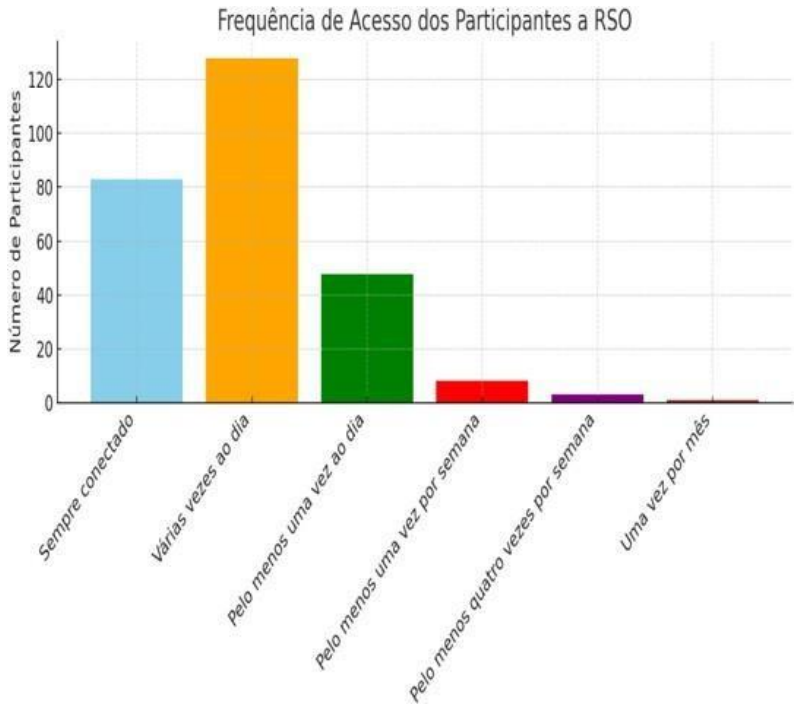

Figura 4.2: Em quais redes sociais você tem uma conta ?

Também perguntamos aos participantes a frequência com que acessam as RSOs 4.2. 83 usuários (30,6%) responderam que ficam conectados em uma ou mais RSOs. Desses participantes, 48 são do grupo 01 e 16 do grupo 02. Já os participantes que responderam que acessam várias vezes ao dia, 128 respondentes, todos do grupo 03 se enquadraram nesse tipo de acesso.

A pesquisa também perguntou quais RSOs os participantes possuem. O Instagram ficou em 1 lugar, com 237 dos participantes. Em seguida veio o YouTube, com 211 participantes. O Facebook possui 198 participantes do estudo, enquanto o Tiktok tem 129 participantes. Por fim, Linkedin e X empataram com 99 participantes cada.

A pesquisa mostrou que os participantes entre 16 e com mais de 46 anos possuem uma média de 04 RSO. O grupo entre 16 a 20 anos possui o maior número de contas no Instagram, YouTube e Facebook, seguido pelo grupo de 21 a 28 anos, com uma média de 78 respondentes. Um ponto interessante é que o grupo 02 apresentou mais participantes na rede social LinkedIn, seguido pelo grupo de 29 a 35 anos (grupo 03), com uma média de 26 participantes.

4.1 Análise das Respostas

Nesta seção, analisamos as respostas dos participantes em relação a oito ameaças a privacidade.

4.1.1 Ameaça à reputação

A ameaça à reputação é definida como exposição de informações privadas por um usuário malicioso. Essa conduta inclui divulgação indevida da intimidade do usuário, distorção de dados pessoais, discriminação injustificada, extorsão e chantagem, afetando negativamente a imagem e a privacidade do indivíduo.

A Figura 4.3 apresenta as respostas dos participantes.

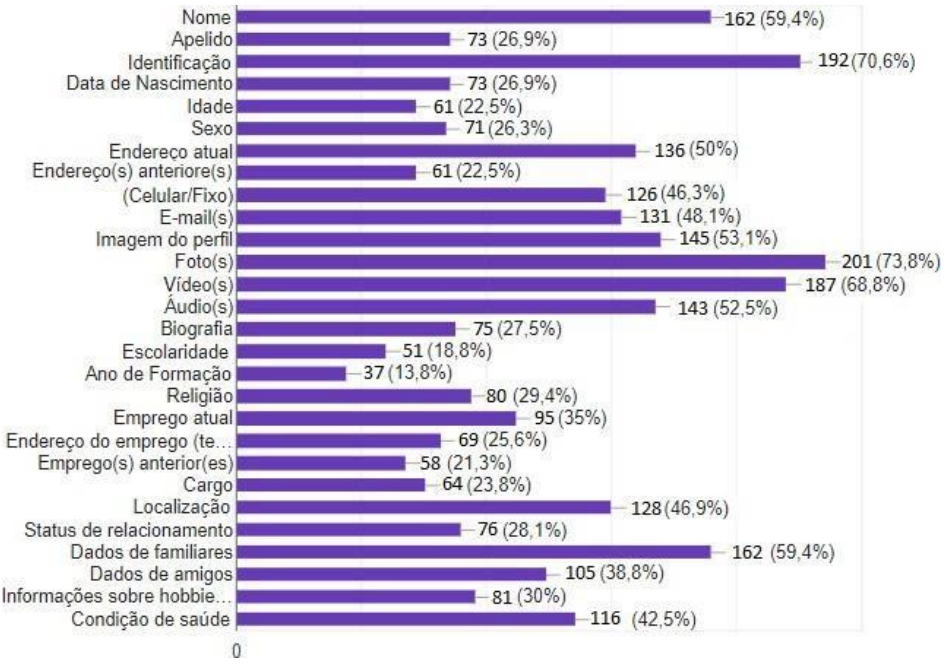

Figura 4.3: Ameaça à Reputação.

De acordo com os participantes, os ativos que consideraram com maior potencial de ameaça a reputação são (1) a **foto de perfil** do usuário da RSO, com 201 respostas (73,8%) dos respondentes), e a **identificação**, com 192 participantes 70,6%). Vale destacar que 49 do 273 participantes escolheram somente esses ativos. Os outros ativos mais relacionados são: **vídeos** (68,6%), **dados familiares** (59,1%), **nome** (59,1%), **imagem do perfil** (52,8%), **áudio** (52,8%), **endereço atual** (50,3%), **E-mail** (47,8%) e **localização** (47,2%). Desses ativos, apenas 47 participantes os escolheram todos eles unicamente.

Ao se analisar as respostas do **grupo 01**, composto pelos participantes mais jovens, identificamos um número de ativos relacionados a essa ameaça variando entre 12 a 16. Já para o **grupo 02**, o número de ativos relacionados a essa ameaça variou entre 9 a 13. Para os grupos 03, 04 e 05, foram relacionados entre 03 a 09 ativos, de acordo com cada participante.

Para validar as respostas para esta ameaça, empregamos o coeficiente de Kappa para medir a confiabilidade do que foi respondido. O resultado dos ativos para o Kappa de Fleiss, para todas as respostas, foi de 0,382, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 6 apresenta a análise do Kappa para cada um dos itens em avaliação.

Os valores de Kappa para cada item, conforme a Tabela 6, mostram uma concordância maior

Tabela 6: Valores de KAPPA para Ameaças a Reputação

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,593	2	Apelido	0,267
3	Identificação	0,703	4	Data de Nascimento	0,267
5	Idade	0,223	6	Sexo	0,260
7	Endereço Atual	0,498	8	Endereço(s) Anteriore(s)	0,223
9	Telefone(s)	0,461	10	E-mail(s)	0,479
11	Imagem do Perfil	0,531	12	Foto(s)	0,736
13	Vídeo(s)	0,684	14	Áudio(s)	0,523
15	Biografia	0,274	16	Escolaridade	0,186
17	Ano de Formação	0,135	18	Religião	0,293
19	Emprego Atual	0,212	20	Endereço do Emprego	0,252
21	Emprego(s) Anterior(es)	0,212	22	Cargo	0,234
23	Localização	0,468	24	Status de Relacionamento	0,278
25	Dados de Familiares	0,593	26	Dados de Amigos	0,384
27	Informações sobre Hobbies	0,296	28	Condição de Saúde	0,424

entre os participantes para dois itens (Fotos e Identificação) com os valores mais próximos de 1. Os itens Vídeo(s), Nome, Dados Familiares, Imagem de Perfil e Áudio(s) assumem valores maiores que 0,5. Já os itens Endereço Atual, E-mail(s), Localização e Telefone(s) ficaram próximos à 0,5 de Kappa.

Dos dois ativos com maior concordância (Fotos e Identificação), **34** do 273 participantes escolheram somente esses. Para os itens Vídeo(s), Nome, Dados Familiares, Imagem de Perfil e Áudio(s), apenas **37** participantes os escolheram unicamente. Já os itens Endereço Atual, E-mail(s), Localização e Telefone(s), que ficaram próximos à 0,5, não foram escolhidos unicamente por nenhum participante.

4.1.2 Roubo de Identidade

O roubo de identidade é visto como uma séria ameaça à segurança e à privacidade dos indivíduos, resultando em prejuízos financeiros, emocionais e psicológicos significativos. A Figura 4.4 apresenta as respostas dos participantes para essa ameaça.

Na Figura 4.4 podemos notar que os participantes elegeram os ativos Identificação (89,4%), Nome (83,1%), E-mail (62,5%), Endereço atual (58,8%), Data de nascimento (58,1%), Foto de perfil (55,0%) como os mais relacionados à ameaça de roubo de identidade.

Durante a análise das respostas, notamos que grupo 01 relacionou entre 14 a 21 ativos, sendo Nome e Identificação como escolhidos por todos. O grupo 02 escolheu entre 11 a 15 ativos. Já os grupos 03, 04 e 05 variaram entre 03 a 08 ativos. Fazendo uma análise com base na frequência de acessos, todos os que estão constantemente conectados escolheram os ativos Nome, Identificação, Telefone(s) e E-mail(s). Os mesmos ativos foram escolhidos pelos usuários que se conectam várias vezes ao dia. Por outro lado, para os usuários que acessam menos indicaram ao menos três ativos, tipicamente Sexo, Foto(s) e Vídeo(s).

A média geral do Kappa para roubo de identidade foi de 0,388, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 7 apresenta a análise do Kappa para cada um dos itens em avaliação.

Conforme a Tabela, os ativos com uma concordância maior entre os participantes foram **Nome** e **Identificação**, com os valores acima de 0,8. Os ativos **Data de Nascimento**, **Endereço Atual**, **Telefone(s)**, **E-mail(s)**, **Imagem do Perfil** e **Foto(s)** ficaram acima de à 0,5 de Kappa.

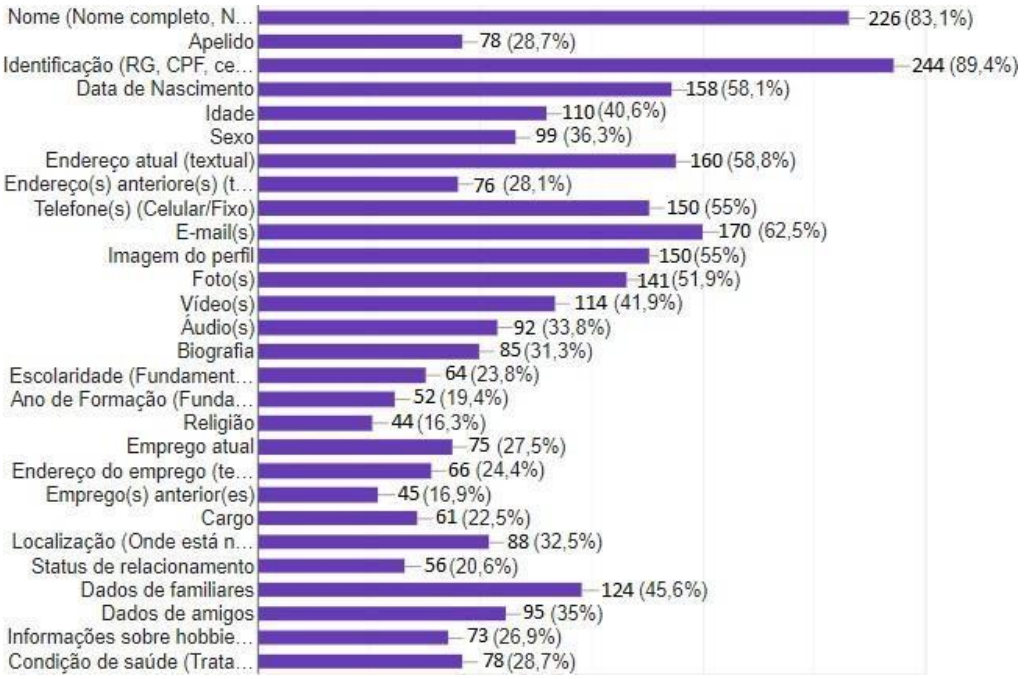

Figura 4.4: Roubo de Identidade

Tabela 7: Valores de KAPPA para Roubo de Identidade

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,827	2	Apelido	0,285
3	Identificação	0,893	4	Data de Nascimento	0,578
5	Idade	0,402	6	Sexo	0,362
7	Endereço Atual	0,586	8	Endereço(s) Anteriore(s)	0,278
9	Telefone(s)	0,549	10	E-mail(s)	0,622
11	Imagem do Perfil	0,549	12	Foto(s)	0,516
13	Vídeo(s)	0,417	14	Áudio(s)	0,336
15	Biografia	0,311	16	Escolaridade	0,234
17	Ano de Formação	0,190	18	Religião	0,161
19	Emprego Atual	0,274	20	Endereço do Emprego	0,241
21	Emprego(s) Anterior(es)	0,164	22	Cargo	0,223
23	Localização	0,322	24	Status de Relacionamento	0,205
25	Dados de Familiares	0,454	26	Dados de Amigos	0,347
27	Informações sobre Hobbies	0,267	28	Condição de Saúde	0,285

4.1.3 Cyberstalking

Cyberstalking é utilizado para assediar ou perseguir um indivíduo ou grupo é caracterizado por comportamentos indesejados ou ameaçadores que são impostos repetidamente.

A Figura 4.5 apresenta as respostas dos participantes para esta ameaça.

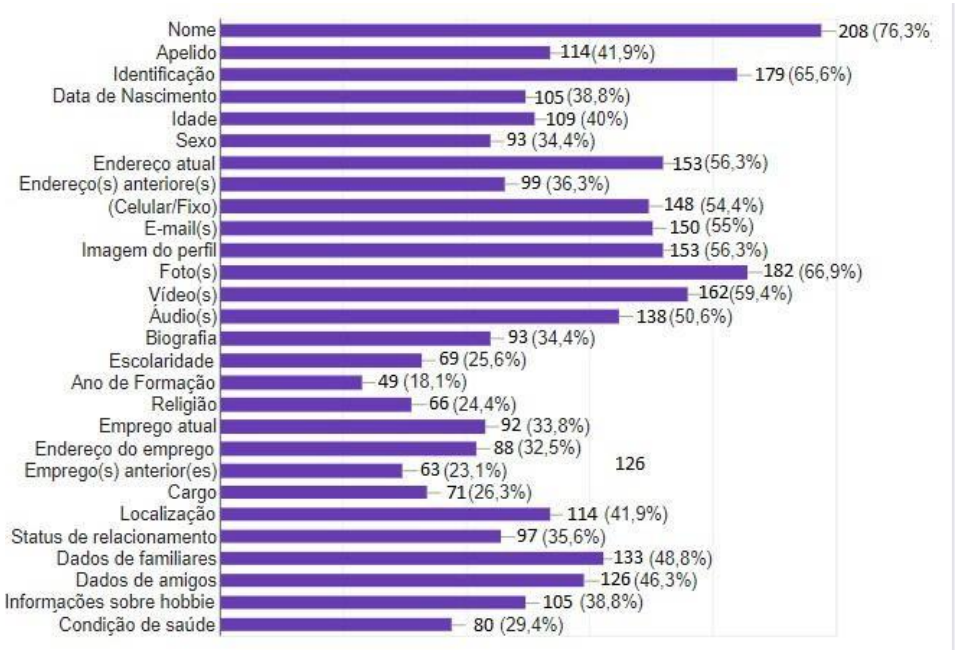

Figura 4.5: Cyberstalking

Os ativos como **Nome**, **Foto**, **Identificação**, **Vídeos**, **Imagem do Perfil**, **Endereço atual**, **E-mail**, **Telefone**, **Áudio** e **Dados de familiares** foram os mais selecionados pelos respondentes.

Durante a análise das respostas considerando o grupo 01, notamos que a quantidade de ativos escolhidos variou entre 19 e 26, sendo os ativos mais destacados **Nome**, **Identificação**, **Endereço Atual**, **Telefone**, **E-mail(s)**, **Imagem do Perfil**, **Foto(s)**, **Vídeo(s)** e **Áudio(s)**. Para o Grupo 02, a escolha de ativos variou de 08 a 22 ativos. Já para os grupos 03, 04 e 05, as escolha também ficaram de 08 a 19 ativos.

Analisando os usuários de acordo com a frequência de acesso, o grupo que permanece constantemente conectado focou mais nos ativos **Nome**, **Apelido** e **Identificação**, correspondendo a mais de 65,0% das respostas. O grupo de usuários que acessam várias vezes ao dia destacou **Nome**, **Identificação** e **Foto(s)** como os ativos mais presentes. Os usuários que acessam uma vez por semana identificaram **Condição de Saúde** como o ativo mais frequente. Aqueles que acessam quatro vezes por semana destacaram **Apelido**, **Sexo**, **Foto(s)** e **Vídeo(s)** como os principais ativos presentes nas respostas. Por fim, o último grupo apresentou **Nome**, **Telefone(s)**, **E-mail(s)** e **Imagem do Perfil** como os ativos mais listados.

Em relação a concordância, a média geral do Kappa foi de 0,423, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 8 apresenta a análise do Kappa para cada um dos itens em avaliação.

A Tabela 8 revela uma concordância maior entre os participantes para o ativos **Nome**, **Identificação** e **Foto(s)**.

Tabela 8: Valores de KAPPA para Cyberstalking

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,761	2	Apelido	0,417
3	Identificação	0,655	4	Data de Nascimento	0,384
5	Idade	0,399	6	Sexo	0,340
7	Endereço Atual	0,560	8	Endereço(s) Anteriore(s)	0,362
9	Telefone(s)	0,545	10	E-mail(s)	0,549
11	Imagem do Perfil	0,560	12	Foto(s)	0,666
13	Vídeo(s)	0,593	14	Áudio(s)	0,505
15	Biografia	0,340	16	Escolaridade	0,252
17	Ano de Formação	0,179	18	Religião	0,241
19	Emprego Atual	0,336	20	Endereço do Emprego	0,322
21	Emprego(s) Anterior(es)	0,230	22	Cargo	0,260
23	Localização	0,417	24	Status de Relacionamento	0,355
25	Dados de Familiares	0,487	26	Dados de Amigos	0,461
27	Informações sobre Hobbies	0,384	28	Condição de Saúde	0,293

4.1.4 Espionagem ou Monitoramento

A espionagem ou monitoramento de usuários é uma ameaça que envolve a coleta de informações, atividades e interações dos usuários, geralmente com o objetivo de obter vantagens indevidas, causar danos ou violar a privacidade das pessoas. A Figura 4.6 apresenta as respostas dos participantes para esta ameaça.

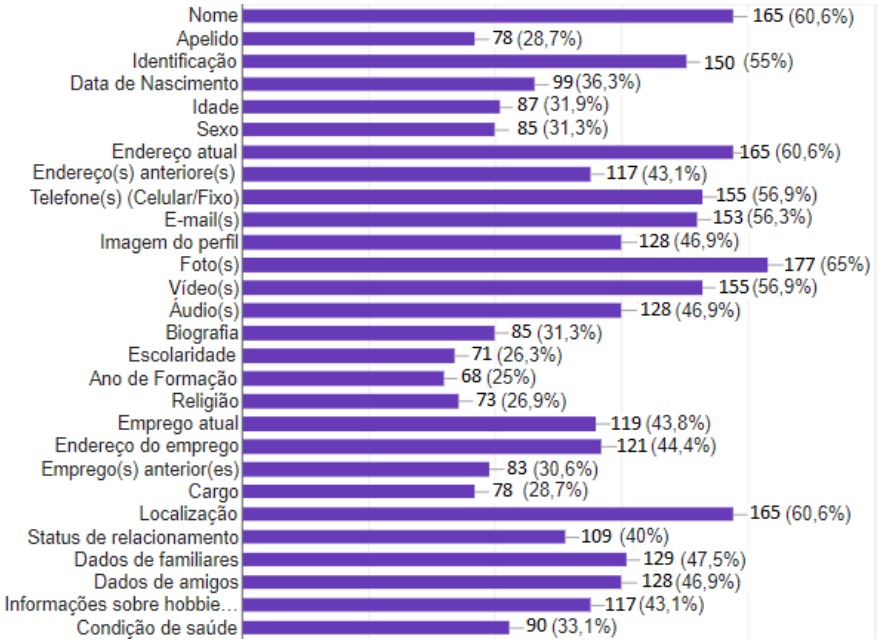

Figura 4.6: Espionagem ou Monitoramento.

Os ativos **Fotos**, **Vídeos**, **Nome**, **Localização**, **Telefone**, **Imagem do Perfil**, **Endereço Atual**, **E-mail**, **Áudio** e **Dados de Familiares** foram os mais selecionados pelos respondentes.

Os usuários que ficam constantemente conectados à RSO foram os que mais destacaram ativos relacionadas à ameaça de espionagem ou monitoramento, com uma média de 24 ativos de informação. Os usuários que acessam várias vezes ao dia apresentaram uma média de 16 ativos. Aqueles que acessam pelo menos uma vez por dia destacaram o ativo **Endereço Atual**, com um intervalo de 07 a 15 ativos selecionados. Os respondentes que acessam uma vez por semana indicaram uma média de 21 ativos destacados, enquanto os que acessam quatro vezes por semana apresentaram uma média de 15 ativos. Os que acessam uma vez por mês selecionaram uma média de 12 ativos, e aqueles que acessam pelo menos uma vez por mês apontaram 6 ativos selecionados.

A média geral do Kappa foi de 0,428, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 9 apresenta a análise do Kappa para cada um dos itens em avaliação.

Tabela 9: Valores de KAPPA para Espionagem ou Monitoramento

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,604	2	Apelido	0,285
3	Identificação	0,549	4	Data de Nascimento	0,362
5	Idade	0,318	6	Sexo	0,311
7	Endereço Atual	0,604	8	Endereço(s) Anteriore(s)	0,428
9	Telefone(s)	0,567	10	E-mail(s)	0,560
11	Imagem do Perfil	0,468	12	Foto(s)	0,648
13	Vídeo(s)	0,567	14	Áudio(s)	0,468
15	Biografia	0,311	16	Escolaridade	0,260
17	Ano de Formação	0,249	18	Religião	0,267
19	Emprego Atual	0,435	20	Endereço do Emprego	0,443
21	Emprego(s) Anterior(es)	0,304	22	Cargo	0,285
23	Localização	0,604	24	Status de Relacionamento	0,399
25	Dados de Familiares	0,472	26	Dados de Amigos	0,468
27	Informações sobre Hobbies	0,428	28	Condição de Saúde	0,329

A Tabela 9 mostra uma concordância maior entre os participantes para quatro itens (**Nome**, **Endereço Atual**, **Foto(s)** e **Localização**) com os valores apontados acima de 0,6. Desses quatro ativos **53**, dos 273 participantes, os escolheram essa combinação unicamente, totalizando 19,41% dos entrevistados.

4.1.5 Gravação não Autorizada

A ameaça por Gravação não autorizada, seja de conversas em chats, videochamadas ou chamadas de áudio, tem o objetivo de chantagear a vítima ou distorcer os dados coletados para exibi-los inadequadamente. A figura 4.7 apresenta as respostas dos participantes sobre esta ameaça.

Os ativos mais selecionado pelos participantes foram *Foto(s)*, **Vídeo(s)** e **Áudio(s)**, com média acima de 60,0%, tendo metade dos participantes informando pelo menos uma delas.

Durante a análise das respostas por idade do grupo 01, os ativos **Vídeo(s)** e **Áudio(s)** foram os mais selecionados (93,75%) e com uma média de 13 ativos por participante. Para o grupo 02, os ativos **Foto(s)**, **Vídeo(s)** e **Áudio(s)** apresentaram média de 72,28% entre os participante, com a quantidade de escolhas variando entre 05 a 11 ativos. As médias de ativos informados pelos grupos 03, 04 e 05 foram, respectivamente, de 04 a 12 ativos.

Já na análise dos usuários, para os que estão sempre conectados o número de ativos selecionados apresentou uma variância entre 05 a 13 selecionados. Entre os usuários que acessam varias vezes ao dia, o intervalo foi entre 04 a 07 ativos. Por outro lado, usuários que acessam

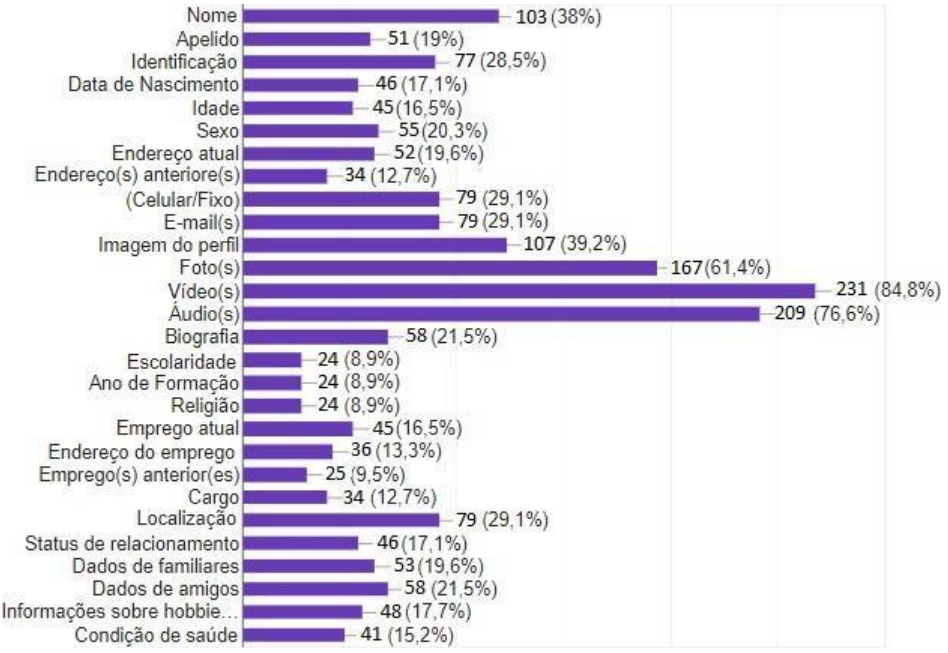

Figura 4.7: Gravação não Autorizada.

a rede quatro vezes por semana, pelo menos uma vez por semana ou pelo menos uma vez por mês, a média ficou entre 02 a 13 ativos presentes como ameaças, sendo **Foto(s)** e **Vídeo(s)** os mais presentes.

A média geral do Kappa foi de 0,251, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 10 apresenta a análise do Kappa para cada um dos itens em avaliação.

Tabela 10: Valores de KAPPA para Gravação não autorizada

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,377	2	Apelido	0,186
3	Identificação	0,282	4	Data de Nascimento	0,168
5	Idade	0,164	6	Sexo	0,201
7	Endereço Atual	0,190	8	Endereço(s) Anteriore(s)	0,124
9	Telefone(s)	0,289	10	E-mail(s)	0,289
11	Imagem do Perfil	0,391	12	Foto(s)	0,611
13	Vídeo(s)	0,846	14	Áudio(s)	0,765
15	Biografia	0,212	16	Escolaridade	0,087
17	Ano de Formação	0,087	18	Religião	0,087
19	Emprego Atual	0,164	20	Endereço do Emprego	0,131
21	Emprego(s) Anterior(es)	0,091	22	Cargo	0,124
23	Localização	0,289	24	Status de Relacionamento	0,168
25	Dados de Familiares	0,194	26	Dados de Amigos	0,212
27	Informações sobre Hobbies	0,175	28	Condição de Saúde	0,150

Os valores de Kappa para item, conforme a Tabela 10, mostram uma concordância maior

entre os participantes para três ativos (**Foto(s)**, **Vídeo(s)** e **Áudio(s)**) com os valores acima de 0,6. Os ativos **Nome** e **Imagem de Perfil** assumem valores maiores que 0,3, considerado baixo. Dos três ativos com maior concordância, **44** do 273 participantes escolheram somente esses.

4.1.6 Clonagem de Perfil

A ameaça por Clonagem de Perfil envolve a utilização dos dados compartilhados por um usuário para clonar seu perfil, sem que a rede social ou o próprio usuário percebam. A Figura 4.8 revela os ativos que os participantes consideram como possíveis à ameaça de clonagem de perfil.

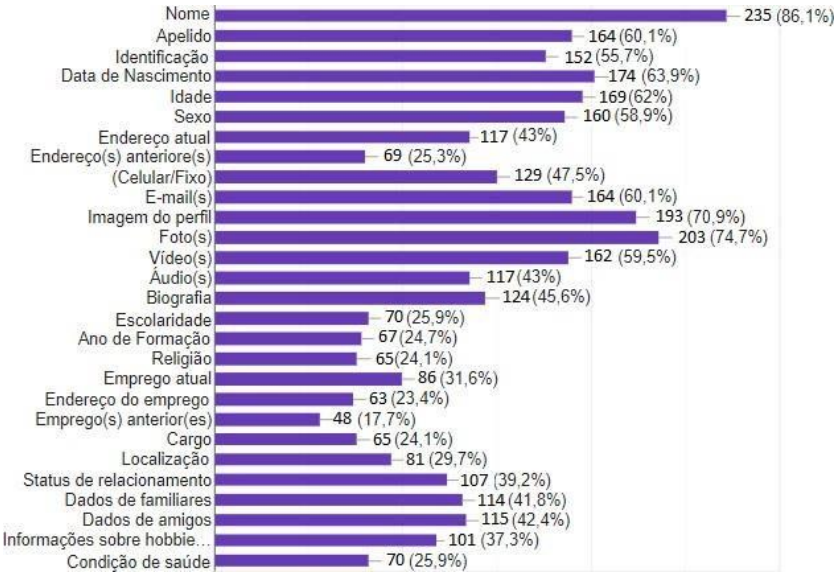

Figura 4.8: Clonagem de Perfil

Dentre os ativos de informação, **Nome** foi o mais frequentemente listado, com 235 votos dos participantes. Em seguida vieram os ativos **Fotos** (203 participantes) e **Imagem do Perfil** (193 participantes).

A análise das respostas por idade do Grupo 01 revelou que o ativo **Nome** foi o mais selecionado, com uma média de 98,15%. O segundo ativo foi **Foto(s)**, com um total de 82 respostas entre os jovens. A média de ativos selecionados pelo grupo 01 foi de 14 ativos. O grupo 02 também apresentou uma média de 14 ativos selecionados, enquanto os grupos 03, 04 e 05 tiveram médias de 07 a 11 ativos.

Analisando pela frequência de conexão dos usuários, aqueles que estão sempre conectados apresentaram uma variância entre 12 a 17 ativos selecionadas. Entre os usuários que acessam várias vezes ao dia, o intervalo foi de 14 a 17 ativos. Usuários que acessam a rede quatro vezes por semana, pelo menos uma vez por semana ou pelo menos uma vez por mês indicaram uma média entre 05 a 07 ativos selecionados.

A média geral do Kappa foi de 0,442, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 11 apresenta a análise do Kappa para cada um dos itens em avaliação.

Tabela 11: Valores de KAPPA para Clonagem de perfil

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,860	2	Apelido	0,600
3	Identificação	0,556	4	Data de Nascimento	0,637
5	Idade	0,619	6	Sexo	0,586
7	Endereço Atual	0,428	8	Endereço(s) Anteriore(s)	0,252
9	Telefone(s)	0,472	10	E-mail(s)	0,600
11	Imagem do Perfil	0,706	12	Foto(s)	0,743
13	Vídeo(s)	0,593	14	Áudio(s)	0,428
15	Biografia	0,454	16	Escolaridade	0,256
17	Ano de Formação	0,245	18	Religião	0,238
19	Emprego Atual	0,315	20	Endereço do Emprego	0,230
21	Emprego(s) Anterior(es)	0,175	22	Cargo	0,238
23	Localização	0,296	24	Status de Relacionamento	0,391
25	Dados de Familiares	0,417	26	Dados de Amigos	0,421
27	Informações sobre Hobbies	0,369	28	Condição de Saúde	0,256

Conforme a Tabela 11, existe uma concordância maior entre os participantes para três itens (**Nome**, **Imagem do Perfil** e **Foto(s)**) com os valores apontado acima de 0,7. Os ativos como **Apelido**, **Identificação**, **Data de Nascimento**, **Idade**, **Sexo**, **E-mail(s)** e **Vídeo(s)** ficaram acima de à 0,5 de acordo com o Kappa. Dos três ativos com maior concordância, **51** do 273 respondentes selecionaram somente esses, o que em números representa 18,68% dos participantes.

4.1.7 Rastreamento e Inferência de Dados

A ameaça de rastreamento e inferência de dados consiste na descoberta de informações pessoais não diretamente compartilhadas pelo usuário em seus perfis. A Figura 4.9, revela os ativos que os participantes consideram como possíveis em relação a esta ameaça.

Conforme as respostas dos participantes, 06 ativos foram selecionados por mais de 50,00%: **Nome**, **Identificação**, **Endereço Atual**, **Telefone**, **E-mail** e **Localização**.

Por meio da análise das respostas por idade do grupo 01, notamos que o ativo **Nome** foi o mais selecionado, com uma média de 98,15%. O segundo ativo mais frequente foi **Foto(s)**, com um total de 82 respostas entre os jovens. A média de ativos selecionados pelo grupo 01 foi de 14, com variações nas respostas sobre os ativos selecionados. O grupo 02 apresentou uma média de 14 ativos selecionados, enquanto os grupos 03, 04 e 05 apresentaram médias de 07 a 11 ativos, conforme as respostas de cada participante.

Já analisando de acordo com a frequência de conexão, aqueles que estão sempre conectados apresentaram uma variação entre 12 e 17 ativos selecionados. Entre os usuários que acessam várias vezes ao dia, o intervalo foi de 14 a 17 ativos informados. Usuários que acessam a rede quatro vezes por semana, pelo menos uma vez por semana, ou pelo menos uma vez por mês, indicaram uma média entre 05 e 07 ativos selecionados.

A média geral do Kappa foi de 0,342, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 12 apresenta a análise do Kappa para cada um dos itens em avaliação.

Conforme a Tabela 12, existe uma concordância maior entre os participantes para seis itens (**Nome, Identificação, Endereço Atual, Telefone(s), E-mail(s) e Localização**) com os valores apontado acima de 0,5. Desses ativos, **17** do 273 participantes os escolheram unicamente essa combinação.

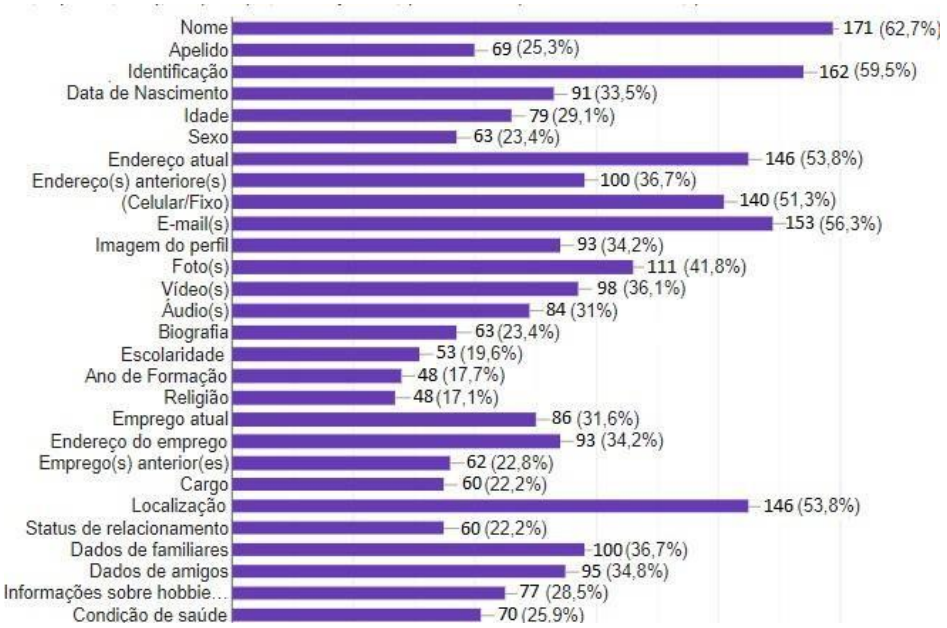

Figura 4.9: Rastreamento e Inferência de Dados.

Tabela 12: Valores de KAPPA para Rastreamento e Inferência

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,626	2	Apelido	0,252
3	Identificação	0,593	4	Data de Nascimento	0,333
5	Idade	0,289	6	Sexo	0,230
7	Endereço Atual	0,534	8	Endereço(s) Anteriore(s)	0,366
9	Telefone(s)	0,512	10	E-mail(s)	0,560
11	Imagem do Perfil	0,340	12	Foto(s)	0,406
13	Vídeo(s)	0,358	14	Áudio(s)	0,307
15	Biografia	0,230	16	Escolaridade	0,194
17	Ano de Formação	0,175	18	Religião	0,175
19	Emprego Atual	0,315	20	Endereço do Emprego	0,340
21	Emprego(s) Anterior(es)	0,227	22	Cargo	0,219
23	Localização	0,534	24	Status de Relacionamento	0,219
25	Dados de Familiares	0,366	26	Dados de Amigos	0,347
27	Informações sobre Hobbies	0,282	28	Condição de Saúde	0,256

4.1.8 Reconhecimento Facial

A ameaça por Reconhecimento Facial envolve a identificação do rosto de uma pessoa em uma foto ou vídeo e a posterior referência cruzada com outros conjuntos de dados para expor informações pessoais. A Figura 4.10 representa os ativos que foram listados pelos respondentes que consideram ameaça por reconhecimento Facial.

Dos ativos selecionados pelos participantes, **Imagem do Perfil**, **Foto(s)**, **Vídeo(s)**, **Nome** e **Identificação** foram os mais destacados, com uma média de 60,0% dos participantes. Um dado interessante nessa ameaça é que os respondentes com idades entre 16 e 45 anos consideraram o

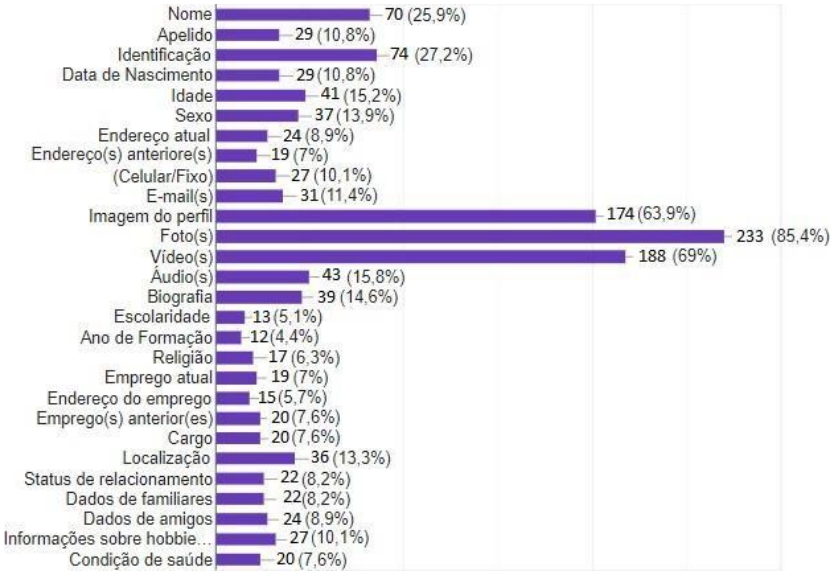

Figura 4.10: Reconhecimento Facial.

ativo **Foto** como a principal ameaça para o usuário.

Ao analisar os usuários que ficam sempre conectados, os ativos **Vídeo(s)** e **Imagem do Perfil** apresentaram um índice de 80,0% de presença. O grupo que acessa várias vezes ao dia apresentou o maior índice de resposta, com 10 ativos, sendo **Foto(s)** o mais frequente entre os demais. Os usuários que acessam uma vez por semana apresentaram um índice de 04 ativos, enquanto os participantes que acessam quatro vezes por semana tiveram uma média de 07 informações selecionadas. Aqueles que acessam uma vez por mês apresentaram 05 informações selecionadas.

A média geral do Kappa foi de 0,172, o que pode ser interpretado como concordância mais perto do acaso do que uma concordância perfeita. A Tabela 13 apresenta a análise do Kappa para cada um dos itens em avaliação.

Tabela 13: Valores de KAPPA para Reconhecimento Facial

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,256	2	Apelido	0,106
3	Identificação	0,271	4	Data de Nascimento	0,106
5	Idade	0,150	6	Sexo	0,135
7	Endereço Atual	0,087	8	Endereço(s) Anteriore(s)	0,069
9	Telefone(s)	0,098	10	E-mail(s)	0,113
11	Imagem do Perfil	0,637	12	Foto(s)	0,853
13	Vídeo(s)	0,688	14	Áudio(s)	0,157
15	Biografia	0,142	16	Escolaridade	0,047
17	Ano de Formação	0,043	18	Religião	0,062
19	Emprego Atual	0,069	20	Endereço do Emprego	0,054
21	Emprego(s) Anterior(es)	0,073	22	Cargo	0,073
23	Localização	0,131	24	Status de Relacionamento	0,080
25	Dados de Familiares	0,080	26	Dados de Amigos	0,087
27	Informações sobre Hobbies	0,098	28	Condição de Saúde	0,073

Conforme a Tabela 13, mostram uma concordância maior entre os participantes para três itens (Imagem do Perfil, Foto(s) e Vídeo(s)) com os valores apontado acima de 0,6. Os itens apontados com maior concordância em Reconhecimento Facial, **42** do 273 participantes os escolheram unicamente.

4.2 Discussão dos Resultados

A Tabela 14 sumariza os valores médios de Kappa para todas as ameaças avaliadas no questionário.

Tabela 14: **Kappa Médio de todas as Ameaças**

Ameaças	Kappa Médio	Interpretação da Análise
Cyberstalking	0,423	Concordância Ao Acaso
Roubo de Identidade	0,388	Concordância Ao Acaso
Reconhecimento Facial	0,172	Concordância Ao Acaso
Ameaça à reputação	0,382	Concordância Ao Acaso
Rastreamento e Inferência	0,342	Concordância Ao Acaso
Clonagem de Perfil	0,442	Concordância Ao Acaso
Espionagem	0,428	Concordância Ao Acaso
Gravação não autorizada	0,251	Concordância Ao Acaso

Uma vez que um valor acima de 0,5 pode ser considerado como uma concordância média, nenhuma das ameaças atingiu esse patamar. Todas ficam mais próximas de uma concordância ao acaso. Desta forma, os resultados apresentados na Tabela 14 demonstram que a função esperada do questionário não foi alcançada.

Assumindo que as perguntas existentes no questionário não são o problema, tendo em vista que é a pergunta é praticamente a mesma e os itens a serem escolhidos são os mesmos, elencamos duas possibilidades. A primeira delas é a falta de conhecimento sobre o assunto. Embora tenhamos apresentado dois catálogos (ameaças e ativos) para estudo e familiarização com o assunto, os participantes não foram obrigados a acessá-los. Notamos que apenas 128 participantes visualizaram ambos. Vale ressaltar que dos 273 participantes, 185 se declararam como estudando, formado ou atuando na área de Tecnologia da Informação. É bastante plausível que, por ser, estar ou atuar na área de computação, a maioria dos participantes tenha ignorado os catálogos e respondido apenas com base em seus conhecimentos próprios.

A segunda possibilidade é o tempo de resposta. Ao analisar o tempo de acesso para responder ao questionário, inclusive com a visualização dos catálogos, notamos que o intervalo de tempo varia entre 3 e 5 minutos (o menor tempo foi 03min01s e o maior de 05min23s).

A Figura 4.11 ilustra todos os ativos escolhidos pelos usuários para representar as ameaças. Analisando as respostas dos usuários em relação às ameaças, fica claro que, tanto por grupo de idade quanto por frequência de acesso, as respostas variam parcialmente em relação ao ativo mais presente, apresentando uma média para cada faixa (idade x frequência de acesso). No entanto, há uma variação nas respostas de cada categoria. Enquanto alguns usuários responderam que apenas um ativo representa uma ameaça, outros identificaram todos os ativos como possíveis ameaças.

Um destaque importante no primeiro estudo, vem dos respondentes que possuem mais de uma Rede Social Online (RSO) foram os que mais informaram ativos que poderiam ser

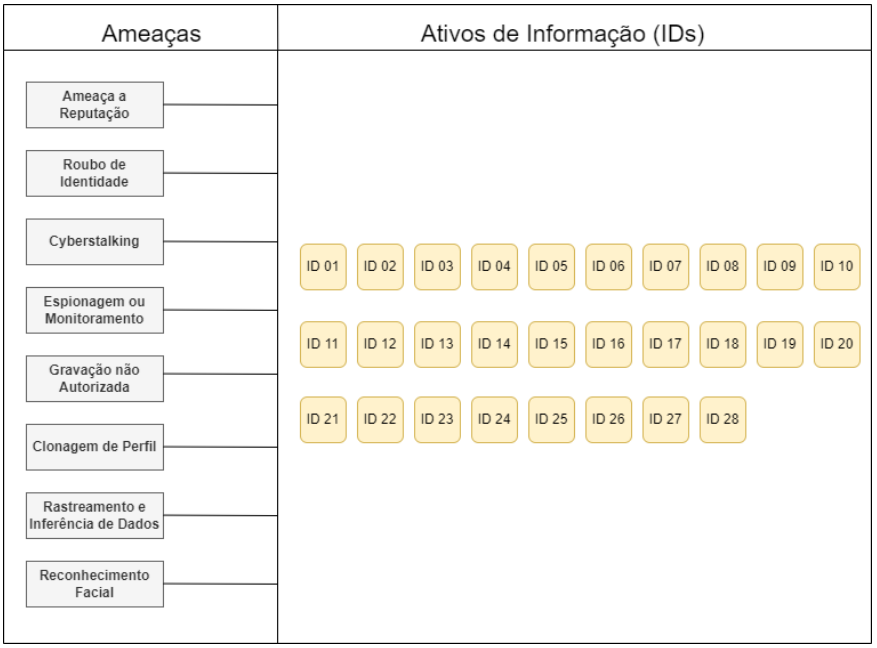

Figura 4.11: Cateterização das Ameaças.

comprometidos. Em contraste, os que possuíam apenas uma rede social indicaram, em média, ao menos sete ativos que poderiam ser comprometidos por essa ameaça.

Capítulo 5

Segundo Estudo

Diante da falta de concordância no primeiro estudo, montamos um segundo. Como participantes, escolhemos convidar especialistas na área de segurança da informação. Entramos em contato através de e-mail, grupos de WhatsApp e no Linkedln. No total, obtivemos o aceite de 17 especialistas. O mesmo questionário utilizado pelo público geral foi aplicado a eles e da mesma forma (TCLE, acesso aos catálogos e resposta as oito perguntas).

5.1 Análise das Respostas

Nesta seção, analisamos as respostas dos participantes em relação a oito ameaças a privacidade.

5.1.1 Ameaça à reputação

A Figura 5.1 representa a resposta dos 17 especialistas em relação à ameaça a reputação.

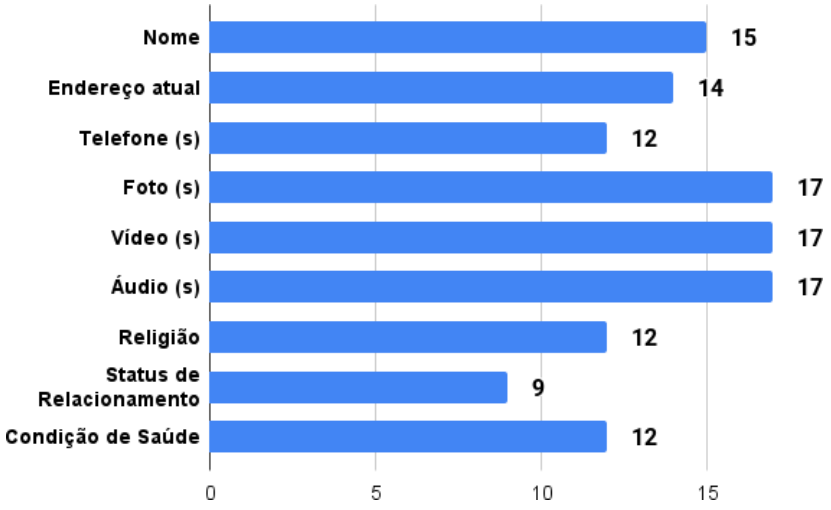

Figura 5.1: Ameaça a Reputação - Especialistas.

A Figura demonstra que os especialistas listaram um total de 09 ativos, alguns sendo escolhidos por todos. Os ativos selecionados pelos especialistas foram: **Nome**, **Endereço Atual**, **Telefone(s)**, **Foto(s)**, **Vídeo(s)**, **Áudio(s)**, **Religião**, **Status de Relacionamento** e **Condição de Saúde**.

A Tabela 15 apresenta a análise do Kappa somente para os itens que foram avaliados.

Tabela 15: Valores de KAPPA para Ameaça a Reputação

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,882	7	Endereço Atual	0,823
9	Telefone(s)	0,705	12	Foto(s)	1,000
13	Vídeos(s)	1,000	14	Áudio(s)	1,000
18	Religião	0,705	24	Status de Relacionamento	0,529
28	Condição de Saúde	0,705			

A avaliação da concordância dos especialistas apresentou-se como excelente, com Kappa médio de **0,816**.

5.1.2 Roubo de Identidade

A Figura 5.2 ilustra a resposta dos especialistas.

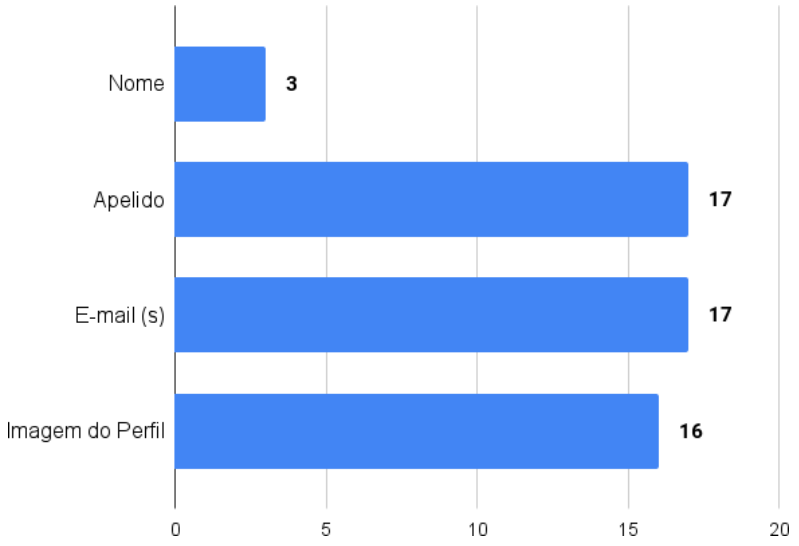

Figura 5.2: Análise de dados - Roubo de Identidade

Para todos os especialistas, somente os ativos de informação **Nome**, **Apelido**, **Telefon(s)** e **E-mail(s)** foram considerados como necessários para identificar ameaças de roubo de identidade, com 100,00% de respostas. Nota-se que para esta ameaça, os ativos relacionados são aqueles frequentemente solicitados quando um usuário necessita trocar ou recuperar sua senha de acesso, independentemente se é em uma RSO ou outro tipo de sistema ou plataforma.

No caso desta ameaça, o coeficiente de Kappa dos especialista foi 1, provando que as respostas convergiram para uma concordância perfeita.

5.1.3 Cyberstalking

A Figura 5.3 ilustra as respostas dos 17 especialistas sobre ativos ligados a Cyberstalking.

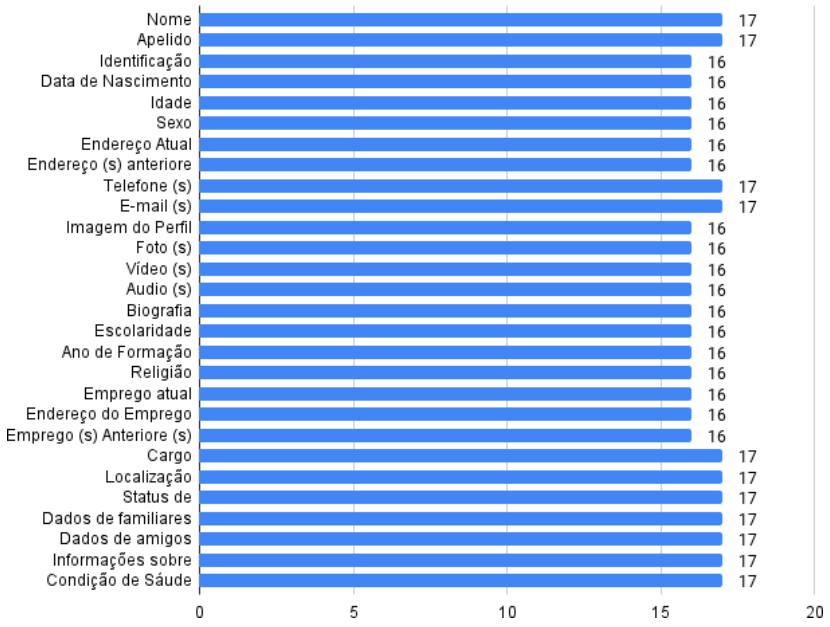

Figura 5.3: Cyberstalking

A Tabela 16 apresenta a análise do Kappa somente para os itens que foram avaliados.

Tabela 16: Valores de KAPPA para Cyberstalking

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	1,000	2	Apelido	1,000
3	Identificação	0,941	4	Data de Nascimento	0,941
5	Idade	0,941	6	Sexo	0,941
7	Endereço Atual	0,941	8	Endereço(s) Anteriore(s)	0,941
9	Telefone(s)	1,000	10	E-mail(s)	1,000
11	Imagem do Perfil	0,941	12	Foto(s)	0,941
13	Vídeo(s)	0,941	14	Áudio(s)	0,941
15	Biografia	0,941	16	Escolaridade	0,941
17	Ano de Formação	0,941	18	Religião	0,941
19	Emprego Atual	0,941	20	Endereço do Emprego	0,941
21	Emprego(s) Anterior(es)	0,941	22	Cargo	1,000
23	Localização	1,000	24	Status de Relacionamento	1,000
25	Dados de Familiares	1,000	26	Dados de Amigos	1,000
27	Informações sobre Hobbies	1,000	28	Condição de Saúde	1,000

A avaliação por concordância dos especialistas conforme a Tabela 16 apresentou como excelente **0,946**.

5.1.4 Espionagem ou Monitoramento

A Figura 5.4 ilustra as respostas dos especialistas.

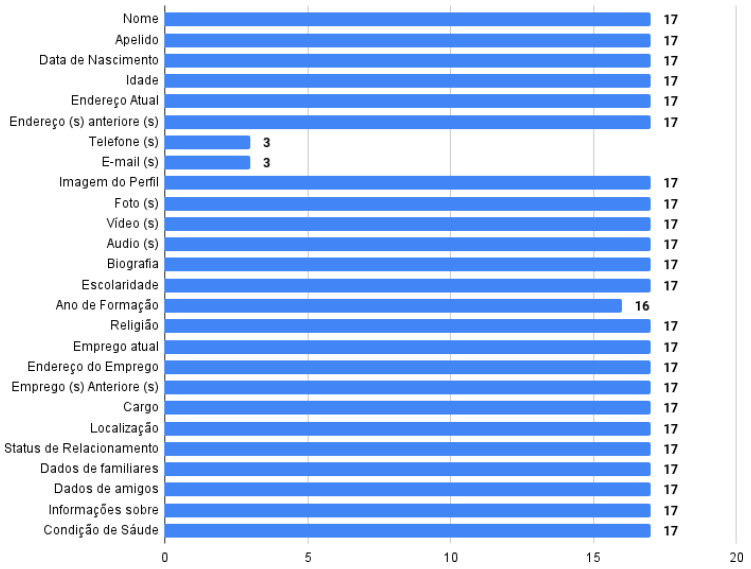

Figura 5.4: Espionagem - Especialistas.

A análise das respostas revelou que os especialistas listaram um total de 26 ativos, com uma média de 3 a 17 respostas por ativo. Os ativos não selecionados pelos especialistas foram: **Identificação** e **Sexo**.

A Tabela 17 apresenta a análise do Kappa somente para os itens que foram avaliados.

Tabela 17: Valores de KAPPA para Espionagem ou Monitoramento

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	1,000	2	Apelido	1,000
4	Data de Nascimento	1,000	5	Idade	1,000
7	Endereço Atual	1,000	8	Endereço(s) Anteriores(s)	1,000
9	Telefone(s)	0,176	10	E-mail(s)	0,176
11	Imagem do Perfil	1,000	12	Foto(s)	1,000
13	Vídeo(s)	1,000	14	Áudio(s)	1,000
15	Biografia	1,000	16	Escolaridade	1,000
17	Ano de Formação	0,941	18	Religião	1,000
19	Emprego Atual	1,000	20	Endereço do Emprego	1,000
21	Emprego(s) Anterior(es)	1,000	22	Cargo	1,000
23	Localização	1,000	24	Status de Relacionamento	1,000
25	Dados de Familiares	1,000	26	Dados de Amigos	1,000
27	Informações sobre Hobbies	1,000	28	Condição de Saúde	1,000

Novamente, o kappa médio apresentou-se como excelente (**0,939**), mostrando uma alta concordância entre os especialistas.

5.1.5 Gravação não Autorizada

A Figura 5.5 ilustra as respostas dos especialistas.

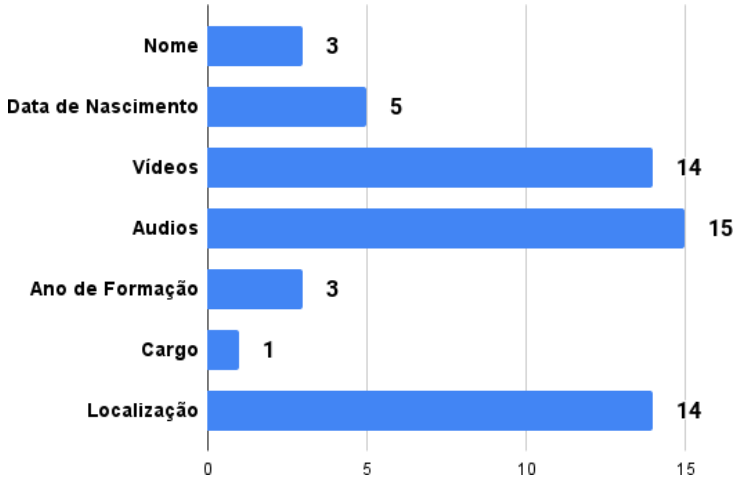

Figura 5.5: Gravação não autorizada 17- Especialistas.

A Tabela 18 apresenta a análise do Kappa somente para os itens que foram avaliados.

Tabela 18: Valores de KAPPA para Gravação não Autorizada

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,176	4	Data de Nascimento	0,294
13	Vídeo(s)	0,823	14	Áudio(s)	0,882
17	Ano de Formação	0,176	22	Cargo	0,058
23	Localização	0,823			

Os valores de Kappa para cada item respondido na Tabela 18 mostram uma concordância maior entre os avaliadores para três itens (**Áudio(s)**, **Vídeos(s)** e **Localização**) com os valores próximos a 1 (0,882, 0,823 e 0,823, respectivamente). Todos os outros itens (Data de Nascimento, Nome, Ano de Formação e Cargo) assumiram valores próximos que 0.

Dos três ativos com maior concordância (Áudio(s), Foto(s) e Localização), 10 especialistas escolheram eles unicamente. Os demais optaram outras combinações de ativos, como Nome e Localização e Data de Nascimento, Vídeo(s), Audio(s) e Ano de Formação, por exemplo.

5.1.6 Clonagem de Perfil

A Figura 5.6 ilustra as respostas dos especialistas.

As respostas dos especialistas revelaram que, ao todo, foram listados 18 ativos dos 28 disponíveis. Os ativos selecionados incluem **Idade**, **E-mail(s)**, **Biografia**, **Escolaridade**, **Emprego Atual** e **Localização**. Os demais ativos apresentaram uma variação mínima, com apenas 7 informações selecionadas.

A Tabela 19 apresenta a análise do Kappa somente para os itens que foram avaliados.

A avaliação por concordância dos especialistas apresentou-se como excelente **0,888**.

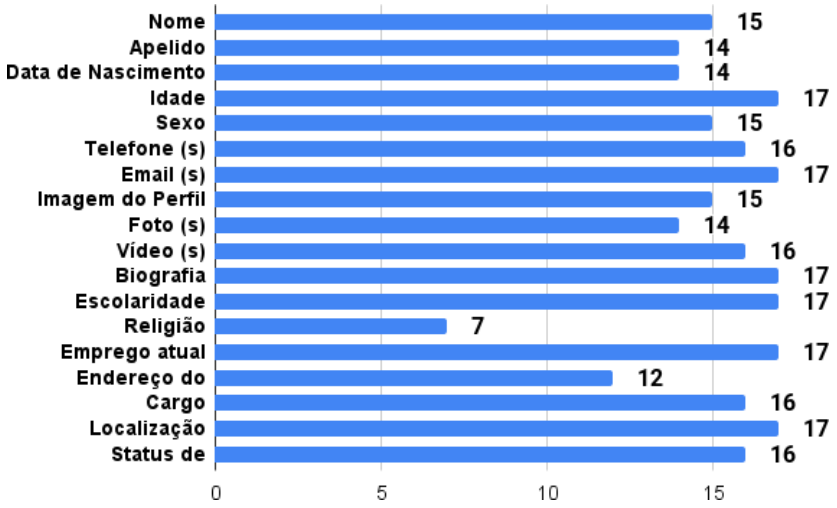

Figura 5.6: Clonagem de Perfil - Especialistas.

Tabela 19: Valores de KAPPA para Clonagem de Perfil

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,833	2	Apelido	0,777
4	Data de Nascimento	0,777	5	Idade	1,000
6	Sexo	0,833	9	Telefone(s)	0,888
10	E-mail(s)	1,000	11	Imagem do perfil	0,833
12	Foto(s)	0,777	13	Vídeo(s)	0,888
15	Biografia	1,000	16	Escolaridade	1,000
18	Religião	0,388	19	Emprego Atual	1,000
20	Endereço do Emprego	0,666	22	Cargo	0,888
23	Localização	1,000	24	Status de Relacionamento	0,888

5.1.7 Rastreamento e Inferência de Dados

A Figura 5.7, ilustra as respostas dos 17 especialistas sobre Rastreamento e Inferência de Dados.

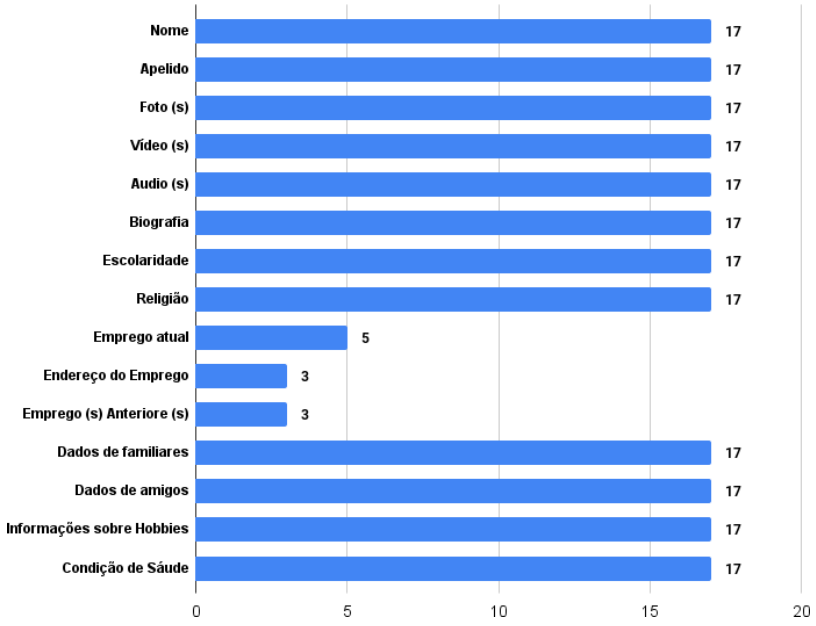

Figura 5.7: Rastreamento e Inferência de Dados

A Tabela 20 apresenta a análise do Kappa somente para os itens que foram avaliados.

Tabela 20: Valores de KAPPA para Rastreamento e Inferência de Dados

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	1,000	2	Apelido	1,000
12	Foto(s)	1,000	13	Vídeo(s)	1,000
14	Áudio(s)	1,000	15	Biografia	1,000
14	Escolaridade	1,000	18	Religião	1,000
19	Emprego Atual	0,294	20	Endereço do Emprego	0,176
21	Emprego(s) Anteriore(s)	0,176	25	Dados de Familiares	1,000
26	Dados de amigos	1,000	27	Informações sobre Hobbies	1,000

A avaliação de concordância apontou um resultado médio de**0,863**, considerado excelente para os 14 ativos de informação avaliados.

5.1.8 Reconhecimento Facial

Segundo as respostas dos especialistas (Figura 5.8), os ativos **Nome**, **Sexo**, **Áudio(s)**, **Biografia** e **Ano de Formação** não foram caracterizados como uma ameaça para o reconhecimento Facial.

A Tabela 21 apresenta a análise do Kappa somente para os itens que foram avaliados.

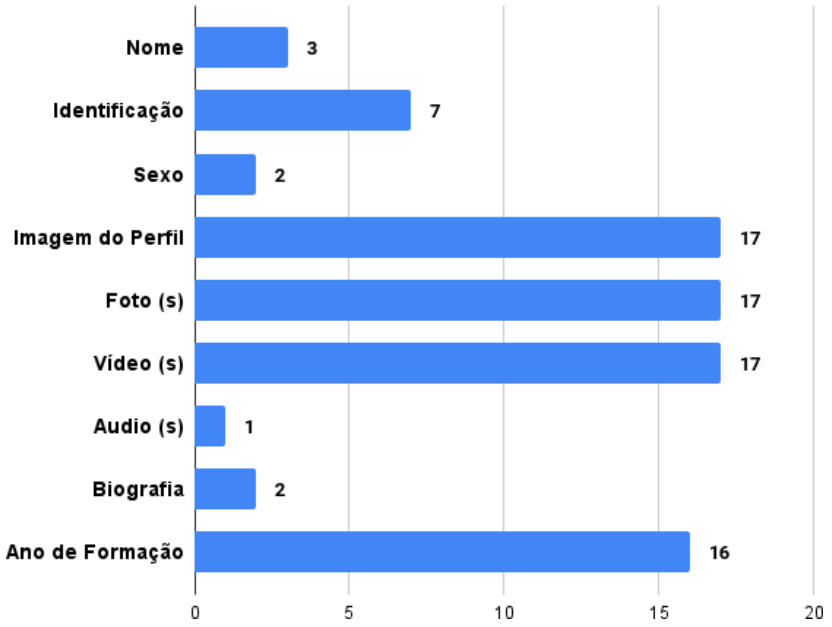

Figura 5.8: Reconhecimento Facial

Tabela 21: Valores de KAPPA para Reconhecimento Facial

Item	Ativos	Kappa	Item	Ativos	Kappa
1	Nome	0,176	3	Identificação	0,411
6	Sexo	0,117	11	Imagem do Perfil	1,000
12	Foto(s)	1,000	13	Vídeo(s)	1,000
14	Áudio(s)	0,058	15	Biografia	0,117
17	Ano de Formação	0,176			

5.2 Discussão dos Resultados

Os valores de Kappa para a ameaça de **Roubo de Identidade** mostraram a unanimidade dos especialistas para os quatro ativos (Nome, Apelido, Telefone(s) e E-mail(s)). Em seguida, a ameaça de **Cyberstalking** apresentou a segunda maior concordância, com um valor de 0,964. A terceira ameaça com maior concordância foi **Espionagem**, com um valor de 0,934. **Clonagem de Perfil** foi a próxima ameaça, com um valor de 0,886, seguida por **Rastreamento e Inferência**, com 0,831. A **Ameaça à Reputação** apresentou uma concordância forte com nove ativos selecionados.

Vale destacar que, das oito ameaças avaliadas, duas não foram consideradas unânimes, apresentando concordância ao acaso, os valores apresentados na Tabela 18 e 21. Essas ameaças são: Gravação não Autorizada, onde o ativo Vídeo(s) obteve 88,23% de preferência (15 dos 17 participantes); e Reconhecimento Facial, onde, dos nove ativos selecionados, ao menos um especialista informou um ativo diferente dos demais.

A Tabela 22 sumariza os valores médios de Kappa para todas as ameaças avaliadas no questionário. Assumindo que um valor abaixo de 0,5 indicam *Concordância ao Acaso* e valores acima de 0,5 indicam *Concordância Perfeita ou Quase Perfeita*, notamos que as respostas dos especialistas apresentaram melhores concordâncias. Tal fato pode ser interpretado pelo grau de conhecimento sobre o tema que estes participantes apresentam.

Tabela 22: **Kappa Médio de todas as Ameaças**

Ameaças	Kappa Médio	Interpretação da Análise
Cyberstalking	0,964	Concordância Quase Perfeita
Roubo de Identidade	1,000	Concordância Perfeita
Reconhecimento Facial	0,450	Concordância ao Acaso
Ameaça à reputação	0,816	Concordância Quase Perfeita
Rastreamento e Inferência	0,843	Concordância Quase Perfeita
Clonagem de Perfil	0,842	Concordância Quase Perfeita
Espionagem	0,934	Concordância Quase Perfeita
Gravação não autorizada	0,461	Concordância ao Acaso

No geral, a pesquisa mostrou uma concordância perfeita ou considerada quase perfeita entre os especialistas, como exceção às ameaças de **Gravação não autorizada** e **Reconhecimento Facial**, onde, em média, 07 especialistas escolheram itens possivelmente não relacionados as ameaças.

Assim como no público geral, notamos que, por mais que tenhamos disponibilizado os catálogos, apenas 09 especialistas os acessaram. Embora todos os participantes tenham afirmados serem formados na área de Segurança e estarem atuando na área de computação, quase a metade respondeu ao questionário apenas com base em seus conhecimentos próprios. Por outro lado, o tempo de acesso para responder ao questionário, inclusive com a visualização dos catálogos, foi um pouco maior em comparação ao público geral. O intervalo de tempo para os especialistas varia entre 5 e 6 minutos (o menor tempo foi 05min12s e o maior de 06min43s).

A Figura 5.9 vincula as ameaças a privacidade com os ativos de informação, com base nas respostas dos especialistas.

Nota-se, na Figura, que a **Ameaça a Reputação**, com Kappa médio de 0,793, é vinculada aos ativos Nome (ID1), Endereço Atual (ID7), Telefone(s) (ID9), Foto(s) (ID12), Vídeo(s) (ID13), Áudio(s) (ID14), Religião (ID18), Status de Relacionamento (ID24) e Condições de Saúde (ID28). Já a ameaça de **Roubo de Identidade**, com Kappa igual a 1, é composta por

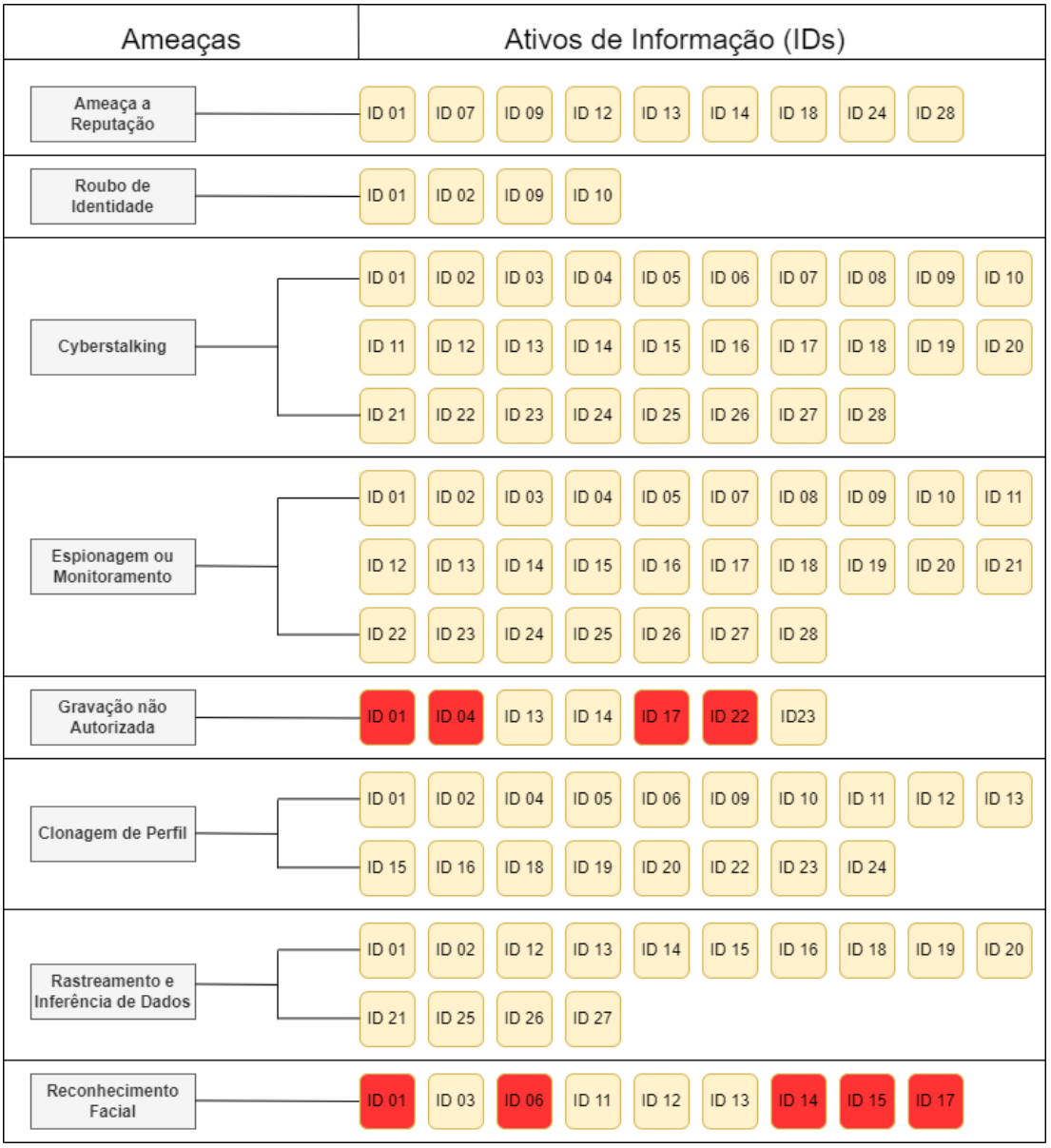

Figura 5.9: Categorização dos Ativos de Informação.

Nome (ID1), Apelido (ID2), Telefone(s) (ID9) e E-mail(s) (ID10). A ameaça de **Cyberstalking**, com Kappa médio de 0,964, é composta por todos os 28 ativos e que a de **Espionagem ou Monitoramento**, com Kappa médio de 0,934, também, apenas com a ausência do ativo Sexo (ID6).

A ameaça de **Clonagem de Perfil**, com Kappa médio de 0,886, é composta por Nome (ID1), Apelido (ID2), Data de Nascimento (ID4), Idade (ID5), Sexo (ID6), Telefone(s) (ID9), E-mail(s) (ID10), Imagem de Perfil (ID11), Foto(s) (ID12), Vídeo(s) (ID13), Biografia (ID15), Escolaridade (ID16), Religião (ID18), Emprego Atual (ID19), Endereço do Emprego (ID20), Cargo (ID22),

Localização (ID23) e Status de Relacionamento (ID24). Já a ameaça de **Rastreamento e Inferência de Dados**, com Kappa médio de 0,831, é composta por Nome (ID1), Apelido (ID2), Foto(s) (ID12), Vídeo(s) (ID13), Áudio(s) (ID14), Biografia (ID15), Escolaridade (ID16), Religião (ID18), Emprego Atual (ID19), Endereço do Emprego (ID20), Empregos Anteriore(s) (ID21), Dados Familiares (ID25), Dados de Amigos (ID27) e Informações sobre Hobbies (ID27). Por fim, as ameaças de **Gravação não Autorizada** e **Reconhecimento Facial** foram as que apresentaram os menores valores de Kappa (0,461 e 0,437, respectivamente). Em ambas, marcamos de vermelho os ativos que degradam o Kappa das ameaças. No caso da **Gravação não Autorizada**, Nome (ID1), Data de Nascimento (ID4), Ano de Formação (ID17) e Cargo (ID22) foram selecionados como relevantes para a identificação da ameaça. Já para **Reconhecimento Facial**, os ativos foram Nome (ID1), Sexo (ID6), Áudio(s) (ID14), Biografia (ID15) e Ano de Formação (ID17).

5.3 Considerações Finais

Ao abordar as ameaças de RSO, é essencial considerar diversos fatores relacionados à segurança da informação, o que são as ameaças e como ocorrem. O catalogo de ameaça a privacidade demonstra como ela ocorre em cada cenário, e o catalogo de ativos de informação como funciona uma determinada informação na RSO, com o objetivo de conscientizar o usuário uma determinada postagem.

Por fim, a pesquisa também destaca algumas das ameaças à validade que devem ser consideradas ao analisar os resultados de uma pesquisa de opinião como esta. É fundamental abordar essas ameaças com rigor e adotar medidas para garantir a precisão e a confiabilidade dos insights obtidos. Em suma, esta pesquisa oferece uma visão valiosa das percepções dos respondentes.

Apesar das ferramentas utilizadas, para avaliar as ameaças em redes sociais online, como elas ocorrem é fundamental que o usuário tenha conhecimento, para não comprometer a segurança do usuário, o uso das redes sociais potencializa seus efeitos pois a abrangência das RSO é muito grande e vem crescendo a cada ano. Contudo, esses mecanismos de privacidade que existem atualmente por si só não resolvem o problema. A maior vulnerabilidade é o próprio usuário e sua atitude para com a segurança digital. A mudança de atitude passa por educação digital, conscientização e ceticismo.

Capítulo 6

Conclusões

Neste trabalho apresentamos um estudo exploratório, com público geral e especialista em segurança da informação, que correlacionou ameaças a privacidade em RSO com ativos de informação expostos pelos próprios usuários. A avaliação das ameaças de privacidade é essencial para proteger os dados pessoais dos usuários em RSOs.

Nossa avaliação mostrou que o público geral não quer ou não consegue perceber as ameaças a que estão expostos, tendo que não responderam ao questionário sem acessar conteúdos explanatórios sobre o tema e, literalmente, marcaram o que quiseram sem avaliar adequadamente o assunto. Também notamos que os especialistas, embora também não tenho feito uso total do material de apoio, conseguiram, provavelmente graças a sua formação e área profissional, correlacionar de modo mais coerente as ameaças e ativos.

A prova de conceitos revela os resultados dos usuários nas RSOs, seja no **LinkedIn** ou no **X** (antigo Twitter). Os resultados apontaram os riscos dessas ameaças de acordo com a exposição do usuário, seja no perfil ou em uma determinada postagem, de acordo com os ativos. Fica claro o risco da ameaça ocorrer a partir das informações publicadas. A análise demonstrou que usuários que frequentemente compartilham dados sensíveis, como localização, informações pessoais, e detalhes profissionais, estão mais suscetíveis a ataques como cyberstalking, roubo de identidade, gravação não autorizada, entre as demais abordadas nesta pesquisa.

Nossos resultados não são, ainda, os ideais, mas pudemos elaborar uma categorização das ameaças e os ativos relacionados a elas.

Como trabalhos futuros, pretendemos: (i) reaplicar o questionário, em ambos os públicos, mas agora ofertando um treinamento sobre ameaças e ativos; (ii) refatorar a categorização elaborada; (iii) construir um ferramental que nos permita extrair de RSOs os ativos de informação expostos pelos usurários, com o intuito de explicar, na prática, o problema da privacidade e consequentemente a criação de soluções.

6.1 Limitações

Durante a pesquisa houve limitações nas pesquisas dentre ela pode-se destacar:

1. **Formulário de avaliação:** Para uma avaliação consistente sobre ameaças em RSOs foi necessário um formulário de pesquisa, e assim uma quantidade de respondentes para validar seus dados iniciais. Viés de seleção: A seleção dos participantes da pesquisa pode introduzir viés de seleção, especialmente se a amostra não for aleatória ou se houver dificuldade em recrutar participantes diversificados, o que pode afetar a validade externa dos resultados. Disponibilidade

de dados: A pesquisa pode enfrentar desafios relacionados à disponibilidade e acessibilidade dos dados das RSOs, especialmente se houver restrições de privacidade ou políticas de uso de dados que limitem o acesso aos perfis e postagens dos usuários.

2. **Disponibilidade de dados**: limitações ao usar um web crawler em uma pesquisa que envolve redes sociais online. Aqui estão algumas delas: Políticas de Privacidade, Restrições de API e Volume e Velocidade dos Dados

3. **Aspectos Éticos**: A coleta e análise de dados de RSOs podem levantar questões éticas, especialmente em relação à privacidade dos usuários e ao uso responsável dos dados pessoais.

4. **Amostra limitada**: De acordo com a metodologia aplicada, a pesquisa enfrentou limitações relacionadas ao tamanho da amostra, o que pode afetar a representatividade dos resultados e a generalização das conclusões.

5. **Precisão da análise**: A identificação e análise das ameaças nos perfis e postagens dos usuários podem ser subjetivas e suscetíveis a erros de interpretação, de acordo com a interação do usuário, o que pode afetar a confiabilidade e validade dos resultados.

6. **Limitações técnicas**: Restrições técnicas, como a disponibilidade de ferramentas de análise de dados ou capacidade de processamento, limitando a profundidade e abrangência da análise das ameaças nas RSOs.

7. **Complexidade das ameaças**: As ameaças em RSOs podem ser complexas E envolvendo uma variedade de informações, atributos, o que pode dificultou a identificação e classificação das ameaças de forma precisa e abrangente.

6.2 Trabalhos Futuros

Alguns possíveis trabalhos futuros derivados da pesquisa de mestrado em identificação de ameaças em Redes Sociais Online (RSOs), tanto nos perfis quanto nas postagens, incluem:

Desenvolvimento de ferramentas de análise: Projetar e desenvolver ferramentas de análise automatizada para identificar e classificar ameaças de privacidade em perfis e postagens de usuários em RSOs. Isso pode envolver a criação de algoritmos de aprendizado de máquina e técnicas de processamento de linguagem natural.

Avaliação de medidas preventivas: Investigar a eficácia de medidas preventivas, como configurações de privacidade, políticas de plataforma e conscientização dos usuários, na redução da exposição a ameaças de privacidade em RSOs.

linguagem NLP

Análise longitudinal: Realizar estudos longitudinais para acompanhar as tendências e padrões de ameaças de privacidade ao longo do tempo em diferentes plataformas de redes sociais, permitindo uma compreensão mais abrangente das mudanças e evoluções nas ameaças.

Estudos comparativos: Realizar estudos comparativos entre diferentes plataformas de redes sociais para entender como as políticas, práticas e características das plataformas impactam a exposição a ameaças de privacidade e a segurança dos usuários.

Intervenções educacionais: Desenvolver e avaliar intervenções educacionais destinadas a aumentar a conscientização e o conhecimento dos usuários sobre ameaças de privacidade em RSOs, promovendo práticas seguras e protegendo os dados pessoais dos usuários.

Desenvolvimento de Ferramentas de Monitoramento em Tempo Real: Criar soluções que monitoram e alertam os usuários sobre possíveis ameaças em tempo real, e implementações práticas de sistemas de alerta em tempo real.

Esses trabalhos futuros podem contribuir para avançar o conhecimento e as práticas na área de privacidade e segurança em Redes Sociais Online, fornecendo dados valiosos para proteger os

usuários contra ameaças emergentes e promovendo um ambiente online mais seguro e confiável.

Referências Bibliográficas

(2016). Regulamento geral de proteção de dados (gdpr). Acessado em: setembro de 2024.

(2020). Lei geral de proteção de dados pessoais (lgpd). Acessado em: setembro de 2024.

Abid, Y., Imine, A., and Rusinowitch, M. (2018). Online testing of user profile resilience against inference attacks in social networks. In *European Conference on Advances in Databases and Information Systems*, pages 105–117. Springer.

ABNT (2013). Abnt-associação brasileira de normas técnicas. nbr iso/iec 27002 – tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação. *Cabo*.

Aghasian, E., Garg, S., Gao, L., Yu, S., and Montgomery, J. (2017). Scoring users' privacy disclosure across multiple online social networks. *IEEE access*, 5:13118–13130.

Aktypi, A., Nurse, J., and Goldsmith, M. (2017). Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. volume 2017-January, pages 1–11. cited By 6.

Al-Asmari, H. and Saleh, M. (2019a). A conceptual framework for measuring personal privacy risks in facebook online social network. cited By 0.

Al-Asmari, H. A. and Saleh, M. S. (2019b). A conceptual framework for measuring personal privacy risks in facebook online social network. In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pages 1–6. IEEE.

Alemany, J., Del Val, E., Alberola, J. M., and Garćia-Fornes, A. (2019). Metrics for privacy assessment when sharing information in online social networks. *IEEE Access*, 7:143631–143645.

Almogbel, R. S. and Alkhalifah, A. A. (2022). User behavior in social networks toward privacy and trust: Literature review. *International Journal of Interactive Mobile Technologies (iJIM)*, 16(01):pp. 38–51.

Amanatidis, D., Mylona, I., and Dossis, M. (2022). Social media and consumer behaviour: Exploratory factor analysis. In *2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, pages 1–5.

Basili, V. R. and Rombach, H. D. (1988). The tame project: Towards improvement-oriented software environments. *IEEE Transactions on software engineering*, 14(6):758–773.

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., and Pensa, R. (2019). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies*, 12(4):456–469. cited By 1.

Casas, I., Hurtado, J., and Zhu, X. (2015). Social network privacy: Issues and measurement. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9419:488–502. cited By 2.

Cengiz, A. B., Kalem, G., and Boluk, P. S. (2022). The effect of social media user behaviors on security and privacy threats. *IEEE Access*, 10:57674–57684.

Chakraborty, S., Krishna, R., Ding, Y., and Ray, B. (2022). Deep learning based vulnerability detection: Are we there yet? *IEEE Transactions on Software Engineering*, 48(9):3280–3296.

Chatti Iorio, J. (2018). A importância das redes sociais, da internet e das redes sociais online na mobilidade dos estudantes brasileiros do ensino superior para portugal. *Cadernos De Estudos Sociais*, 2(33).

Chen, J., He, J., Cai, L., and Pan, J. (2018). Disclose more and risk less: Privacy preserving online social network data sharing. *IEEE Transactions on Dependable and Secure Computing*, 17(6):1173–1187.

Çoban, Ö., İnan, A., and Özel, S. A. (2020). Privacy risk analysis for facebook users. In *2020 28th Signal Processing and Communications Applications Conference (SIU)*, pages 1–4. IEEE.

das Mercês Silva, S., Matos, G. S., Nascimento, T. A., and Araújo, F. P. O. (2021). Redes sociais como ferramenta de visibilidade das mulheres nas ciências exatas: análise do perfil@ lindasdaengenharia. In *Anais do XV Women in Information Technology*, pages 330–334. SBC.

De, P. and Dey, S. (2017). Security risk assessment in online social networking: A detailed survey. In *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, pages 291–296. IEEE.

De, S. and Imine, A. (2018a). Privacy scoring of social network user profiles through risk analysis. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10694 LNCS:227–243. cited By 0.

De, S. and Imine, A. (2018b). To reveal or not to reveal: Balancing user-centric social benefit and privacy in online social networks. pages 1157–1164. cited By 3.

Demartini, F. and Ciriaco, D. (2024). 62% da população global está nas redes sociais, diz estudo. https://canaltech.com.br/internet/62-da-populacao-global-esta-nas-redes-sociais-diz-estudo-277763/, note = Acesso em 02/02/2024.

Domingo-Ferrer, J. (2010). Rational privacy disclosure in social networks. In *International conference on modeling decisions for artificial intelligence*, pages 255–265. Springer.

Dong, C. and Zhou, B. (2016). Privacy inference analysis on event-based social networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10047 LNCS:421–438. cited By 0.

Fogues, R., Such, J., Espinosa, A., and Garcia-Fornes, A. (2015). Open challenges in relationship-based privacy mechanisms for social network services. *International Journal of Human-Computer Interaction*, 31(5):350–370. cited By 30.

Gundecha, P., Barbier, G., and Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 511–519.

Han, X., Huang, H., and Wang, L. (2019). F-pad: Private attribute disclosure risk estimation in online social networks. *IEEE Transactions on Dependable and Secure Computing*, 16(6):1054–1069.

Jaafor, O. and Birregah, B. (2015). Multi-layered graph-based model for social engineering vulnerability assessment. In *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 1480–1488. IEEE.

Jin, L., Chen, Y., Wang, T., Hui, P., and Vasilakos, A. V. (2013). Understanding user behavior in online social networks: a survey. *IEEE Communications Magazine*, 51(9):144–150.

Joyee De, S. and Imine, A. (2019a). On consent in online social networks: Privacy impacts and research directions (short paper). In *Risks and Security of Internet and Systems: 13th International Conference, CRiSIS 2018, Arcachon, France, October 16–18, 2018, Revised Selected Papers 13*, pages 128–135. Springer.

Joyee De, S. and Imine, A. (2019b). On consent in online social networks: Privacy impacts and research directions (short paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11391 LNCS:128–135. cited By 0.

Kavianpour, S., Ismail, Z., and Mohtasebi, A. (2011). Effectiveness of using integrated algorithm in preserving privacy of social network sites users. *Communications in Computer and Information Science*, 167 CCIS(PART 2):237–249. cited By 0.

Keele, S. et al. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, Ver. 2.3 EBSE Technical Report. EBSE.

Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.

Kumar, H., Jain, S., and Srivastava, R. (2017). Risk analysis of online social networks. pages 846–851. cited By 1.

Laleh, N., Carminati, B., and Ferrari, E. (2015). Graph based local risk estimation in large scale online social networks. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, pages 528–535. IEEE.

Laorden, C., Sanz, B., Alvarez, G., and Bringas, P. G. (2010). A threat model approach to threats and vulnerabilities in on-line social networks. In *Computational Intelligence in Security for Information Systems 2010: Proceedings of the 3rd International Conference on Computational Intelligence in Security for Information Systems (CISIS'10)*, pages 135–142. Springer.

Lima, D. C. (2022). O direito à privacidade: os limites da exposição nas redes sociais e as suas consequências.

Liu, K. and Terzi, E. (2010). A framework for computing the privacy scores of users in online social networks. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 5(1):1–30.

Mahmood, S. (2012). New privacy threats for facebook and twitter users. pages 164–169. cited By 10.

Malhotra, N., Nunan, D., and Birks, D. (2020). *Marketing Research: An Applied Approach*. Pearson, 6 edition.

Marin, E. e. a. (2020). Inductive and deductive reasoning to assist in cyber-attack prediction. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE.

Mican, D., Sitar-Tăut, D.-A., and Mihuț, I.-S. (2020). User behavior on online social networks: Relationships among social activities and satisfaction. *Symmetry*, 12(10).

Nepali, R. K. and Wang, Y. (2013). Sonet: A social network model for privacy monitoring and ranking. In *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, pages 162–166. IEEE.

Petkos, G., Papadopoulos, S., and Kompatsiaris, Y. (2015). Pscore: A framework for enhancing privacy awareness in online social networks. *2015 10th International Conference on Availability, Reliability and Security*, pages 592–600.

Pushkar, P. and Mittal, U. (2022). User behavior analysis based on their social media interaction. In *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, pages 107–110.

Rathore, S., Sharma, P., Loia, V., Jeong, Y.-S., and Park, J. (2017a). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421:43–69. cited By 35.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., and Park, J. H. (2017b). Social network security: Issues, challenges, threats, and solutions. *Inf. Sci.*, 421:43–69.

Rodrigues, Vilela, F. (2022). Ptmol: a suitable approach for modeling privacy threats in online social networks. Acesso em 04/05/2021.

Smith, J. and Brown, J. (2022). Desafios e complexidades nas configurações de privacidade em redes sociais online: Uma avaliação crítica das implicações e soluções. *Cybersecurity and Privacy Journal*, 10(1):1–15.

Sramka, M. (2012). Privacy scores: Assessing privacy risks beyond social networks. *Infocommunications Journal*, 4(4):36–41. cited By 1.

Sramka, M. (2015). Evaluating privacy risks in social networks from the user's perspective. In *Advanced Research in Data Privacy*, pages 251–267. Springer.

Taylor, M., Smith, J., and Brown, J. (2023). Avaliação da eficácia de um novo algoritmo de aprendizado de máquina para detectar e prevenir o uso indevido de dados pessoais em redes sociais. *International Journal of Digital Security and Cybercrime*, 11(1):1–15.

Tucker, R., Tucker, C., and Zheng, J. (2015). Privacy pal: Improving permission safety awareness of third party applications in online social networks. pages 1268–1273. cited By 2.

Wang, Y. and Nepali, R. (2015). Privacy threat modeling framework for online social networks. pages 358–363. cited By 5.

Watanabe, C., Amagasa, T., and Liu, L. (2011). Privacy risks and countermeasures in publishing and mining social network data. pages 55–66. cited By 6.

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer.

Zeng, Y., Sun, Y., Xing, L., and Vokkarane, V. (2014). Trust-aware privacy evaluation in online social networks. In *2014 IEEE International Conference on Communications (ICC)*, pages 932–938. IEEE.

Zeng, Y., Sun, Y., Xing, L., and Vokkarane, V. (2015). A study of online social network privacy via the tape framework. *IEEE Journal on Selected Topics in Signal Processing*, 9(7):1270–1284. cited By 7.