Artigo | *Article*

Ciência da Informação em Revista
ISSN: 2358-0763

Potenciais riscos à privacidade de dados pessoais em Serviços de Redes Sociais Online: uma Revisão Sistemática de Literatura, classificada a partir da Taxonomia da Privacidade

Potential risks to the privacy of personal data in Online Social Network Services: a Systematic Literature Review, classified from the Taxonomy of Privacy

Débora Matni Fonteles
Mestranda em Ciência da Informação
Universidade Federal do Pará, Brasil
dmatnif@gmail.com

Larissa Lima da Silva
Mestra em Ciência da Informação
Universidade Federal do Pará, Brasil
larissasilva@ufpa.br

Amanda Garcia Gomes
Doutoranda em Ciência da Informação
Universidade Federal do Pará, Brasil
garcia.gomes@unesp.br

Fernando de Assis Rodrigues
Doutor em Ciência da Informação
Universidade Federal do Pará, Brasil
fernando@rodrigues.pro.br

Resumo
A opacidade no tratamento de dados pessoais, especialmente, em Serviços de Redes Sociais Online pode desencadear problemas relacionados à privacidade dos indivíduos, pois se trata de espaços que transitam entre o público e o privado. O objetivo da pesquisa consiste em identificar potenciais riscos à privacidade no universo dos Serviços de Redes Sociais Online na literatura científica e classificá-los a partir de uma Taxonomia da Privacidade, demonstrando a relação entre os subgrupos e os assuntos de cada uma das comunicações científicas analisadas. Adotou-se uma Revisão Sistemática de Literatura organizada em fases, de natureza qualitativa e caráter exploratório, a partir da recuperação das comunicações científicas nas bases de dados BRAPCI, SciELO e EBSCOhost. Os resultados apresentaram ocorrências nos subgrupos vigilância, interrogatório, agregação, identificação, insegurança, uso secundário, exclusão, quebra do sigilo, divulgação, exposição, aumento do acesso, chantagem, apropriação, distorção, intromissão e interferência decisional. Conclui-se que a utilização da Taxonomia da Privacidade permitiu a identificação da incidência dos potenciais riscos abordados na literatura.

Palavras-chave: Serviços de Redes Sociais Online; privacidade; dados; Taxonomia da Privacidade.

Abstract
The opacity in the processing of personal data, especially in Online Social Network Services, could trigger problems related to the privacy of individuals, as these are spaces that transit between the public and the private. The objective of the research is to identify in the scientific literature potential risks to privacy in the universe of Online Social Networking Services and classify them based on a Taxonomy of Privacy, demonstrating the relationship between the subgroups and the subjects of each of the analyzed scientific communications. A Systematic Literature Review was adopted, organized in phases, of a qualitative and exploratory nature, based on the recovery of scientific communications in the BRAPCI, SciELO, and EBSCOhost databases. The results showed occurrences in the subgroups surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion, and decisional interference. It concluded that the Taxonomy of Privacy use allowed the identification of the incidence of potential risks addressed in the literature.

Keywords: *Online Social Network Services; privacy; data; Taxonomy of Privacy.*

Submetido em: 04/05/2023
Aceito em: 28/12/2023
Publicado em: 26/01/2024

doi: 10.28998/cirev.2024v11e15480

1 INTRODUÇÃO

O desenvolvimento da Internet e a consolidação de serviços Web, tais como os Serviços de Redes Sociais Online (SRSO), fazem com que as trocas informacionais que ocorrem no ciberespaço transitem entre as esferas pública e privada. O cruzamento destas duas instâncias, ao combinar ferramentas públicas e dados privados, torna complexa a questão da privacidade da informação na Web (Mai, 2016). A troca de informações privadas por meio de dispositivos, provedores e serviços de comunicação ligados à Internet é um possível cenário com risco de perda da privacidade para os indivíduos, quando não oferecem garantias quanto ao bloqueio do acesso de terceiros a dados pessoais (Fogel; Nehmad, 2009; Tufekci, 2008; Zimmer, 2010).

A questão da privacidade de dados pessoais é interdisciplinar, por reunir questionamentos e fenômenos ligados à esfera informacional, jurídica e tecnológica. O fato das etapas de coleta e de armazenamento de dados pessoais serem parte de um Ciclo de Vida de Dados (Sant'Ana, 2016), torna esse fenômeno passível de investigação sob o olhar da Ciência da Informação, ao representar um cenário ligado ao comportamento da informação – que no contexto desta pesquisa se constrói a partir dos dados pessoais dos indivíduos que utilizam os SRSO –, seus fluxos e meios de acesso (Borko, 1968).

O caráter interdisciplinar da privacidade dos dados pessoais em SRSO, que dá origem a comunicações científicas publicadas em distintas áreas do conhecimento, justifica a realização de uma Revisão Sistemática de Literatura (RSL) sobre o tema, ao contribuir com a compreensão sobre os potenciais riscos apontados nas comunicações científicas sobre a privacidade em SRSO.

Como problema de pesquisa, destaca-se que a ausência de uma classificação das comunicações científicas, por meio de uma taxonomia ligada ao contexto da privacidade na Web, dificulta uma percepção sistematizada sobre como pesquisadores compreendem potenciais riscos e consequências à privacidade dos dados pessoais disponíveis em SRSO.

O objetivo da pesquisa consiste em identificar potenciais riscos à privacidade no universo dos SRSO na literatura científica e classificá-los a partir de uma Taxonomia da Privacidade, demonstrando a relação entre os subgrupos e os assuntos de cada uma das comunicações científicas analisadas.

O artigo está estruturado em cinco seções, sendo a primeira seção a introdução. A segunda seção é destinada à apresentação do conceito de privacidade, de dados pessoais, no contexto do SRSO, e da Taxonomia da Privacidade. Na terceira seção, os procedimentos metodológicos aplicados para a RSL são detalhados. Na quarta seção, são apresentados os resultados e discussão, a partir da categorização proposta pela Taxonomia da Privacidade. A quinta seção contém as considerações finais, que sintetizam os resultados da pesquisa e apresentam indicações de pesquisas futuras sobre privacidade de dados pessoais.

2 REFERENCIAL TEÓRICO

A privacidade pode significar a vontade de não ser observado ou vigiado, pode expressar a vontade de manutenção da reputação, do direito de não ser incomodado, ou mesmo pode significar o desejo de ficar só (Warren; Brandeis, 1890; Solove, 2008). A privacidade é compreendida como uma necessidade humana, considerada um direito fundamental para dignidade e formação da personalidade do cidadão, além de essencial ao pleno exercício da cidadania e liberdade (Misugi; Freitas; Efing, 2016). Assim como, o direito à pro-

teção e controle dos dados pessoais (Wang, 2011; Leonardi, 2012). Dados pessoais é qualquer informação que identifique, direta ou indiretamente, um indivíduo em particular, por meio de números identificadores ou por fatores inerentes às suas características físicas, psicológicas, econômicas, culturais ou sociais (European Parliament, 1995). No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) regulamenta o tratamento dos dados pessoais sobre coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, controle da informação, modificação, comunicação, transferência, difusão e extração (Brasil, 2018). A norma brasileira está comprometida com as discussões que visam determinar limitações às intervenções de terceiros no espaço privado dos indivíduos, incluindo os dados pessoais, sobretudo, dos que transitam na Web.

Os SRSO são serviços que promovem o inter-relacionamento dos indivíduos, de grupos e de instituições por meio da construção de perfis públicos e semipúblicos (Boyd; Ellison, 2008; Rodrigues; Sant'Ana, 2018). Uma das características dos SRSO é a coleta de dados (Sant'Ana, 2016) como condição de utilização dos serviços, a atribuição de um identificador único, a possibilidade de compartilhamento de dados com parceiros do serviço ou agentes externos, coleta de dados gerados a partir das atividades online dos indivíduos, como, por exemplo, horários de acesso, localização geográfica, e tipo de conexão de Internet (Rodrigues; Sant'Ana, 2018).

No contexto dos SRSO, o incentivo à publicação de dados pessoais, identificados ou identificáveis, fornecidos regularmente a esses serviços, juntamente a retratos íntimos da vida social de um indivíduo; a visibilidade dos dados pessoais por meio das configurações de privacidade dos SRSO, ou seja, a exposição pública nas relações dos usuários; a organização de grandes quantidades de dados pessoais em coleções para a realização de comércio eletrônico; e o fato de empresas privadas serem as responsáveis pelo desenvolvimento e pela manutenção dos SRSO, são alguns exemplos dos potenciais riscos à privacidade que a interação nestes serviços podem apresentar (Gross; Acquisti, 2005; Mislove, 2007; Rodrigues; Sant'Ana, 2016; Kokolakis, 2017).

Devido ao volume de dados que podem ser coletados pelos SRSO, há a possibilidade de se coletar dados pessoais. Neste sentido, tanto o processo de coleta de dados praticada pelos SRSO, quanto a possibilidade de acesso por terceiros a informações, por meio de perfis públicos, podem contribuir para potenciais riscos à privacidade (Rodrigues; Sant'Ana, 2018).

Os indivíduos utilizam os serviços oferecidos pelos SRSO mediante a concordância das condições descritas no documento denominado de termo de uso. O conteúdo informacional do documento contém a descrição das formas de coleta de dados e de compartilhamento com agentes externos aos SRSO. Nesta concordância das condições de uso, observa-se um problema: a insciência dos indivíduos quanto às sucessivas coletas de dados e à possibilidade de compartilhamento dos conjuntos de dados com empresas parceiras dos SRSO e agentes externos (Doneda, 2012; Rodrigues, 2017; Novo; Azevedo, 2014).

Diante da existência de contextos que ocorrem coletas de dados no ciberespaço, a utilização de uma taxonomia como instrumento de classificação pode contribuir para classificar atividades que podem ser prejudiciais à privacidade dos indivíduos. A Taxonomia da Privacidade visa simplificar o entendimento das atividades que de alguma forma possam prejudicar ou violar a privacidade dos indivíduos. Está dividida em quatro grupos que reúnem 16 subgrupos (cada subgrupo possui uma definição de sua atividade prejudicial), descreve o *modus operandi* e as características da violação, conforme o Quadro 1.

Quadro 1 – Grupos e subgrupos da Taxonomia da Privacidade

Grupo	Subgrupo	Atividades
Coleta de informação	Vigilância	Encadeadas com o propósito de vigiar um indivíduo no seu espaço privado ou em espaço público.
	Interrogatório	De processos de coleta de dados, baseados em interrogatórios e entrevistas.
Processamento de informação	Agregação	Vinculadas ao processo de combinação de dados de múltiplas fontes sobre indivíduos, com o propósito de revelar fatos ocultos, quando analisados separadamente.
	Identificação	A partir do processo de vinculação de dados que permitam a (re)identificação de usuário (e de seus dados pessoais) com suas respectivas pessoas.
	Insegurança	Que não perpassam segurança sobre questões de acesso a dados pessoais aos envolvidos.
	Uso secundário	Que envolvem o uso de dados coletados para um determinado propósito e utilizados a posteriori para outras finalidades.
	Exclusão	Que apresentam opacidade ao indivíduo no processo de armazenamento de dados pessoais, no compartilhamento destes dados a terceiros e na ausência ou na inabilidade de participação nas decisões sobre questões envolvendo a coleta, o armazenamento, o uso e o compartilhamento destes dados.
Disseminação de informação	Quebra de sigilo	Em que ocorrem a quebra de confiança entre as partes em manter a confidencialidade das informações sobre indivíduos.
	Divulgação	De divulgação e de disseminação de informações sobre um indivíduo, que acarretam mudanças na maneira que outros indivíduos julgam seu caráter.
	Exposição	Vinculadas à exposição para terceiros de atributos emocionais ou físicos de intimidade do indivíduo, tais como a nudez, funções corporais e informações de cunho privado.
	Aumento do acesso	Que visam amplificar o acesso a dados pessoais além do previsto ou do combinado entre as partes.
	Chantagem	De controle, de dominação, de intimidação ou de ameaças a pessoas ou grupos, por terceiros.
	Apropriação	Que utilizam dados pessoais de um determinado sujeito em benefício de um terceiro ou para chancelar um serviço ou um produto, sem o pleno consentimento do sujeito.
	Distorção	De disseminação de informações falsas ou interpretadas de maneira dúbia sobre um indivíduo.
Invasão	Intromissão	Com o propósito de realizar incursões em assuntos ou em informações de caráter privado.
	Interferência decisional	De envolvimento do Estado em assuntos de caráter privado, alterando decisões em nome do indivíduo.

Fonte: Elaborado com base em Rodrigues e Sant'Ana (2016).

A distribuição dos 16 subgrupos nos quatro grupos, conforme o Quadro 1, ocorre da seguinte forma: o primeiro grupo trata de riscos à privacidade, provenientes da coleta de informação (subgrupos Vigilância e Interrogatório); o segundo grupo aborda questões ligadas ao processamento das informações (subgrupos Quebra de sigilo, Divulgação, Exposição, Aumento do acesso, Chantagem, Apropriação, Distorção); o terceiro grupo é a disseminação de informações (subgrupos Agregação, Identificação, Insegurança, Uso secundário, Exclusão); e, por fim, o quarto grupo é Invasão (subgrupos Intromissão e Interferência decisional).

3 PROCEDIMENTOS METODOLÓGICOS

Trata-se de uma RSL com adaptações do modelo de Conforto, Amaral e Silva (2011), de natureza qualitativa e caráter exploratório, o protocolo está organizado em três fases. Cada fase possui etapas detalhadas no Quadro 2. Foram utilizadas como materiais de apoio à RSL: Tesauros, Plataforma Sucupira, Google G-Suite, computador com acesso à Internet e gerenciador de referências bibliográficas Zotero.

Quadro 2 – Detalhamento das Fases e Etapas da Revisão Sistemática de Literatura

Fase	Etapa		
	Nº	Objetivo	Detalhamento
Entrada	1	Definir as atividades iniciais da RSL alinhadas ao objetivo da pesquisa	Foram identificadas pesquisas sobre potenciais riscos à privacidade no contexto dos SRSO na literatura científica.
	2	Definir as bases	As bases de dados selecionadas foram: a Base de Dados em Ciência da Informação (BRAPCI), a Scientific Electronic Library Online (SCIELO) e a EBSCOhost.
	3	Definir os critérios de inclusão e de exclusão	Foram definidos os seguintes critérios de inclusão: 1. artigos científicos em periódicos e anais em congressos; 2. apenas os que estiverem em texto completo; 3. idioma português; 4. artigos que contenham em suas palavras-chave, resumo ou introdução os termos “Redes sociais ou Redes Sociais Online ou Redes Sociais On-line ou Mídias sociais” além de privacidade.
			Foram definidos os seguintes critérios de exclusão: 1. idioma estrangeiro; 2. artigos sem aderência com o tema investigado.
	4	Estabelecer os critérios de qualidade	Foram utilizados apenas os artigos indexados estratos Qualis igual ou superior a B2.
	5	Estabelecer os filtros disponíveis nas bases	Foram utilizados como filtros: título; resumo e palavras-chave.
Processamento	1	Realizar as buscas das comunicações científicas nas bases	Foram utilizados as *strings* Redes Sociais e suas variações. Redes Sociais e a combinação com o termo privacidade, acrescentando-se às *strings* o termo booleano AND.
	2	Registrar dados e metadados	Os metadados registrados em planilha eletrônica foram: autoria, título do artigo ou dos anais de congresso, título do periódico, palavras-chave, resumo e quantidade de citações.
	3	Realizar a leitura e análise	Foram realizadas leituras técnicas a partir de título, resumo, palavras-chave, introdução e considerações finais; e, quando necessário, do texto completo.
Saída	1	Cadastrar e arquivar as comunicações científicas	Os textos completos das comunicações científicas foram cadastrados e arquivados no formato *Portable Document Format* (PDF) no gerenciador de referências Zotero.
	2	Sintetizar os estudos analisados	Uma síntese das pesquisas selecionadas foi produzida.
	3	Formular os resultados	Os resultados acerca dos SRSO e os potenciais riscos identificados e analisados nesta investigação foram formulados.

Fonte: Elaborado pelos autores (2023).

A fase de Entrada é composta por cinco etapas e refere-se à utilização de estratégias com o propósito de recuperar o quantitativo de comunicações científicas analisadas.

Primeiramente definiram-se as atividades iniciais da RSL alinhadas ao objetivo da pesquisa. Em seguida, foram selecionadas as bases para coleta: Base de Dados em Ciência da Informação (BRAPCI), Scientific Electronic Library Online (SCIELO) e EBSCO Information Services.

Posteriormente, definiram-se os critérios de inclusão e de exclusão: artigos de periódicos e os anais de congressos, os que estiverem em texto completo, em idioma da língua portuguesa e artigos que contenham em suas palavras-chave, resumo ou introdução os termos "Redes sociais ou Redes Sociais Online ou Redes Sociais On-line ou Mídias sociais" além de privacidade. Foi estabelecido como critério de qualidade utilizar apenas os artigos indexados nos estratos Qualis[1] igual ou superior a B2. Por fim, foram estabelecidos os filtros disponíveis nas bases sendo: título, resumo e palavras-chave.

A fase de Processamento possui três etapas e compreende a execução das buscas nas bases. Para isso, foram utilizadas as *strings* de busca: Redes Sociais e suas variações, Redes Sociais e a combinação com o termo privacidade, acrescentando-se às *strings* o termo booleano AND. Posteriormente, foram registrados em planilha os dados e metadados de artigos e anais de congressos, sendo: autoria, título do artigo ou dos anais de congresso, título do periódico, palavras-chave, resumo, quantidade de citações, *hyperlink* para o acesso ao texto completo, base de conhecimento e o estrato Qualis dos periódicos. Por fim, realizou-se o processo de leitura e análise dos artigos de periódicos e anais de congressos selecionados.

A última fase é a Saída composta por três etapas e compreende a organização dos artigos. Assim se realizou o cadastro e arquivamento dos artigos de periódicos e dos anais de congressos. Posteriormente, os arquivos em *Portable Document Format* (PDF) foram armazenados no *software* Zotero. Por fim, produziu-se a síntese a partir dos estudos analisados. Por fim, formularam-se os resultados acerca dos SRSO e os potenciais riscos identificados e analisados nesta investigação.

4 RESULTADOS E DISCUSSÃO

A busca por comunicações científicas sobre SRSO e a privacidade em três bases, a BRAPCI, a SciELO e a EBSCOhost, resultou em um quantitativo de 331 comunicações científicas, sendo descartadas 311. Obteve-se uma amostra de 20 comunicações científicas para a análise. Registra-se que na amostra de comunicações científicas não houve casos de duplicidade, ou seja, um mesmo documento não foi identificado em diferentes bases de conhecimento. A realização das buscas compreendeu o período entre 10 de novembro de 2021 a 13 de dezembro de 2021.

As comunicações científicas foram classificadas nos subgrupos da Taxonomia da Privacidade, onde foram consideradas as discussões apresentadas pelos autores e a relação com o potencial risco à privacidade descrito no subgrupo. A apresentação dos resultados e a discussão segue a ordem de organização dos quatro grupos (Coleta, Processamento, Disseminação e Invasão) e os respectivos 16 subgrupos. No Quadro 3 (Apêndice A), é apresentada uma síntese dos resultados encontrados nesta seção.

[1] Na ocasião da pesquisa, a última classificação dos estratos dos periódicos em vigor era a do quadriênio 2013 - 2016. Foram considerados para análise dos artigos indexados em periódicos com estrato Qualis igual ou superior a B2 (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, c2021).

4.1. Grupo I: Coleta de informação (subgrupos: Vigilância e Interrogatório)

O subgrupo Vigilância é conceituado como o ato de monitorar indivíduos ou instituições em espaços privados e públicos (Rodrigues; Sant'Ana, 2016). Neste subgrupo, foram classificadas comunicações científicas que apresentaram relações entre os SRSO e as ações de vigilância. Observou-se que estão divididas em dois grupos: a) relacionado a ações de vigilância que podem ser realizadas por meio das ferramentas do serviço (Rosado; Tomé, 2015; Fugazza; Saldanha, 2018; Barriga, 2020; Leitzke; Rigo, 2020) e b) possíveis implicações a partir do uso dos serviços que possibilitam ações de vigilância (Assumpção; Sant'Ana; Santos, 2015; Streck; Pellanda, 2017; Lima, 2018; Barriga, 2020).

No primeiro grupo, que inclui as ações que podem ser realizadas através das ferramentas dos serviços, foi identificada uma comunicação científica que compara os SRSO como um novo modelo de vigilância com potencial risco à privacidade, pois ocorre em ambientes digitais e permitem a criação de multiperfis, acesso por dispositivos móveis e tecnológicos, além do uso simultâneo de outros SRSO (Rosado; Tomé, 2015). Essas características possibilitam monitorar um indivíduo em espaços públicos ou privados, pois a disponibilidade para o uso dos serviços, aliado a permissões concedidas pelo indivíduo contribui para a ausência de percepção sobre o monitoramento das atividades realizadas nesses ambientes.

O monitoramento das atividades dos indivíduos em ambientes digitais, como os SRSO, por meio das ferramentas do serviço é similar ao panóptico[2], pois é possível observar e monitorar as atividades dos indivíduos pelos serviços sem ter conhecimento de quem está por trás do gerenciamento dos fluxos de dados (Fugazza; Saldanha, 2018; Barriga, 2020; Leitzke; Rigo, 2020). Destaca-se que as ações de vigilância podem ser passíveis de realização pelo detentor dos SRSO (*e.g.* tem acesso aos dados diretamente) e por outros indivíduos que os utilizam (*e.g*. *cyberstalker*[3]) (Fugazza; Saldanha, 2018). Por outro lado, atribui-se aos detentores de SRSO a adoção de estratégias para incentivar a interação entre os indivíduos, com a oferta de ferramentas dos serviços (*e.g.* salas de bate-papo, murais, notícias sobre eventos, mensagens instantâneas e publicação de vídeos) ampliando assim as ocasiões e as oportunidades de monitorar as atividades dos indivíduos (Barriga, 2020). Leitzke e Rigo (2020) discutem o panóptico na perspectiva da propagação de discursos e opiniões, viabilizados pelas ferramentas dos serviços, divulgados como verdades inquestionáveis de um grupo majoritário sobre um minoritário, na tentativa do estabelecimento de relações de poder, decorrente do processo de vigilância como forma de se exercer controle.

Foram apontados como possíveis problemas geracionais a relação entre Tecnologias de Informação e Comunicação (TIC), vigilância e coleta de dados (Hage; Kublikowski, 2019; Mendes-Campos; Féres-Carneiro; Magalhães, 2020). Refletem que pode existir uma relação entre esses elementos, sendo um problema geracional que impacta na percepção de privacidade quando os indivíduos utilizam as ferramentas do SRSO para interação (Hage; Kublikowski, 2019). Experiências vivenciadas pelos indivíduos que usaram TIC antes e após a consolidação da Internet, sobretudo, com o crescimento de SRSO, podem apresentar

[2] Panóptico é um termo utilizado para designar uma penitenciária ideal que permite a um único vigilante observar todos os prisioneiros, sem que estes possam saber se estão ou não sendo observados.

[3] Termo inglês, associado à prática da importunação, perseguição resultante de ações de vigilância de forma constante, seja em meio físico ou online, com a intenção de identificar dados e informações decorrentes, por exemplo, do uso de um SRSO. ALMEIDA, V. O que é stalkear e como denunciar stalking? **Olhar Digital**, 14 jul. 2022. Disponível em: https://olhardigital.com.br/2022/07/14/tira-duvidas/o-que-e-stalkear-e-como-denunciar-stalking. Acesso em: 13 abr. 2023.

percepções diferentes sobre ambientes seguros e o fornecimento de dados (Mendes-Campos; Féres-Carneiro; Magalhães, 2020), ocasionando a diminuição da percepção de coleta de dados que pode contribuir para ações de vigilância.

As ferramentas dos SRSO são oferecidas e estimuladas para interação entre os indivíduos e podem desencadear ações de vigilância por outros indivíduos ou por agentes externos (Fugazza; Saldanha, 2018; Barriga, 2020). Há um entendimento de que é possível a realização de ações de vigilância entre indivíduos e agentes externos nesses serviços, incluindo, no caso dos agentes externos, a vigilância de entes públicos, representando um potencial risco à privacidade quando é possível verificar as atividades realizadas no SRSO e externo ao serviço.

No segundo grupo, de possíveis implicações a partir do uso dos serviços que possibilitam ações de vigilância, as comunicações científicas analisadas apontaram ser possível identificar potenciais riscos à privacidade a partir do uso dos SRSO. A associação da Internet e o uso de dispositivos móveis atua como meio facilitador de acesso aos SRSO (Assumpção; Santana; Santos, 2015; Streck; Pellanda, 2017; Lima, 2018; Barriga, 2020). A variedade de dispositivos tecnológicos (*e.g. smartphones* e computadores pessoais) são meios com os quais o indivíduo pode realizar o acesso em SRSO. Esta facilidade no acesso intensificou o uso destes serviços pelos indivíduos, resultando na produção de expressivos volumes de dados e de metadados que podem ser utilizados para monitorar os espaços público e privado (Assumpção; Santana; Santos, 2015). Os dispositivos móveis possuem a função de captura de imagens de fácil utilização, produzidas com câmeras embarcadas no *hardware*, tornando o registro e o envio de imagens fluido e fácil para SRSO (em poucos passos) (Streck; Pellanda, 2017). A variedade de dispositivos tecnológicos associado ao uso intensivo da Internet têm impacto na velocidade com que os indivíduos acessam SRSO, e, por conseguinte, na produção e no aumento do volume de dados e de metadados, desencadeando possíveis ações de vigilância pelos detentores de SRSO e por agentes externos (Streck; Pellanda, 2017).

Foi identificado ainda uma comunicação científica sobre o Instagram, que apresentou possíveis implicações quanto ao uso, com estímulo à produção de dados de forma instantânea (Streck; Pellanda, 2017). No Instagram, os conteúdos são predominantemente de imagens e vídeos compostos por dados e metadados, que podem conter conjuntos de dados sensíveis e pessoais. O efeito do estímulo na produção instantânea é a coleta de dados e a possibilidade de obtenção de novas informações (Streck; Pellanda, 2017). A relação entre a composição dos conjuntos de dados e o estímulo à publicação de imagens feito pelo serviço podem contribuir para a obtenção de dados com a finalidade de monitoramento no espaço público ou privado (ocasião de ações pertinentes ao subgrupo Vigilância).

O uso de SRSO está intimamente vinculado ao constante preenchimento de formulários, obrigatórios e opcionais. O subgrupo Interrogatório reúne atividades com processos de coleta de dados, baseados em interrogatórios e entrevistas (Rodrigues; Sant'Ana, 2016). No caso dos SRSO, os dados são solicitados e fornecidos no momento do preenchimento de formulários de edição de perfil, no preenchimento de informações adicionais a um recurso audiovisual, entre outros (Boyd; Ellison, 2007; Rodrigues; Sant'Ana, 2016).

Neste subgrupo, foi classificado uma comunicação científica que apresentou potenciais riscos à privacidade no preenchimento obrigatório de formulários, no qual os dados informados incluem nome, sobrenome, idade, gênero, data de nascimento, número

do Cadastro de Pessoa Física (CPF) e telefone (Sá, 2018). Essa condição obrigatória de registro de dados informados se configura como um potencial risco à privacidade, pois os dados pessoais coletados podem ser armazenados em banco de dados e, conforme o descrito na política de privacidade, podem ser compartilhados com terceiros (Lima, 2018; Sá, 2018).

4.2 Grupo II: Processamento de informação (subgrupos: Agregação, Identificação, Insegurança, Uso secundário e Exclusão)

O subgrupo Agregação reúne atividades relacionadas ao processo de combinação de dados originados de múltiplas fontes sobre indivíduos, com o propósito de revelar fatos ocultos (Rodrigues; Sant'Ana, 2016). Foram classificadas comunicações científicas que apresentaram a existência de múltiplas fontes geradoras de dados e a contribuição de dispositivos móveis para gerar metadados como a localização da captura de uma imagem como potenciais riscos à privacidade (Jurno; D'Andréa, 2017; Streck; Pellanda, 2017; Rosado; Tomé, 2015; Assumpção; Sant'Ana; Santos, 2015).

A possibilidade de acesso a múltiplas fontes geradoras de dados sobre indivíduos pode contribuir para combiná-los e reuni-los em banco de dados com o intuito de possibilitar novas percepções, não disponíveis quando analisadas individualmente (Rosado; Tomé, 2015; Jurno; D'Andréa, 2017; Streck; Pellanda, 2017). Uma das fontes geradoras de dados é a própria utilização dos SRSO, por meio das ferramentas do serviço, como, por exemplo, o envio de uma imagem e a publicação pelo SRSO (data e horário), o compartilhamento de um conteúdo no serviço (perfis relacionados), a atribuição de *hashtags* (específicas ou gerais) nos conteúdos veiculados nesse ambiente. As curtidas e os comentários, quando associados a outros dados, podem apresentar afinidades a assuntos, tais como política e religião (Jurno; D'Andréa, 2017).

Entre os serviços oferecidos existe a possibilidade de enviar uma imagem e o SRSO realizar a publicação. Neste processo estão incluídos os metadados sobre o local e a data da captura da imagem (Streck; Pellanda, 2017). A partir da publicação, os metadados gerados podem ser utilizados para combinar com outros dados, como, por exemplo, dados de localização de um estabelecimento próximo, localização fornecida pelo dispositivo móvel e dados da rede de conexão pela qual foi enviada a imagem, assim reunindo dados de múltiplas fontes (Assumpção; Sant'Ana; Santos, 2015).

O subgrupo Identificação congrega atividades que a vinculação de dados permite a (re)identificação de indivíduos (Rodrigues; Sant'Ana, 2016). As comunicações científicas classificadas apresentaram discussões que envolvem os dados identificáveis por meio de imagens e uso de técnicas de identificação de dados por SRSO.

O envio de imagens e a publicação por SRSO podem conter dados passíveis de identificação (Martorell; Nascimento; Garrafa, 2016). A exposição de imagens em centros cirúrgicos ou em consultórios podem conter dados que permitam a (re)identificação dos indivíduos, caso sejam reunidos com outros dados, como, por exemplo, o nome de perfil, o número de telefone, o endereço domiciliar aproximado ou fotografias de outras fontes de informação (Martorell; Nascimento; Garrafa, 2016). Quanto ao uso de técnicas de (re)identificação de dados em SRSO, as comunicações científicas apontam preocupações com o reconhecimento facial (Martorell; Nascimento; Garrafa, 2016; Assumpção; Sant'Ana; Santos, 2015). O reconhecimento facial é uma forma de identificação de dados realizada por meio de análise de imagem, ainda que um indivíduo tenha enviado uma imagem ao SRSO

contendo parte do rosto, existe a possibilidade de conter dados suficientes para identificar características que combinadas a outras fontes de informação, permitem identificá-lo em diversos serviços online (Assumpção; Sant'Ana; Santos, 2015), característica do subgrupo Identificação.

As atividades que coletam dados e não dão visibilidade aos processos de segurança sobre questões de acesso a dados pessoais aos envolvidos são características do subgrupo Insegurança (Rodrigues; Sant'Ana, 2016). Neste subgrupo, foram classificados comunicações científicas que apresentaram como potenciais riscos à privacidade, discussões sobre SRSO como ambientes públicos podem estar sujeitos às implicações da visibilidade e acesso a dados por terceiros de forma não autorizada, acesso a dados por agentes externos e indivíduos usuários do SRSO, e a opacidade na transparência sobre o que é realizado com os dados a partir da Política de Privacidade (Assumpção; Sant'Ana; Santos, 2015; Rebs, 2017; Fugazza; Saldanha, 2018; Borges, 2020).

Os SRSO são constituídos como ambientes públicos, mas podem ser percebidos pelos indivíduos que os utilizam como ambiente privado, no qual esta dificuldade de percepção pode representar um potencial risco à privacidade (Assumpção; Sant'Ana; Santos, 2015; Rebs, 2017). O envio de dados pessoais e a coleta de dados sobre a utilização que o indivíduo realiza nos serviços podem ser coletados por agentes externos, via *Application Programming Interface* ou por técnicas como a raspagem de dados. Entretanto, os serviços não descrevem limitações ou quais dados estão sujeitos à proteção nas Políticas de Privacidade, configurando como elemento de opacidade entre instituição e indivíduos (Assumpção; Sant'Ana; Santos, 2015). A visibilidade e o acesso aos conteúdos enviados aos SRSO podem ser recuperados por outros indivíduos externos à rede de contatos do perfil, por exemplo, o anonimato por criação de perfil falso para raspagem de dados (Rebs, 2017), caracterizando uma situação de insegurança.

A Política de Privacidade é um documento que descreve a forma de utilização dos dados coletados, porém, seu conteúdo documental pode gerar insegurança sobre os limites do processamento dos dados em outros contextos (Fugazza; Saldanha, 2018; Borges, 2020). A permissão dada às instituições para o acesso a dados ocorre quando os indivíduos aceitam as condições descritas nos termos de uso, no qual as detentoras de SRSO se utilizam dessa condição de proprietária dos dados para realizar de forma deliberada o acesso e a coleta de dados, gerando falta de entendimento pelos indivíduos sobre o que de fato é realizado. Para Borges (2020), um dos aspectos que podem causar insegurança em SRSO é o *modus operandi* e a Política de Privacidade. Por exemplo, no caso do Facebook esta situação é referente a uma de suas cláusulas, a modificação unilateral. O impasse sobre este tema é que indivíduos estão automaticamente concordando com a cláusula quando realizam um registro no serviço, o que faz com que o Meta Platforms Inc. altere a qualquer tempo o conteúdo do termo (modificação unilateral), cabendo ao indivíduo concordar para continuar utilizando os serviços.

O subgrupo Uso secundário está relacionado a ações de coleta de dados que possuem sua finalidade original alterada, direcionado a utilização dos dados para outros propósitos (Rodrigues; Sant'Ana, 2016). Foram classificadas comunicações científicas relacionadas à possibilidade de elaboração de diários completos sobre um indivíduo que podem ser utilizados para fins diferentes da proposta inicial apresentada pelo SRSO e a personalização de perfis como estratégia de *marketing* adotada por empresas, que visa identificar preferências e interesses dos indivíduos a partir dos dados coletados (Zakiee; Hage; Kublikowski, 2019; Fugazza; Saldanha, 2018; Borges, 2020).

A formação de diários completos sobre um indivíduo, como os produzidos no Instagram, podem ser utilizados para fins diferentes da proposta inicial do SRSO, gerando uma sensação de segurança aos usuários sobre os seus dados (Zakiee; Hage; Kublikowski, 2019). Todavia, os dados de indivíduos podem ser utilizados para ações de *marketing* direcionado (ou personalizado) de conteúdos políticos e ideológicos, e estes podem ser considerados como uso secundário de dados, uma vez que a obtenção dos dados pelo SRSO, conforme a política de privacidade, são para direcionar o consumo de produtos e serviços (Borges, 2020; Jurno, D'Andréa, 2017; Fugazza; Saldanha, 2018). Os perfis dos indivíduos reúnem suas preferências, e essa dinâmica é instrumentalizada pelos dados fornecidos, de modo que seja possível direcionar produtos e serviços que indivíduos em SRSO são mais propensos a adquirir. Por exemplo, os dados reunidos a partir da ação dos algoritmos são processados e transformados em informações sobre os indivíduos, sendo compartilhadas e até comercializadas com outras empresas (Jurno; D'Andréa, 2017), caracterizando o subgrupo Uso secundário.

O subgrupo Exclusão trata de questões ligadas às atividades exercidas sem transparência ao indivíduo no que se refere aos processos de armazenamento de dados pessoais, no compartilhamento desses dados a terceiros, e na ausência ou na falta de capacidade de participação nas decisões sobre questões ligadas aos seus dados (Rodrigues; Sant'Ana, 2016).

A exclusão da participação na decisão de compartilhar dados pode ocorrer entre indivíduos que utilizam SRSO, foram caracterizadas como ações exercidas sem transparência o uso de dados de pacientes sendo compartilhados com outros indivíduos em SRSO (Martorell; Nascimento; Garrafa, 2016). Quando se trata de informações entre profissionais da saúde e pacientes, o compartilhamento de dados, ainda que com fins informativos, devem ser precedidos de permissão conforme as normas dos conselhos federais da área da saúde. Os dados dos pacientes quando utilizados e compartilhados sem a participação de decisão destes pode caracterizar uma ação de exclusão.

Casos de recompartilhamento de publicações ou de compartilhamento em cadeia (*e.g.* o compartilhamento do compartilhamento de uma publicação) podem ser caracterizadas também como exclusão (Amaral Filho; Blanco, 2014; Borges, 2020; Gonzatti; Bittencourt; Esmitiz, 2015; Santos; Porto; Alturas, 2010). Ao enviar um conteúdo para o serviço e disponibilizar para uma lista restrita de perfis, ainda é possível que o conteúdo seja recompartilhado a terceiros por um perfil incluído na lista (compartilhamento do compartilhamento), isso representa que o indivíduo foi excluído da decisão de permitir esta ação.

A possibilidade de cópias dos dados armazenados pelos detentores do serviço é outro fator que contribui para a exclusão. O indivíduo é excluído do processo decisório sobre a replicabilidade em outras bases sob a guarda de terceiros, de agentes externos, inclusive transferindo seus dados para outros países. Uma publicação com imagem em uma página, pode ser armazenada como cópia em outros bancos de dados diferentes dos SRSO, como as *Content Delivery Network* (CDN) (Assumpção; Santana; Santos, 2015; Jurno; D'Andréa; 2017; Streck; Pellanda, 2017). Assim, a atividade de exclusão está relacionada ao uso indevido de dados, associada à ausência de autorização formal pelo indivíduo para uso e compartilhamento de dados por profissionais de qualquer atividade profissional ou por qualquer outro indivíduo.

4.3 Grupo III: Disseminação de informação (subgrupos: Quebra do sigilo, Divulgação, Exposição, Aumento do acesso, Chantagem, Apropriação e Distorção)

O subgrupo Quebra do sigilo consiste em atividades que ocorrem a quebra de confiança entre as partes em manter a confidencialidade das informações sobre indivíduos. Trata-se da ruptura de confiança de uma das partes envolvidas na manutenção da privacidade (Rodrigues; Sant'Ana, 2016). Foram classificados neste subgrupo comunicações científicas que apresentaram discussões sobre a utilização de imagens de procedimentos estéticos em pacientes e elementos disponíveis para a proteção de dados de visualização identificadas nos SRSO (Martorell; Nascimento; Garrafa, 2016; Santos; Porto; Alturas, 2010; Assumpção; Sant'Ana; Santos, 2015).

As publicações realizadas pelos perfis de profissionais de saúde podem ser utilizadas como meio de promoção de suas atividades. Considerou-se como uso inadequado de imagens de pacientes que ocorreram de forma indevida e não autorizada. O uso destas imagens poderia desencadear implicações para a privacidade dos pacientes, como a ridicularização ou o julgamento, mesmo quando a intenção do publicador seja de publicizar seu serviço (Martorell; Nascimento; Garrafa, 2016). A quebra do sigilo dentro do SRSO foi caracterizada porque houve confiança entre as partes para a captura da imagem (fora do serviço), porém, a publicação no SRSO pode apresentar risco à privacidade do sujeito retratado na imagem por se tratar de um contexto da saúde e de caráter privado.

No envio de um conteúdo e na publicação pelo SRSO podem ser realizados ajustes de configuração sobre quem poderá visualizar a publicação, como mecanismo de proteção sobre o acesso ao conteúdo. Entretanto, alguns serviços permitem a possibilidade de outros indivíduos participantes da rede realizarem um novo recompartilhamento, podendo ser contrário ao primeiro ajuste e caracterizando uma ação no subgrupo Quebra de sigilo (Santos; Porto; Alturas, 2010; Assumpção; Sant'Ana; Santos, 2015).

A disseminação de informações sobre um indivíduo gera mudanças na maneira que outros indivíduos julgam seu caráter, atividade do subgrupo Divulgação (Rodrigues; Sant'Ana, 2016). Foi classificado neste subgrupo uma comunicação científica que apresenta discussões sobre o termo extimidade, que se refere à capacidade de expor a intimidade em ambientes digitais, principalmente, em SRSO (Mendes-Campos; Féres-Carneiro; Magalhães, 2020). O entendimento de privacidade como algo relacionado ao espaço físico foi alterado devido às TIC, pois serviços baseados em tecnologias que diminuem a percepção de que SRSO são espaços públicos e que existe a capacidade de reunir dados sobre os indivíduos. Aliado ao estímulo de realizar publicações em SRSO, os indivíduos produzem dados por meio das publicações, como, por exemplo, o envio de imagens e vídeos, os comentários e as reações (Mendes-Campos; Féres-Carneiro; Magalhães, 2020).

Neste sentido, quando são publicados dados pessoais ou fatos íntimos dos indivíduos existe um potencial risco à privacidade, por exemplo, a discussão entre um casal, a imagem em locais que podem ser socialmente reprováveis à sua comunidade e um resultado de teste. Especialmente nas publicações realizadas por mulheres existe maior possibilidade de desencadear ações de perseguições que provocam constrangimento ou a restrição da liberdade (Mendes-Campos; Féres-Carneiro; Magalhães, 2020). Além disso, é possível a distorção da publicação, por meio de alterações em imagens e textos, ocasionando mudanças na forma que outros indivíduos julgam seu caráter, caracterizando o subgrupo Divulgação.

O subgrupo Exposição concentra atividades em que ocorre a exposição para terceiros de atributos emocionais ou físicos de intimidade do indivíduo como nudez, funções corporais e informações privadas (Rodrigues; Sant'Ana, 2016). Foram classificados neste subgrupo as comunicações científicas relacionadas à facilidade de utilização dos SRSO como uma das formas de contribuir para exposição de dados, a exposição de dados de pacientes na área da saúde, a exposição dados financeiros quando não adotada medidas de proteção e a exposição de características físicas dos indivíduos em SRSO (Zakiee; Hage; Kublikowski, 2019; Martorell; Nascimento; Garrafa, 2016; Purim; Tizzot, 2019; Everton, *et al.*, 2014; Rebs, 2017).

Os SRSO estimulam os indivíduos a expor momentos do cotidiano, sobretudo entre indivíduos nascidos após a consolidação da Internet e de dispositivos móveis (Zakiee; Hage; Kublikowski, 2019). Estes estímulos têm como objetivo a publicação de experiências positivas para outros indivíduos utilizando as ferramentas disponibilizadas pelo SRSO. As publicações que ocorrem por imagens, vídeos e áudios podem trazer como consequência a diminuição da percepção de possíveis riscos de exposição para terceiros sobre atributos pessoais (Zakiee; Hage; Kublikowski, 2019).

A ausência de proteção dos dados sensíveis relacionados à saúde do indivíduo pode levar à exposição de informações de cunho privado a terceiros. A utilização de dados sigilosos para a promoção de atividades profissionais deve ser precedida de autorização formal dos pacientes, ainda que seja utilizado para fins de pesquisa e atividades profissionais, os dados sensíveis devem ser anonimizados (Martorell; Nascimento; Garrafa, 2016; Purim; Tizzot, 2019).

Os dados financeiros são de cunho privado, sendo restrito ao próprio indivíduo ou à instituição para qual forneceu os dados. A exposição de dados em SRSO que coletam dados financeiros para realização de compras pode ter potencial de desencadear atividades prejudiciais ao indivíduo como a ocorrência de fraudes e golpes, sendo imprescindível a proteção (Everton, *et al*., 2014).

A exposição de conteúdos pessoais para terceiros em SRSO também pode desencadear a propagação de discurso de ódio. A publicação feita por um indivíduo pode receber comentários desrespeitosos por meio do anonimato com a criação de perfis falsos (Rebs, 2017). Nesse sentido, a exposição de imagens por usuários poderá estar sujeita a práticas criminosas por terceiros, como, por exemplo, um caso de racismo ocorrido no Facebook com uma atriz brasileira explorado na literatura analisada (Rebs, 2017).

O subgrupo Aumento do acesso são atividades que buscam amplificar o acesso a dados pessoais além do previsto ou do combinado entre as partes (Rodrigues; Sant'Ana, 2016). Foram classificadas neste subgrupo comunicações científicas que apresentaram como potenciais riscos à privacidade a ausência de preocupação dos usuários em relação à coleta de dados feita pelos SRSO e a descrição nos termos de uso dos SRSO sobre os processos de utilização dos dados coletados (Sá, 2018; Fugazza; Saldanha, 2018; Borges, 2020; Barriga, 2020).

Na pesquisa realizada por Sá (2018), a prática de covisualização (televisão social) dos conteúdos audiovisuais em SRSO é recente. O fenômeno pode ser observado na interação dos indivíduos com outros indivíduos por meio de dispositivos tecnológicos, no qual esta interação deixa rastros, como a exigência de fornecimento de metadados como critério para acesso aos SRSO (*e.g.* endereço de e-mail, nome e CPF). A ausência de preocupação dos indivíduos sobre a privacidade e o fornecimento de dados pode estar relacionada ao volume informacional dos termos de uso dos SRSO (Sá, 2018). Sá (2018) também apresenta

preocupações sobre os rastros deixados nesses serviços e a possibilidade de ampliar o acesso além do previsto, uma vez que os termos de uso não apresentam de forma transparente as limitações sobre os acessos por outros usuários ou terceiros, caracterizando o subgrupo Aumento do acesso.

Fugazza e Saldanha (2018) apresentam preocupações com o conteúdo informacional dos termos de uso, sob a ética da informação em SRSO. A descrição nos termos de uso dos SRSO sobre os processos de utilização dos dados coletados se distancia da transparência sobre o que é realizado com os dados, existindo a possibilidade de amplificar o acesso a dados a terceiros, a agentes externos, armazenamento dos dados em outros países e entre os usuários dos serviços (Fugazza; Saldanha, 2018). A ausência de transparência sobre o que pode ser realizado com os dados coletados, por meio da permissão via termo de uso e o compartilhamento com as conexões, podem ser atividades caracterizadas no subgrupo Aumento do acesso.

A utilização dos dados coletados, via permissão dos termos de uso pelos SRSO, é uma das principais formas de subsistência das instituições (Fugazza; Saldanha, 2018; Borges, 2020). É necessária a reflexão ética sobre o propósito de uso dos dados para o *marketing* e a utilização de algoritmos pelos serviços para a monetização (processo de captação de recurso financeiro de um serviço oferecido sem inscrição ou mensalidade pelo seu uso), pois existem implicações à privacidade dos indivíduos. Ambientes que coletam dados devem apresentar condições que permitam aos indivíduos conhecer para qual finalidade e como estão sendo utilizados os dados obtidos, contribuindo para a transparência (Fugazza; Saldanha, 2018).

Fatores como a identificação de públicos para direcionar anunciantes e apontar preferências a partir do volume de dados gerado pelos indivíduos no SRSO, inexistência de limitações quanto à quantidade de dados coletados e modificação unilateral das cláusulas do termo de uso são condições que podem ser realizadas a critério dos detentores do serviço (Borges, 2020). A ausência de transparência sobre o processamento dos dados e funcionamento dos algoritmos contribuem para potenciais atividades que podem ampliar o acesso a dados além do previsto entre as partes, caracterizando o subgrupo Aumento do acesso.

No contexto do debate político, os SRSO aparecem como uma das formas de comunicação de partidos políticos e a ampliação do acesso aos dados dos indivíduos apresenta preocupações para privacidade (Barriga, 2020). A relação entre dados dos indivíduos e a sua apropriação pelos SRSO poderia contribuir para ações de vigilância pelo Estado, ao serem veiculados nesses serviços publicações realizadas pelos políticos nas campanhas eleitorais. Devido à supremacia do interesse público, poderia utilizar-se de recursos tecnológicos, como os SRSO, para observar as ações e as preferências dos indivíduos (Barriga, 2020).

Atividades com o propósito de controlar, dominar, intimidar com ameaças a pessoas ou grupos, por terceiros são caracterizadas no subgrupo Chantagem (Rodrigues; Sant'Ana, 2016). Comunicações científicas classificadas neste subgrupo apresentaram como preocupações a possibilidade de anonimato, por meio da criação de perfis falsos, e a existência de situações ameaçadoras a pessoas ou a grupos (Rebs, 2018; Santos; Porto; Alturas, 2010).

A possibilidade de criação de perfis falsos pode contribuir para o discurso de ódio proferido por indivíduos que se sentem protegidos por um possível anonimato no SRSO (Rebs, 2018). Os indivíduos que praticam atividades elencadas no subgrupo Chantagem se utilizam da infraestrutura e dos recursos do SRSO (criação de vários perfis) para a prática de

violência simbólica com o intuito de humilhar as vítimas por meio de palavras ofensivas ou distorcendo narrativas (Santos; Porto; Alturas, 2010).

O subgrupo Apropriação é conceituado como o ato de se apropriar de dados realizando a vinculação de dados dos indivíduos a uma propaganda publicitária, com a intenção de obter benefícios (Rodrigues; Sant'Ana, 2016). Foram classificadas neste subgrupo comunicações científicas que apresentaram relações entre os SRSO e a apropriação de dados. Observou-se que as comunicações científicas estão divididas entre a apropriação de dados por meio de vínculo a propagandas (Fugazza; Saldanha, 2018) e apropriação de imagens por profissionais de saúde (Purim; Tizzot, 2019).

A forma de obtenção de lucro pelos SRSO é por meio de propagandas. O serviço funciona como intermediário entre potenciais consumidores (indivíduos que utilizam os serviços) e as empresas em busca de clientes. Esta intermediação tem base nos dados dos indivíduos para direcionar as propagandas. Neste sentido, poderia existir um risco à privacidade quando os SRSO utilizam os dados de indivíduos para segmentá-lo, agrupá-lo e direcioná-lo para a oferta de um serviço ou produto de um terceiro ou para chancelar um serviço ou um produto sem o seu consentimento, sendo esta uma ação que contraria a ética da informação (Fugazza; Saldanha, 2018). O uso de imagens de pacientes por profissionais de saúde que atuam na área da estética pode ser considerado uma atividade de apropriação se houver a utilização dos dados pessoais dos pacientes para chancelar um produto ou serviço sem seu consentimento, pois esta prática pode ter a pretensão de autopromoção e o alcance de um maior número de clientes (Purim; Tizzot; 2019).

O ato de disseminar informações falsas ou interpretadas de maneira dúbia sobre um indivíduo são características do subgrupo Distorção (Rodrigues; Sant'Ana, 2016). Foi classificada neste subgrupo uma comunicação científica que apresentou as implicações sobre os recursos utilizados na distorção em contextos dos SRSO. Entre as ferramentas disponibilizadas pelos SRSO existem recursos capazes de distorcer ou alterar o conteúdo informacional. Por exemplo, o SRSO Instagram possui diferentes filtros que podem tornar uma imagem alterada por meio de aplicação de filtros na intenção de torná-la diferente do original, dando a falsa percepção de realidade. Este tipo de prática tem potencial risco de modificar o contexto original, fazendo com que os demais indivíduos tenham acesso apenas a uma parte dos dados e das informações, ou fazer com que fatos ou determinados dados dos indivíduos sejam omitidos da imagem original, distorcendo os fatos originais (Streck; Pellanda, 2017).

4.4 Grupo IV Invasão (subgrupos: Intromissão e Interferência decisional)

Conceitua-se o subgrupo Intromissão o ato de adentrar assuntos que tenham caráter privado (Rodrigues; Sant'Ana, 2016). O envio de imagens, vídeos e mensagens de texto podem ser processadas pelos SRSO como forma de tornar as experiências melhores no serviço. Todavia, estes dados podem ser processados, segmentados e categorizados com a finalidade de minerar informações sobre os indivíduos, permitindo identificar, por exemplo, posições religiosas por símbolos em imagens do indivíduo, posições políticas por textos nas mensagens, entre outros (Barriga, 2020; Purim; Tizzot, 2019; Streck; Pellanda, 2017). Outra possível forma de incursão por meio dos serviços disponibilizados é a personalização do *feed* de notícias, pois neste recurso são gerados dados de preferência, interações com outros perfis e páginas, interações com propagandas que poderiam ser utilizados pelos detentores

dos SRSO para aumentar o repertório de informações sobre o indivíduo e direcionar o conteúdo, a partir de suas preferências privadas (Jurno; D'Andréa; 2017).

Ações de envolvimento do Estado em assuntos de caráter privado, alterando decisões em nome do indivíduo são características do subgrupo Interferência decisional (Rodrigues; Sant'Ana, 2016). Foi classificada uma comunicação científica que aborda possíveis implicações da utilização dos SRSO pelo Estado (Barriga, 2020). Uma das implicações levantadas pelo autor poderia ser o direcionamento de conteúdos políticos, a partir das preferências e inclinações políticas dos indivíduos, isso poderia ocasionar alterações nas decisões dos indivíduos, caracterizando uma ação de interferência decisional.

5 CONSIDERAÇÕES FINAIS

Os SRSO são espaços públicos online que oferecem serviços de entretenimento por meio da interação entre indivíduos e reúnem extensas quantidades de dados. Estes serviços possuem como característica a possibilidade de atribuir um identificador único a cada perfil criado e realizar sucessivas coletas de dados quando o indivíduo utiliza ou realiza atividades externas ao SRSO.

Diante da existência de um contexto permeado pelo fluxo de dados com potencialidades de uso, a Ciência da Informação pode contribuir para a identificação dos problemas e apontar soluções. Assim, uma das contribuições está na utilização de uma taxonomia que possibilita classificar e sistematizar os potenciais riscos à privacidade debatidos na literatura científica sobre uso de dados pessoais no contexto de privacidade, sobretudo, em SRSO.

O estreitamento entre espaços públicos e privados, as possíveis consequências em caso de violação do uso dos dados pessoais e os interesses dos envolvidos no processo são fatores que podem apresentar riscos à privacidade dos indivíduos que utilizam serviços online, especialmente, os SRSO. Desse modo, esta pesquisa buscou identificar potenciais riscos à privacidade no universo dos SRSO na literatura científica e classificá-los a partir de uma Taxonomia da Privacidade, demonstrando a relação entre os subgrupos e os assuntos de cada uma das comunicações científicas analisadas.

As comunicações científicas foram classificadas nos 16 subgrupos e tiveram ocorrência em mais de um subgrupo, pois foi considerada a aderência das discussões apresentadas no artigo com as descrições dos subgrupos. A classificação das comunicações científicas apresentou maior incidência no grupo Coleta de informação, especialmente no subgrupo Vigilância, com preocupações referentes à forma de obtenção dos dados dos indivíduos, ainda que externo ao SRSO, o aumento do repertório de informações caracterizando uma possível forma de vigilância nos espaços público e privado viabilizada pelos dispositivos tecnológicos como os *smartphones*. Foram abordadas discussões sobre a obrigatoriedade de preenchimento de formulários com as informações pessoais nos SRSO, caracterizando o subgrupo Interrogatório.

No grupo Processamento de informação, as comunicações científicas tiveram maior incidência no subgrupo Exclusão. As discussões abordaram sobre o distanciamento entre o detentor do SRSO e o indivíduo que o utiliza sobre a participação na decisão do tratamento que os dados recebem, caracterizando uma situação de exclusão das decisões. Houve pesquisas classificadas neste subgrupo que apresentaram relações com outros subgrupos como: Agregação, a existência de múltiplas fontes que geram dados que podem ser replicados em outros contextos sem a participação do indivíduo; Identificação, a existência

de dados passíveis de identificação sem a possibilidade do indivíduo decidir pela anonimização; Insegurança com implicações da visibilidade e do acesso a dados por terceiros de forma não autorizada e Uso secundário, os casos de compartilhamento em cadeia feitos por outros indivíduos para chancela de serviços ou produtos sem a participação do primeiro indivíduo.

No caso do grupo Disseminação da informação, as comunicações científicas foram classificadas nos subgrupos Quebra do sigilo, Divulgação, Exposição, Aumento do acesso, Chantagem, Apropriação e Distorção. Nesses subgrupos, foram apresentados como preocupações: os elementos disponíveis para a proteção de dados de visualização identificados nos SRSO com potencial da quebra do sigilo, a divulgação de momentos cotidianos em SRSO, a exposição de dados pessoais e sensíveis nos serviços, a possibilidade do aumento do acesso aos dados dos indivíduos por outros indivíduos usuários dos serviços ou agentes externos, a criação de perfis falsos como possibilidade de realizar chantagens ou disseminar discurso de ódio, a apropriação dos dados dos indivíduos com fins lucrativos ou para a promoção de um serviço/produto, por fim, possíveis implicações das distorções possibilitadas pelas ferramentas de interação dos SRSO.

Invasão é o grupo que contém os subgrupos Intromissão e Interferência decisional. O primeiro subgrupo apresentou comunicações científicas que expressaram preocupações sobre as consequências do processamento, da segmentação e da categorização dos dados com a finalidade de minerar informações sobre os indivíduos, permitindo identificar, por exemplo, posições religiosas e políticas por textos nas mensagens, aumentando o repertório de informações. O segundo subgrupo foi abordado como interferência decisional das implicações que poderia ser o direcionamento de conteúdos políticos a partir das preferências e inclinações políticas, isso poderia ocasionar alterações nas decisões dos indivíduos.

Conclui-se que a utilização da Taxonomia da Privacidade permitiu a classificação das comunicações científicas obtidas por meio de uma RSL que envolveu temas de privacidade, SRSO, dados e atores envolvidos. Desse modo, a classificação das pesquisas permitirá à comunidade científica perceber a identificação da incidência dos potenciais riscos à privacidade, abordados na literatura. Espera-se que os resultados obtidos a partir da classificação realizada nesta pesquisa contribuam com a possibilidade de investigações futuras em assuntos de baixa aderência ou pouco explorados pela literatura, uma maior atenção sobre as principais e potenciais ações prejudiciais aos dados pessoais em SRSO.

REFERÊNCIAS

AMARAL FILHO, O. A.; BLANCO, D. R. O espetáculo cultural na rede social: a abordagem midiática do Coletivo Dirigível de teatro na Rede Social Digital Facebook. **Sessões do Imaginário**, Porto Alegre, v. 19, n. 31, p. 29-38, 2014. Disponível em: file:///C:/Users/User/Downloads/admin,+Blanco.pdf. Acesso em: 2 fev. 2022.

ASSUMPÇÃO, F. S.; SANT'ANA, R. C. G.; SANTOS, P. L. V. A. C. Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais. **Em Questão**, Porto Alegre, v. 21, n. 2, p. 31-48, 2015. DOI: 10.19132/1808-5245212.31-48. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/54545. Acesso em: 2 fev. 2022.

BARRIGA, A. C. A publicitação do privado na era da pós-verdade: uma exploração às redes sociais dos líderes políticos portugueses. **Observatorio (OBS*)**, [*S. l.*], v. 14, n. 2, 2020. DOI: 10.15847/obsOBS14220201609. Disponível em: https://obs.obercom.pt/index.php/obs/article/view/1609/pdf. Acesso em: 2 fev. 2022.

BORGES, M. T. Mercado, vigilância e Facebook na era do espetacular integrado, ou inside us all there is a code. **Literatura:** teoria, história, crítica, [*S. l.*], v. 22, n. 1, p. 137-178, 2020. DOI: https://doi.org/10.15446/lthc.v22n1.82295. Disponível em: https://www.redalyc.org/journal/5037/503763261005/html/. Acesso em: 2 fev. 2022.

BORKO, H. Information Science: Whatindexação socialit? **American Documentation**, [*S. l.*], v. 19, n. 1, p. 3-5, jan. 1968. Disponível em: https://edisciplinas.usp.br/pluginfile.php/2532327/mod_resource/content/1/Oque%C3%A9CI.pdf. Acesso em: 06 fev. 2020.

BOYD, D. M.; ELLISON, B. N. Social Network Sites: Definition, History, and Scholarship. **Journal of Computer-Mediated Communication**, [*S. l.*], v. 13, n. 1, p. 210-230, 2007. DOI: https://doi.org/10.1111/j.1083-6101.2007.00393.x.Disponível em: https://academic.oup.com/jcmc/article/13/1/210/4583062. Acesso em: 1 jun. 2020.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n° 12.965, de 23 de abril de 2014 (marco civil da internet). **Diário Oficial [da] República Federativa do Brasil**: seção 1, Brasília, DF, n. 157, p. 59, 15 ago. 2018. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337. Acesso em: 21 abr. 2023.

COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR (Brasil). **Plataforma Sucupira**. c2021. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsf. Acesso em: 15 out. 2021.

CONFORTO, E. C.; AMARAL, D. C.; SILVA, S. L. **Roteiro para revisão bibliográfica sistemática:** aplicação no desenvolvimento de produtos e gerenciamento de projetos. *In*: CONGRESSO BRASILEIRO DE GESTÃO DE DESENVOLVIMENTO DE PRODUTO. Porto Alegre: [*s. n.*], 2011. Disponível em: https://edisciplinas.usp.br/pluginfile.php/2205710/mod_resource/content/1/Roteiro%20para%20revis%C3%A3o%20bibliogr%C3%A1fica%20sistem%C3%A1tica.pdf. Acesso em: 20 ago. 2021.

DONEDA, D. Reflexões sobre proteção de dados pessoais em redes sociais. **Revista Internacional de Protección de Datos Personales**, Bogotá, n. 1, p. 3-12, 2012. Disponível em: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Danilo-Doneda_FINAL.pdf.pdf. Acesso em: 11 de jul. 2021.

EUROPEAN PARLIAMENT. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of 291

personal data and on the free movement of such data. **Official Journal of Parliament Communities**, p. 31-39, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/eli/dir/1995/46/oj. Acesso em: 26 abr. 2023.

EVERTON, R. *et al*. Investigando o fenômeno de compras coletivas on-line: fatores que influenciam a intensidade das compras. **Revista de Administração**, Santa Maria, v. 7, p. 196-213, 2014. DOI: 10.5902/198346597084. Disponível em: https://periodicos.ufsm.br/reaufsm/article/download/7084/pdf/70659. Acesso em: 2 fev. 2022.

FOGEL, J.; NEHMAD, E. Internet social network communities: risk taking, trust, and privacy concerns. **Computers in human behavior**, [*S. l.*], v. 25, n. 1, p. 153-160, 2009. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0747563208001519. Acesso em: 20 jan. 2023.

FUGAZZA, G. Q.; SALDANHA, G. S. A questão do direito à privacidade no Facebook: um estudo à luz da ética da informação. **Informação & Informação**, Londrina, v. 23, n. 3, p. 462-494, 2018. Disponível em: https://www.uel.br/revistas/uel/index.php/informacao/article/view/28108. Acesso em: 2 fev. 2022.

GONZATTI, C.; BITTENCOURT, M. C. A.; ESMITIZ, F. De Rainha dos Baixinhos a Rainha dos Memes: o humor como vetor de ciberacontecimentos a partir da ida de Xuxa da Rede Globo para a Rede Record. **Revista Sessões do Imaginário**, Porto Alegre, v. 20, n. 34, 2015. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/20546/14055. Acesso em: 2 fev. 2022.

GROSS, R.; ACQUISTI, A. Information revelation and privacy in online social networks. *In*: WPES: WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY, 5., Alexandria, 2005. **Proceedings** [...]. Alexandria, VA, USA: Association for Computing Machinery, 2005, p. 71-80. Disponível em: https://dl.acm.org/doi/10.1145/1102199.1102214. Acesso em: 18 jul. 2020.

HAGE, Z. C. M.; KUBLIKOWSKI, I. Estilos de uso e significados dos autorretratos no Instagram: Identidades narrativas de adultos jovens brasileiros. **Estudos e Pesquisas em Psicologia**, Rio de Janeiro, v. 19, n. 2, p. 522-539, maio/ago. 2019. Disponível em: http://pepsic.bvsalud.org/pdf/epp/v19n2/v19n2a11.pdf. Acesso em: 19 abr. 2023.

JURNO, A. C.; D'ANDRÉA, C. F. B. (In)visibilidade algorítmica no "feed de notícias" do Facebook. **Contemporanea | Revista de Comunicação e Cultura**, [*S. l.*], v. 15, n. 2, p. 463-484, maio/ago. 2017. Disponível em: https://periodicos.ufba.br/index.php/contemporaneaposcom/article/view/17796/15142. Acesso em: 13 fev. 2022.

KOKOLAKIS, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. **Computers & Security**, [*S. l.*], v. 64, p. 122-134, 2017. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404815001017.

Acesso em: 12 maio 2020.

LEITZKE, A. T. S.; RIGO, L. C. Sociedade de controle e redes sociais na internet: #saúde e #corpo no Instagram. **Movimento:** revista de Educação Física da UFGRS, n. 26, 2020. Disponível em: https://www.scielo.br/j/mov/a/t6BTk4gr9XH9Z3BwLrwMMyp/?format=pdf&lang=pt. Acesso em: 20 dez. 2021.

LEONARDI, M. **Tutela e privacidade na internet**. 1. ed. São Paulo: Saraiva, 2012. v. 1
LIMA, L. A. Diretrizes para aperfeiçoamento e interpretação da lei do marco civil da internet com vistas à garantia do direito à privacidade nas redes sociais. **Prisma Jurídico**, São Paulo, v. 17, n. 1, p. 59-81, 2018. Disponível em: https://periodicos.uninove.br/prisma/article/view/8084/pdf_78. Acesso em: 2 fev. 2023.

MAI, J. E. Big data privacy: The datafication of personal information. **The Information Society**, [*S. l.*], v. 32, n. 3, p. 192-199, 26 maio 2016. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/01972243.2016.1153010?journalCode=utis20. Acesso em: 26 abr. 2023.

MARTORELL, L. B.; NASCIMENTO, W. F.; GARRAFA, V. Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no facebook. **Interface - Comunicação, Saúde, Educação**, [*S. l.*], v. 20, n. 56, p. 13-23, 2015. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1414-32832016000100013&lng=pt&tlng=pt. Acesso em: 11 fev. 2022.

MENDES-CAMPOS, C.; FÉRES-CARNEIRO, T.; MAGALHÃES, A. Extimidade virtual e conjugalidade: possíveis repercussões. **Psicologia**: teoria e prática, São Paulo, v. 22, n. 1, p. 285-299, 2020. Disponível em: http://pepsic.bvsalud.org/pdf/ptp/v22n1/pt_v22n1a10.pdf. Acesso em: 17 de fev. 2021.

MISLOVE, A. *et al*. Measurement and Analysis of Online Social Networks. *In:* CONFERENCE ON INTERNET MEASUREMENT, 7., 2007, San Diego, California. **Proceedings** [...]**.** San Diego, California: Association for Computing Machinery. 2007, p. 29-42. Disponível em: https://dl.acm.org/doi/pdf/10.1145/1298306.1298311. Acesso em: 11 fev. 2022.

MISUGI, G.; FREITAS, C. O. A.; EFING, A. C. Releitura da Privacidade Diante das Novas Tecnologias: Realidade Aumentada, Reconhecimento Facial e Internet das Coisas. **Revista Jurídica Cesumar**, [*S. l.*], v. 16, n. 2, p. 427-453, 2016. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/4433/2804. Acesso em: 24 mar. 2023.

NOVO, R.; AZEVEDO, M. M. A percepção de vulnerabilidade e aplicação ética das informações nas redes sociais pelos sistemas de big data. **Tekhne e Logos**, Botucatu, v. 5, n. 2, 2014. Disponível em: http://revista.fatecbt.edu.br/index.php/tl/article/view/298/214#. Acesso em: 15 jul. 2021.

PURIM, K. S. M.; TIZZOT, E. L. A. Protagonismo dos Estudantes de Medicina no Uso do Facebook na Graduação. **Revista Brasileira de Educação Médica**, [*S. l.*], v. 43, n. 1, p. 187-196, 2019. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022019000100187&tlng=pt. Acesso em: 11 jan. 2021.

REBS, R. R. O excesso no discurso de ódio dos haters. **Fórum Linguístico**, Florianópolis, v. 14, p. 2512-2523, 2017. Disponível em: https://periodicos.ufsc.br/index.php/forum/article/view/1984-8412.2017v14nespp2512/35377. Acesso em: 11 fev. 2021.

RODRIGUES, F. A. **Coleta de dados em redes sociais**: privacidade de dados pessoais no acesso via Application Programming Interface. 2017. 679 f. Tese (Doutorado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação, Universidade Estadual Paulista, Marília, 2017. Disponível em: https://repositorio.unesp.br/handle/11449/149768. Acesso em: 20 abr. 2023.

RODRIGUES, F. A.; SANT'ANA, R. C. G. Use of taxonomy of privacy to identify activities found in social networks' terms of use. **Knowledge Organization**, [*S. l.*], v. 43, n. 4, p. 285-295, 2016.

RODRIGUES, F. A.; SANT'ANA, R. C. G. Contextualização de conceitos teóricos no processo de coleta de dados de Redes Sociais Online. **Informação & Tecnologia**, Marília/João Pessoa, v. 5, n. 1, p. 18-36, jan./jun. 2018. Disponível em: http://hdl.handle.net/20.500.11959/brapci/110391. Acesso em: 26 abr. 2023.

ROSADO, L. A. S.; TOMÉ, V. M. N. As redes sociais na internet e suas apropriações por jovens brasileiros e portugueses em idade escolar. **Revista Brasileira de Estudos Pedagógicos**, [*S. l.*], v. 96, n. 242, p. 11–25, jan. 2015. Disponível em: http://www.scielo.br/j/rbeped/a/Sptq7rTsYB9QyqYXyzTjVts/abstract/?lang=pt. Acesso em: 11 jan. 2021.

SÁ, F. P. Pesquisando co-viewing em redes sociais e aplicativos de mensagem instantânea: ética e desafios. **Comunicação e Sociedade**, [*S. l.*], v. 33, p. 391–408, 2018. Disponível em: https://revistacomsoc.pt/index.php/revistacomsoc/article/view/1071/1051. Acesso em 11 jan. 2021

SANT'ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. **Informação & Informação**, Londrina, v. 21, n. 2, p. 116, 2016. Disponível em: http://www.uel.br/revistas/uel/index.php/informacao/article/view/27940. Acesso em: 11 abr. 2023.

SANTOS, V. S.; PORTO, E.; ALTURAS, B. Análise de mecanismos de controle de acesso nas redes sociais. **Revista Portuguesa e Brasileira de Gestão**, Lisboa, v. 9, n. 3, p. 50-60, jun./set. 2010. Disponível em: https://repositorio.iscte-iul.pt/handle/10071/8638. Acesso em: 17 jan. 2022.

STRECK, M.; PELLANDA, E. C. Instagram como interface da comunicação móvel e ubíqua. **Sessões do Imaginário**, Porto Alegre, v. 22, n. 37, p. 10-19, 2017. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/28017/15936. Acesso em: 10 fev. 2022.

SOLOVE, D. **Understanding privacy.** Cambridge, Massachusetts: Harvard University Press, 2008.

TUFEKCI, Z. Can you see me now? Audience and disclosure regulation in online social network sites. **Bulletin of Science, Technology & Society**, [S. l.], v. 28, n. 1, p. 20-36, 2008. Disponível em: https://journals.sagepub.com/doi/10.1177/0270467607311484. Acesso em: 11 abr. 2023.

WANG, H. **Protecting privacy in China**: a research on China's privacy standards and the possibility of establishing the right to privacy and the information privacy protection legislation in modern China. Heidelberg; New York: Springer, 2011.

WARREN, S.; BRANDEIS, L. The right to privacy. **Harvard law review**, [S. l.], v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?origin=crossref&seq=8. Acesso em: 11 abr. 2023.

ZIMMER, M. "But the data is already public": on the ethics of research in Facebook. **Ethics and Information Technology**, [*S. l.*], v. 12, n. 4, p. 313-325, 2010. Disponível em: https://rdcu.be/daX9J. Acesso em: 11 abr. 2021.

APÊNDICE A – POTENCIAIS RISCOS À PRIVACIDADE DE DADOS EM SRSO CLASSIFICADOS PELA TAXONOMIA DA PRIVACIDADE, ORDENADOS PELO ANO DE PUBLICAÇÃO DA LITERATURA VINCULADA AOS POTENCIAIS RISCOS

Quadro 3 – Potenciais riscos à privacidade de dados em SRSO identificados na literatura analisada, classificados pela Taxonomia da Privacidade

Grupo	Subgrupo	Potenciais riscos à privacidade	Comunicações Científicas
Coleta de dados	Vigilância	Os SRSO podem contribuir para um novo modelo de vigilância, pois o potencial risco à privacidade é o monitoramento no ambiente digital. Foram apontados como um problema geracional a relação entre TIC, vigilância e coleta de dados, pois haveria uma relação entre esses elementos que impacta em uma percepção ambiente seguro quando os indivíduos utilizam as ferramentas do SRSO para interação e no fornecimento de dados. É possível que o uso de dispositivos móveis atue como meio facilitador de acesso aos SRSO que tornaram o uso intenso pelos indivíduos, resultando na produção de grandes volumes de dados que podem ser utilizados para monitoramento.	(ROSADO; TOMÉ, 2015)
			(FUGAZZA; SALDANHA, 2018)
			(BARRIGA, 2020)
			(LEITZKE; RIGO, 2020)
			(ZAKIEE; HAGE; KUBLIKOWSKI, 2019)
			(MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020)
			(ASSUMPÇÃO; SANT'ANA; SANTOS, 2015)
			(STRECK; PELLANDA, 2017)
	Interrogatório	O preenchimento obrigatório de formulários pode configurar como um potencial risco à privacidade, pois os dados pessoais coletados podem ser armazenados em banco de dados e de acordo com a política de privacidade podem ser compartilhados com agentes externos.	(LIMA, 2018)
			(SÁ, 2018)
Processamento da informação	Agregação	A agregação de múltiplas fontes geradoras de dados pode contribuir para reuni-los em bases de dados, no qual uma das fontes geradoras é a própria utilização dos SRSO e metadados dos dispositivos de acesso. As curtidas e os comentários, quando associados a outros dados, podem apresentar afinidades a assuntos, como os que envolvem política e religião.	(ROSADO; TOMÉ, 2015)
			(STRECK; PELLANDA, 2017)
			(JURNO; D'ANDRÉA, 2017)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
	Identificação	O envio de imagens e a publicação por SRSO podem conter dados passíveis de identificação que permitam a (re)identificação dos indivíduos caso sejam reunidos com outros dados. Uso de técnicas de identificação como o reconhecimento facial por SRSO poderia ser uma forma de identificação de dados realizada por meio de análise de imagem, além da possibilidade de conter dados suficientes para identificar características que combinadas a outras permitam identificá-lo.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
	Insegurança	Os SRSO como ambientes públicos podem estar sujeitos às implicações da visibilidade e acesso a dados por terceiros de forma não autorizada. O envio de dados pessoais e a coleta de dados sobre a utilização que o indivíduo realiza nos serviços podem ser coletados por agentes externos. Além disso, não são descritas limitações ou quais conjuntos de dados estão sujeitos a proteção nas Políticas de	(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
			(REBS, 2017)

Grupo	Subgrupo	Potenciais riscos à privacidade	Comunicações Científicas
		Privacidade, configurando-as como elementos de opacidade.	(FUGAZZA; SALDANHA, 2018)
		A opacidade na transparência sobre o que é realizado com os dados a partir da Política de Privacidade é um dos aspectos que podem causar insegurança. No caso do Facebook, maior SRSO em número de usuários, é referente a uma de suas cláusulas, a modificação unilateral. O grande impasse sobre essa cláusula é que quando os indivíduos realizam o registro no serviço estão automaticamente concordando com a cláusula, porém a instituição detentora poderá alterar a qualquer tempo o conteúdo do termo, cabendo ao indivíduo concordar para continuar utilizando os serviços.	(FUGAZZA; SALDANHA, 2018)
			(BORGES, 2020)
	Uso secundário	A formação de diários completos sobre um indivíduo como os produzidos no Instagram podem ser utilizados para diferentes finalidades da proposta de uso do SRSO.	(ZAKIEE; HAGE; KUBLIKOWSKI, 2019)
		O *marketing* direcionado (ou personalizado) de conteúdos políticos e ideológicos podem ser considerados como uso secundário de dados, uma vez que a obtenção dos dados pelo SRSO, conforme a Política de Privacidade, são para direcionar o consumo de produtos e serviços.	(FUGAZZA; SALDANHA, 2018)
			(BORGES, 2020)
			(JURNO; D'ANDRÉA, 2017)
	Exclusão	Casos de compartilhamento em cadeia podem ser caracterizados como atividades de exclusão. Os indivíduos que utilizam SRSO, ao enviar um conteúdo para o serviço e disponibilizar para uma lista restrita de perfis, passam pela possibilidade que o conteúdo seja recompartilhado a terceiros por um perfil incluído na lista, representando que o indivíduo foi excluído da decisão de recompartilhamento. Há possibilidade de cópias dos dados armazenados pelos detentores: o indivíduo é excluído do processo decisório sobre a replicabilidade em outras bases sob a guarda de terceiros ou de agentes externos.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
			(SANTOS; PORTO; ALTURAS, 2010)
			(AMARAL FILHO; BLANCO, 2014)
			(GONZATTI; BITTENCOURT; ESMITIZ, 2015)
			(BORGES, 2020)
			(STRECK; PELLANDA, 2017)
			(JURNO; D'ANDRÉA; 2017)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
Disseminação da Informação	Quebra do sigilo	A utilização de imagens de pacientes em procedimentos estéticos, quando realizadas de forma não autorizada, pode desencadear implicações para a privacidade dos pacientes.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
		O envio de um conteúdo e a publicação pelo SRSO pode ser feito ajustes de configuração sobre quem poderá visualizar a publicação como mecanismo de proteção sobre o acesso ao conteúdo. Entretanto, existe a possibilidade de outros indivíduos participantes da rede de perfis realizarem novo recompartilhamento, podendo ser contrário ao primeiro ajuste.	(SANTOS; PORTO; ALTURAS, 2010)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2017)
	Divulgação	Existe um potencial risco à privacidade quando são publicados dados pessoais ou fatos íntimos dos indivíduos. Especialmente nas publicações realizadas por mulheres, existe maior possibilidade de desencadear ações de perseguições que provocam constrangimento ou a restrição da liberdade.	(MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020)

Grupo	Subgrupo	Potenciais riscos à privacidade	Comunicações Científicas
	Exposição	A facilidade de utilização dos SRSO é uma das formas de contribuir para a exposição de dados. Os SRSO estimulam os indivíduos a expor situações ou momentos do cotidiano, sobretudo indivíduos nascidos após a consolidação da Internet e dos dispositivos móveis.	(ZAKIEE; HAGE; KUBLIKOWSKI, 2019)
		A exposição de dados de pacientes na área da saúde e a utilização de dados sigilosos para a promoção de atividades profissionais deve ser precedida de autorização formal dos pacientes, ainda que seja utilizado para fins de pesquisa e atividades profissionais, os dados sensíveis devem ser anonimizados.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
			(PURIM; TIZZOT, 2019)
		Os dados financeiros são de cunho privado, sendo restrito ao próprio indivíduo ou a instituição para qual forneceu os dados. A exposição de dados em SRSO, que coletam dados financeiros para realização de pagamentos pelo serviço, pode desencadear atividades prejudiciais ao indivíduo como a ocorrência de fraudes e golpes, sendo imprescindível a proteção.	(EVERTON, et al., 2014)
		A exposição de características físicas dos indivíduos em SRSO, no qual a publicação feita por um indivíduo pode receber comentários desrespeitosos por meio do anonimato com a criação de perfis falsos.	(REBS, 2017)
	Aumento do acesso	Constata-se uma ausência ou baixa percepção de preocupações dos usuários em relação à coleta de dados feita pelos SRSO. A prática de covisualização dos conteúdos audiovisuais em SRSO – fenômeno pode ser observado na interação dos indivíduos com outros indivíduos por meio de dispositivos tecnológicos – deixa rastros, como, por exemplo, o fornecimento deliberado de metadados.	(SÁ, 2018)
		Os Termos de Uso dos SRSO apresentam informações que podem aumentar o acesso a dados pessoais de forma opaca ao usuário. Sob a perspectiva da ética da informação em SRSO, há baixa transparência sobre o que pode ser realizado com os dados coletados por meio da permissão via termo de uso e o compartilhamento com as conexões.	(FUGAZZA; SALDANHA, 2018)
		Os dados coletados pelos SRSO podem ter acesso ampliado ao Estado.	(BORGES, 2020)
			(BARRIGA, 2020)
	Chantagem	A possibilidade de criação de perfis falsos pode contribuir para o discurso de ódio e chantagem, proferido por indivíduos que se sentem protegidos por um possível anonimato no SRSO.	(REBS, 2018)
			(SANTOS; PORTO; ALTURAS, 2010)

Grupo	Subgrupo	Potenciais riscos à privacidade	Comunicações Científicas
	Apropriação	A forma de lucro dos SRSO é por meio de propagandas, funcionando como intermediário entre potenciais consumidores (usuários) e as empresas em busca de clientes. Esta intermediação tem base nos dados pessoais para direcionar as propagandas. Existe um risco à privacidade, quando os SRSO utilizam os dados pessoais para chancelar um serviço ou um produto sem consentimento, sendo esta uma ação que contraria a ética da informação.	(FUGAZZA; SALDANHA, 2018)
		O uso de imagens de pacientes por profissionais de saúde que atuam na área da estética pode ser considerado uma atividade de apropriação, se houver a utilização dos dados pessoais dos pacientes para chancelar um produto ou serviço sem consentimento.	(PURIM; TIZZOT; 2019)
	Distorção	Entre as ferramentas disponibilizadas pelos SRSO existem recursos capazes de distorcer ou alterar o conteúdo informacional, tais como diferentes filtros que podem tornar uma imagem alterada na intenção de torná-la diferente do original.	(STRECK; PELLANDA, 2017)
Invasão	Intromissão	O envio de imagens, vídeos e mensagens de texto podem ser processadas pelos SRSO para tornar as experiências melhores no serviço. Todavia, estes dados podem ser processados, segmentados e categorizados para minerar informações sobre os indivíduos, permitindo identificar, por exemplo, posições religiosas ou políticas por símbolos em imagens do usuário.	(STRECK; PELLANDA, 2017)
			(PURIM; TIZZOT, 2019)
			(BARRIGA, 2020)
		Outra possível forma de incursão é a personalização do *feed* de notícias, pois neste recurso são gerados dados de preferência, interações com outros perfis e páginas, interações com propagandas que poderiam ser utilizados pelos detentores dos SRSO para aumentar o repertório de informações sobre o indivíduo e direcionar o conteúdo.	(JURNO; D'ANDRÉA; 2017)
	Interferência decisional	Uma das implicações poderia ser o direcionamento de conteúdos políticos, a partir das preferências e inclinações políticas dos indivíduos.	(BARRIGA, 2020)

Fonte: Elaborado pelos autores (2023).