UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Débora Matni Fonteles

REVISÃO SISTEMÁTICA DE LITERATURA SOBRE OS RISCOS RELACIONADOS À PRIVACIDADE DE DADOS EM SERVIÇOS DE REDES SOCIAIS ONLINE NO BRASIL

Belém

2022

Débora Matni Fonteles

REVISÃO SISTEMÁTICA DE LITERATURA SOBRE OS RISCOS RELACIONADOS À PRIVACIDADE DE DADOS EM SERVIÇOS DE REDES SOCIAIS ONLINE NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação como requisito parcial para a obtenção do grau de Mestre em Ciência da Informação pela Universidade Federal do Pará.
Orientador: Prof. Dr. Fernando de Assis Rodrigues

Belém
2022

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

F682r Fonteles, Débora Matni.
Revisão sistemática de literatura sobre os riscos relacionados à privacidade de dados em Serviços de Redes Sociais Online no Brasil / Débora Matni Fonteles. — 2022.
162 f. : il. color.

Orientador(a): Prof. Dr. Fernando de Assis Rodrigues
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Ciência da Informação, Belém, 2022.

1. Redes sociais on-line. 2. Direito à Privacidade. 3. Proteção de dados. 4. Tecnologia da Informação. I. Título.

CDD 020

Débora Matni Fonteles

REVISÃO SISTEMÁTICA DE LITERATURA SOBRE OS RISCOS RELACIONADOS À PRIVACIDADE DE DADOS EM SERVIÇOS DE REDES SOCIAIS ONLINE NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação como requisito parcial para a obtenção do grau de Mestre em Ciência da Informação pela Universidade Federal do Pará.
Orientador: Prof. Dr. Fernando de Assis Rodrigues

Data de Aprovação
23/05/2022

BANCA EXAMINADORA

_____
Prof. Dr. Fernando de Assis Rodrigues – Orientador
Universidade Federal do Pará (UFPA)

_____
Prof. Dr. Cristian Berrío Zapata
Universidade Federal do Pará (UFPA)

_____
Prof. Dr. Ricardo César Gonçalves Sant'Ana
Universidade Estadual Paulista (UNESP)

AGRADECIMENTOS

Meu agradecimento é direcionado primeiramente à minha família. Aos meus pais por me mostrarem sempre o valor que a educação tem de transformar a vida das pessoas. Ao meu Pai, em especial (*in memoriam*).

Ao meu marido José Antônio Cavalleiro que sempre esteve comigo nos momentos mais difíceis da minha vida. Agradeço pelo carinho, amor, confiança e compreensão.

Aos meus filhos Mellina e José Antônio agradeço todo apoio e força que me deram no momento em eu estava mais fragilizada, enfrentando a dor da perda de um irmão tão querido. Não foi fácil, mas vocês estavam ao meu lado e por diversas vezes me acolheram, me encheram de carinho e não me deixaram desistir do sonho de me tornar mestre. Ao Júnior em especial que foi também meu companheiro nas noites e madrugadas que passamos ora escrevendo, ora trocando conhecimento, rindo ou chorando. Cada detalhe, cada momento que passamos foi muito especial. Amo muito vocês.

Aos meus irmãos que enfrentaram junto comigo a doença, as angústias e a partida de nosso irmão Luiz Cláudio Matni.

A você meu irmão que nos deixou no momento em que tantos outros partiram. Dedico este título de mestre. Você que teve a chance também de se tornar mestre foi tolhido deste direito. Você que poderia ter vivido conosco tantos momentos ainda não vividos foi chamado às pressas para junto de Deus. Mas jamais irão nos tirar a oportunidade de ter convivido com você. Te amo eternamente.

Meu agradecimento especial ao meu Orientador Dr. Fernando de Assis Rodrigues que me fez enxergar o quão importante é o crescimento e o amadurecimento na ciência. Obrigada pelos ensinamentos, pelas muitas horas de orientações, de carinho, de amizade e por ter acreditado em mim. Muito obrigada.

Aos meus colegas de turma também agradeço pela convivência e pelos momentos alegres que mesmo na distância se tornaram importantes. A turma de 2020 foi diferente. Imaginamos que estivéssemos no melhor momento quando se iniciava o ciclo dos componentes curriculares, mas infelizmente tivemos que nos afastar. O afastamento não foi de dias e sim de dois anos, exatamente o tempo para obter o título de mestre. Por fim, devo dizer que somos os mestres formados no novo normal da pandemia de Covid-19.

A banca de avaliação formada pelos Doutores Cristian Berrío Zapata e Ricardo César Gonçalves Sant'Ana deixo um agradecimento especial pelas contribuições que fizeram para que fosse possível encontrar um direcionamento para a concretização da dissertação.

RESUMO

Relacionar o que acontece nas entrelinhas da Tecnologia da Informação e Comunicação com problemas de privacidade e acesso a dados é complexo, porque os indivíduos as utilizam de forma natural. Talvez por isso seja difícil ter senso crítico sobre os objetivos das empresas responsáveis pelo seu desenvolvimento. A investigação tem relevância porque discorre sobre estudos que abordam questões relacionadas às Tecnologias de Comunicação e Informação, aos Serviços de Redes Sociais Online e à privacidade. É um tema que tem estado em evidência por problemas decorrentes de vazamento, uso indevido e da exposição de dados. Tem-se como objetivo geral a elaboração de uma Revisão Sistemática de Literatura a partir de comunicações científicas que abordem aspectos sobre os Serviços de Redes Sociais Online, a privacidade e os potenciais riscos que afetam os dados dos usuários. Os objetivos específicos foram: a) Coletar informações sobre a privacidade de dados em comunicações científicas que tratam do tema de Serviços de Redes Sociais Online, b) Identificar nas comunicações científicas os principais aspectos teóricos relacionados ao contexto de privacidade de dados c) Elencar os potenciais riscos sobre a privacidade de dados identificados na literatura científica, c) Relacionar os principais riscos sobre a privacidade de dados identificados na Revisão aos grupos e subgrupos descritos na taxonomia da privacidade. O Universo de pesquisa foram as comunicações científicas sobre os Serviços de Redes Sociais Online e a privacidade de dados. Adotou-se como método de pesquisa a Revisão Sistemática de Literatura com a realização de busca nas bases Scientific Electronic Library Online, Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação e a Academic Search Premier. Obteve-se como resultado 331 comunicações científicas submetidas a critérios de inclusão, de exclusão, a leitura para verificação de aderência ao tema totalizando 20 comunicações científicas. Nos resultados qualitativos obteve-se aspectos relacionados aos Serviços de Redes Sociais Online, a privacidade e a potenciais riscos que afetam os dados dos usuários. Destaca-se o papel da Tecnologia da Informação e Comunicação e de dispositivos móveis em problemas de privacidade como: uso prolongado, facilidade de acesso aos Serviços de Redes Sociais Online por meio de *smartphones*. Outro aspecto preocupante é a questão da vigilância tanto realizada por empresas quanto pelos usuários. Essas ocorrências em Serviços de Redes Sociais Online leva a discussão de problemas relacionados a uma sociedade de controle que estabelece por exemplo padrões de beleza. Ações prejudiciais cometidas por meio do uso de múltiplos perfis ou de perfis falsos pelos usuários, ambos associados ao anonimato foi também um aspecto abordado, assim como o uso intenso de Serviços de Redes Sociais Online e o compartilhamento ou recompartilhamento de publicações. Conclui-se que os riscos relacionados aos Serviços de Redes Sociais Online e a privacidade foram o acesso a dados sigilosos, julgamentos, constrangimento, perseguição, descontextualização das publicações, além de exposição de grupos protegidos pela legislação brasileira como no caso de crianças. O uso inconsciente e irreflexivo pelos usuários em ambientes online afeta de forma irreversível sua vida, já que há relatos de casos de suicídios provocados por julgamentos.

Palavras-chave: Serviços de Redes Sociais Online. Redes Sociais Online. Privacidade. Riscos à Privacidade de Dados. Tecnologia de Informação e Comunicação.

ABSTRACT

Relating what happens between the lines of Information and Communication Technology with problems of privacy and access to data is complex because individuals use them naturally. Perhaps that is why it is difficult to have a critical sense of the goals of the companies responsible for its development. The investigation is relevant because it discusses studies that address issues related to Communication and Information Technologies, Online Social Network Services, and privacy. It is a topic that has been in evidence for problems arising from leakage, misuse, and data exposure. The general objective is to prepare a Systematic Literature Review from scientific communications that address aspects of Online Social Networking Services, privacy, and potential risks that affect user data. The specific objectives were: a) Collect information about data privacy in scientific communications that deal with the topic of Online Social Networking Services, b) Identify in scientific communications the main theoretical aspects related to the context of data privacy c) List the potential data privacy risks identified in the scientific literature, c) Relate the leading data privacy risks identified in the Review to the groups and subgroups described in the privacy taxonomy. The research Universe was scientific communications about Online Social Networking Services and data privacy. The Systematic Literature Review was adopted as a research method with a search in the Scientific Electronic Library Online databases, the Reference Database for Articles of Journals in Information Science, and the Academic Search Premier. As a result, 331 scientific communications were submitted to inclusion and exclusion criteria, as well as reading to verify adherence to the theme, totaling 20 scientific communications. In the qualitative results, aspects related to Online Social Networking Services, privacy, and potential risks that affect users' data were obtained. The role of Information and Communication Technology and mobile devices in privacy issues are highlighted, such as prolonged use, and ease of access to Online Social Networking Services through smartphones. Another worrying aspect is the surveillance issue carried out by companies and users. These occurrences in Online Social Networking Services lead to the discussion of problems related to a controlled society that establishes, for example, beauty standards. Crimes committed through the use of multiple profiles or false profiles by users, both associated with anonymity, were also an aspect addressed, as well as the intense use of Online Social Networking Services and the sharing or re-sharing of publications. It is concluded that the risks related to Online Social Networking Services and privacy were access to confidential data, judgments, embarrassment, persecution, decontextualization of publications, in addition to the exposure of groups protected by Brazilian legislation as in the case of children. The unconscious and thoughtless use by users in online environments irreversibly affect their lives, as there are reports of cases of suicides provoked by judgments.

Keywords: Online Social Networking Services. Online Social Networking. Privacy. Risks to Data Privacy. Information and Communication Technology.

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BRAPCI	Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação
CAFe	Comunidade Acadêmica Federada
CI	Ciência da Informação
CMC	Comunicações Mediadas pelo Computador
CPF	Cadastro de Pessoa Física
ASP	*Academic Search Premier*
FN	Feed de Notícias
IBICT	Instituto Brasileiro de Informação em Ciência e Tecnologia
IHC	Interação Humano Computador
LGPD	Lei Geral de Proteção de Dados Pessoais
PDF	*Portable Document Format*
RSL	Revisão sistemática de Literatura
SCIELO	*Scientific Electronic Library Online*
SRSO	Serviços de Redes Sociais Online
TIC	Tecnologia da Informação e Comunicação
UFPR	Universidade Federal do Paraná
UNESCO	*United Nations Educational, Scientific and Cultural Organization*

SUMÁRIO

1 INTRODUÇÃO

O acesso à *Web* e à Internet tem proporcionado à sociedade importantes contribuições quanto à forma como os indivíduos se comunicam em função dos avanços decorrentes da Tecnologia da Informação e Comunicação (TIC).

O avanço das TIC pode ser percebido pelo desenvolvimento, disponibilização e pelo uso de dispositivos móveis, de computadores pessoais, de *tablets* e de outros instrumentos utilizados na Interação Humano Computador (IHC) (BRANCO, BARBAS, 2012). Isso tem gerado uma oportunidade para que os indivíduos fiquem cada vez mais conectados à internet, alterando por vezes padrões de comportamento observados por exemplo na utilização de Serviços de Redes Sociais Online (SRSO).

Príncipe (2013, p. 197) menciona que as TIC têm produzido

> [...] sensíveis alterações nos processos tradicionais de comunicação científica, alterando padrões e comportamentos, introduzindo uma série de mudanças e abordagens, possibilitando novas formas de produção, circulação, disseminação, recuperação e uso da informação - listas de discussão, bibliotecas digitais, laboratórios virtuais, arquivos abertos e, mais recentemente, blogs e redes sociais.

O uso de dispositivos computacionais e móveis permite a interatividade entre os indivíduos que se conhecem tão bem nos dias de hoje. Em sintonia, as interfaces dos dispositivos estariam conectadas aos mais importantes sentidos cognitivos do homem, produzindo vantagens como o reconhecimento parcial da fala, as telas tácteis e os comandos por meio da movimentação dos olhos. Esses tipos de interações proporcionam tanto entretenimento quanto alimentam os dispositivos, que tem como características a mutualidade e simultaneidade dos usuários e de sistemas (LÉVY, 1993).

A sociedade em Rede foi descrita por Castells. Nela os indivíduos se conectam e se desconectam ao mesmo tempo de forma local ou global graças ao que ele considera como a maior invenção das TIC, a internet (CASTELLS, 2018). Neste novo contexto, as empresas que atuam na área de TIC desenvolvem dispositivos móveis cada vez mais sofisticados e criam ambientes como os de SRSO com o objetivo de fomentar a IHC e de oferecer aos indivíduos a possibilidade de formarem redes de relacionamento, denominada por Recuero como redes sociais (RECUERO, 2020).

As empresas são as responsáveis pelos aplicativos de SRSO tais como o *Facebook.* Eles são capazes de promover a interação entre os usuários e a formação d7e redes sociais. Entretanto, os SRSO permitem também atividades de acesso e de coleta de dados por meio de publicações feitas pelos usuários. Normalmente as publicações são constituídas por

textos, imagens e vídeos dos usuários ou de amigos e familiares. O problema é que as empresas têm acesso a dados dos usuários mesmo que não façam parte de sua rede de relacionamento (FELT; EVANS, 2008).

Destaca-se que o problema da privacidade de dados em SRSO pode estar associado ao pouco conhecimento que os indivíduos possuem a respeito de como as TIC funcionam, ou ainda pela oferta de algum tipo de anonimato que as empresas dizem oferecer aos usuários (O USO..., 2013; AFFONSO; SANT'ANA, 2018). O risco decorrente do baixo conhecimento que os indivíduos possuem sobre os SRSO - um produto de TIC - tem levantado problemas de privacidade de dados que ainda não é possível mensurar com assertividade.

Para Roza (2018) este problema tem relação com a excessiva visibilidade que é própria dos SRSO. A visibilidade que torna público os dados pessoais dos usuários possibilita também o compartilhamento de dados com terceiros, levando a ocorrência de potenciais ações de violações de privacidade (BARNES, 2006; FUNG *et al.*, 2010; RODRIGUES; SANT'ANA, 2016; RODRIGUES, 2017).

Neste sentido, é possível definir que os SRSO são ambientes por meio do qual os indivíduos se interrelacionam, produzem, buscam e compartilham dados. As empresas proprietárias de SRSO incentivam os indivíduos a criarem perfis públicos, privados, ou mistos com a intenção de coletar dados, de compartilhar estes dados com agentes externos para oferecer a compra de produtos ou a utilizar serviços ofertados por meio de propagandas veiculadas nos SRSO (BOYD; ELLISON, 2007; GROSS; ACQUISTI, 2005, ; RODRIGUES, 2017).

Em síntese, a pesquisa está nucleada em um contexto de averiguação na literatura científica as informações características ou funcionamento de SRSO, bem como os potenciais riscos para a privacidade relacionados tanto à produção quanto ao compartilhamento de dados a partir do uso de SRSO pelos usuários.

1.1 Problema de pesquisa

O processo de comunicação e de interação entre os indivíduos produzem dados que podem ser tanto quantitativos quanto qualitativos (NOVO; AZEVEDO, 2014). Por exemplo, o peso de um indivíduo (quantitativo) e o estado civil (qualitativo) (BOFF; FORTES; FREITAS, 2018). Um dos ambientes onde há a produção de dados é nos SRSO, considerados por Recuero (2020, p. 102) como "[...] espaços utilizados para a expressão

das redes sociais na Internet". Castells entende, assim, que as redes sociais são teias de relacionamentos sociais que estão em constante expansão (CASTELLS, 2018).

Em uma outra percepção, os SRSO são ambientes onde se coletam dados pessoais. A diferença entre os SRSO e os demais tipos de Comunicações Mediadas pelo Computador (CMC) é a forma com que se expõem os dados dos usuários. Além disso, existe uma outra característica observada nos SRSO que é o compartilhamento de dados, que é próprio dos relacionamentos sociais e fazem parte de toda essa estrutura (RECUERO, 2020; DONEDA, 2012).

Além de serem produzidos e de serem compartilhados, os dados dos usuários são também armazenados em nuvem (RECUERO, 2020, p. 24), ou seja, persistem em data centers, com acesso via internet.

Mesmo que exista uma parcela de usuários com conhecimento sobre os riscos causados à privacidade de dados e mesmo que eles demonstrem ter uma certa preocupação com o que é feito com seus dados, ainda sim, depositam dados de maneira natural quando utilizam os SRSO, tais como o *Facebook* (FONTELES, 2020). Quando um usuário realiza um registro no *Facebook, Instagram* ou *TikTok* e não restringe sua página como privada - o que pode ser feito por meio de ajuste de configuração - acaba permitindo que seus dados publicados em SRSO - fotografias, vídeos, mensagens fiquem visíveis aos demais integrantes de sua rede de relacionamento via interface, bem como a instituições, a empresas, e a governos (BARNES, 2006; DONEDA, 2012; RECUERO, 2020). Isto acontece porque os SRSO possuem uma outra característica que é a exposição pública.

Para Doneda (2012, p. 8)

> [...] o compartilhamento destas informações com terceiros; a exposição destas informações em perfis públicos ou semi-restritos; a sua utilização para a categorização do usuário dentro de um determinado perfil de comportamento e tantas outras modalidades de tratamento possíveis - que não raro extrapolam as possibilidades de tratamento de informações pessoais compartilhadas nas interações sociais tradicionais.

É importante ressaltar que além de coletarem dados as empresas de SRSO coletam também metadados, ou seja, dados adicionais como a georeferenciação[1]. Complementarmente, os dados disponíveis em outros serviços podem ser cruzados, por exemplo, com a localidade que o usuário posta em sua página pessoal. Este recurso é

[1] Processo através do qual algo ou alguém pode ser localizado com base em coordenadas geográficas, especialmente a latitude e a longitude, do lugar onde esse objeto ou pessoa em questão estão.**Geolocalização**. Dicio: dicionário online de português. Disponível em: <https://www.dicio.com.br/geolocalizacao/>. Acesso em: 2 mar. 2022.

utilizado para identificar dados em postagens por meio de *hashtag,* que por sua vez podem ser utilizados em campanhas de marketing (NOVO; AZEVEDO, 2014).

Portanto, os SRSO podem ser ambientes de conflitos de interesse relacionados à privacidade de dados. Primeiro, porque os usuários podem não conhecer as consequências do compartilhamento de dados. As empresas de SRSO disponibilizam os dados coletados dos usuários com agentes externos, que por sua vez comercializam produtos e serviços aos próprios usuários dos SRSO. Esta é uma prática comum nos SRSO e é uma forma das empresas obterem lucro. Segundo, a maioria dos usuários ainda não tem consciência de que os dados produzidos em um SRSO pertençam a si e, com isso, cria-se uma abertura para que as empresas se apropriem dos dados pessoais (DONEDA, 2012; RODRIGUES, 2017; NOVO; AZEVEDO, 2014).

A privacidade vem sendo discutida muito antes da internet, e traz questões relacionadas desde a veiculação de notícias falsas até aspectos ligados a questões de vigilância e a autogestão da privacidade, que consiste no ato de consentir que os dados possam ser utilizados e compartilhados. Com o passar do tempo estas questões se tornaram mais complexas, mesmo porque nos dias atuais o tema tem relação com as TIC (SOLOVE, 2008, 2012).

O crescente uso da internet e de dispositivos móveis no século XX tornou a comunicação entre os indivíduos mais intensa, evidenciando ainda mais os problemas de privacidade. Pariser (2012) detalha, por exemplo, o perigo da identificação de faces humanas em imagens e vídeos. Outro problema originado da relação entre as TIC e a privacidade é o de tentar proteger os dados ao mesmo tempo em que se executa o seu compartilhamento (CHEN; ZHAO, 2012; SOLOVE, 2008). Casos como estes interferem na privacidade dos indivíduos e em especial, na condição do anonimato.

No Brasil, a Lei nº 13.709, de 14 de agosto de 2018, chamada popularmente de Lei Geral de Proteção de Dados Pessoais (LGPD), descreve em seu texto condutas de como os dados pessoais devam ser tratados, estendendo-se também aos meios digitais. A LGPD prevê a proteção de dados tanto de pessoas físicas como de pessoas jurídicas, seja de direito público ou privado (BRASIL, 2018).

Nesta perspectiva, Gross e Acquisti (2005), Mislove (2007), Rodrigues e Sant'Ana (2016) e Kokolakis (2017) relatam outros problemas relacionados aos SRSO e à privacidade, tais como:

- Incentivo à publicação de dados pessoais identificados ou identificáveis (além de dados de contato) que são regularmente fornecidos, juntamente com retratos íntimos da vida social de um indivíduo;
- A visibilidade dos dados pessoais que são variáveis ou seja nos SRSO qualquer membro pode visualizar o perfil de qualquer outro membro;
- Há uma organização de grandes quantidades de dados pessoais em coleções para a realização de comércio eletrônico;
- Existência de exposição pública nas conexões dos usuários, considerado como uma das principais características dos SRSO;
- Empresas privadas são as responsáveis pelo desenvolvimento e pela manutenção dos SRSO. No entanto, seu uso por usuários passou a despertar uma certa preocupação, mesmo porque elas não se limitam apenas a coletar dados dos usuários, mas compartilham os dados com outras empresas, governos e permitem o acesso a dados por outros indivíduos.

Neste sentido, os problemas relacionados à privacidade de dados em SRSO se ampliam e representam possíveis danos aos dados dos usuários. Acrescenta-se que é necessário solucionar os problemas que afetam a privacidade e também é preciso desenvolver conceitos capazes de orientar o desenvolvimento de políticas com as devidas interpretações legais (SOLOVE, 2008).

A análise das questões problematizadas por estes autores evidencia que se trata de um contexto interdisciplinar, no qual dados pessoais armazenados nos SRSO são passíveis de coleta por agentes externos, sendo portanto um fenômeno que pode ser investigado por diferentes prismas. A Ciência da Informação (CI), com seu caráter interdisciplinar e social (SARACEVIC, 1995), é aderente a este contexto, especialmente pelo seu objeto de estudo: dado, informação e conhecimento. A existência de comunicações científicas de distintas áreas do conhecimento precisam ser reunidas, disseminadas e trazidas para reflexão e debate pela CI, já que os SRSO é uma realidade das TIC.

Portanto, o problema desta pesquisa é a dificuldade em identificar os principais elementos teóricos e aspectos relacionados à produção, uso e compartilhamento de dados em SRSO e de seus riscos para a privacidade de dados dos usuários abordados na literatura científica.

1.2 Objetivo

Elaborar uma Revisão sistemática de Literatura (RSL) a partir da análise de comunicações científicas que abordem aspectos sobre os SRSO, a privacidade e os potenciais riscos que afetam a segurança de dados dos usuários.

Os objetivos específicos elaborados para esta pesquisa são:

1. Coletar informações sobre a privacidade de dados em comunicações científicas que tratem do tema de SRSO;
2. Identificar nas comunicações científicas os principais aspectos teóricos relacionados ao contexto de privacidade de dados em SRSO;
3. Elencar os potenciais riscos sobre a privacidade de dados em SRSO identificados na literatura científica;
4. Relacionar os principais riscos sobre a privacidade de dados identificados na RSL aos grupos e subgrupos definidos e descritos na taxonomia da privacidade.

1.3 Justificativa

Pesquisas de Doneda (2012), de Barnes (2006), de Chen e Zhao (2012), de Boff, Fortes e Freitas (2018), Gross e Acquisti (2005), de Novo e Azevedo (2014), de Recuero (2020), de Rodrigues e Sant'Ana (2016), de Rodrigues (2017), de Roza (2018) e de Solove (2008) como tantos outros, destacam aspectos que envolvem o uso de SRSO, do compartilhamento de dados e os problemas sobre a privacidade de dados.

As TIC promovem benefícios à sociedade tais como novas formas de interação, ao mesmo tempo originam problemas como os informacionais, seja por meio da produção excessiva de dados ou pela falta de confiança sobre aquilo que é produzido e disseminado, ou de quais dados podem ser revelados ou mesmo de quem pode ter acesso a eles (CHEN; ZHAO, 2012; ROZA, 2018).

Na visão de Boff, Fortes e Freitas (2018), as TIC não podem ser consideradas como boas ou ruins para a sociedade. Entretanto, a sua utilização exerce um certo controle sobre os indivíduos comparando-se a um panóptico tecnológico. Neste sentido, se estabelece uma situação análoga em que os SRSO podem ser considerados como um tipo de panóptico, pois empresas de SRSO possuem a capacidade vigiar os interesses dos usuários, controlar e manipular dados por meio da utilização de algoritmos, comprometendo a privacidade dos usuários e de seus dados.

Os algoritmos são recursos tecnológicos utilizados por empresas. Eles dão suporte na programação e na execução de atividades em SRSO. Eles são responsáveis por fazerem

a coleta e a decodificação de dados a fim de identificar os gostos e interesses dos usuários (KAUFMAN; SANTAELLA, 2020). Os usuários podem ter seus dados coletados ao acessar, por exemplo, um *web site* em algum buscador na internet a fim de fazer uma reserva em um quarto de hotel para as férias. Isso porque os algoritmos identificam os dados dos usuários e seus interesses baseados em suas pesquisas ou em dados identificáveis no site. Após a identificação dos interesses de conteúdo dos usuários, os algoritmos selecionam e encaminham sites de propagandas de hotéis, bem como de companhias aéreas, restaurantes e locais de passeio.

Para Kaufman e Santaella (2020, p. 8):

> [...] a personalização dos acessos online é resultado de modelos estatísticos (algoritmos de IA) treinados com base nos dados gerados da movimentação dos usuários no ambiente digital, e de arquiteturas "neutras" do ponto de vista ideológico e/ou político e/ou quaisquer outros interesses afora a eficácia dos resultados estimados (agradar os clientes, aumentar a movimentação nas plataformas, gerar mais dados, ampliar o potencial de ganhos financeiros dos controladores das plataformas).

Não há uma definição universal sobre o conceito de privacidade, pois pode significar muitos elementos como, por exemplo, ter liberdade sobre aquilo que se pensa, ou a necessidade de se ficar sozinho ou mesmo de ter controle sobre suas próprias informações (SOLOVE, 2008).

No cenário dos SRSO ninguém consegue estar só, já que são ambientes que permitem conexão com outros usuários. Não há controle sobre os dados pois durante o registro em um SRSO permite-se que os dados sejam compartilhados com terceiros. E talvez ter a liberdade sobre aquilo que se pensa não seja algo tão possível assim. Às vezes tem-se a sensação de que nos SRSO se está até adivinhando o que os usuários estão pensando, pois os algoritmos são acionados para identificar seus gostos e interesses.

Pesquisas confirmam que a vigilância de atividades por empresas e por governos sobre os indivíduos é algo possível. Foi realizada uma pesquisa com cidadãos estadunidenses onde foi constatado que 70% dos entrevistados afirmaram que seus dados estão menos seguros agora do que em cinco anos atrás (AUXIER *et al.*, 2019).

Este tipo de controle é detalhado em pesquisas vinculadas a inúmeras universidades, divulgadas em comunicações científicas, tais como os artigos de periódicos, trazendo como resultados a identificação dos riscos relacionados ao uso de SRSO e a problemas tais como o da privacidade de dados.

Portanto, uma RSL pode minimizar a dispersão destas pesquisas e contribuir com o aumento da visibilidade de pesquisas produzidas no Brasil em diferentes áreas do conhecimento - tais como a Comunicação, o Direito e a CI - além de outras que direcionem suas investigações ao tema de SRSO e os potenciais riscos à privacidade de dados.

Sobre os usuários, dados do Relatório Digital de 2020 elaborado em parceria com *Hootsuite* indica que mais de 4,5 bilhões de indivíduos utilizam a internet. Isto corresponde a aproximadamente 60% da população mundial. Cerca de 3,8 bilhões são usuários de SRSO. Os indivíduos que se conectam à internet por meio de *smartphones* e de outros dispositivos móveis representam aproximadamente 92%. Há também uma expectativa de que estes números nos próximos anos possam crescer, chegando a quase metade da população mundial utilizando a internet (KEMP, 2020).

Um usuário fica conectado à internet em média seis horas e quarenta e três minutos (KEMP, 2020), tempo suficiente para que as empresas de SRSO acionem algoritmos para coletar, armazenar e utilizar os dados pessoais disponibilizados gratuitamente pelos usuários no *Facebook,* que possui 2,5 bilhões de usuários ativos, ou pelo *TikTok*, que tem aproximadamente 800 milhões de usuários. Os dados foram obtidos em pesquisa realizada no ano de 2019 (KEMP, 2020).

No Brasil, segundo dados da Agência Brasil, existem 134 milhões de brasileiros com acesso à internet. Quanto ao uso da conexão e de SRSO têm-se os seguintes dados: aproximadamente 58% dos brasileiros utilizam computador, 90% deles conectam-se todos os dias à internet. As atividades mais executadas pelos usuários são o acesso aos SRSO com 76% e a utilização dos serviços de mensagens instantâneas, com 92% (VALENTE, 2020).

Portanto, observa-se a partir das estatísticas que existe um público cada vez mais conectado, os quais fornecem dados por meio dos SRSO. Contudo, emerge uma preocupação com aquilo que está sendo disponibilizado e utilizado por terceiros, já que os indivíduos ainda não perceberam que os SRSO ficam acessíveis publicamente a qualquer indivíduo com boas ou más intenções e isso consequentemente traz riscos já no momento do registro em um SRSO, uma vez que é necessário realizar o aceite quanto às condições determinadas nos termos de usos das empresas proprietárias de SRSO (RODRIGUES, 2017).

Com o uso da internet e de SRSO cada vez mais comum na sociedade e dos problemas já relatados em comunicações científicas como a de Rodrigues e Sant'Ana (2016) que descreveram os potenciais tipos de riscos para a privacidade de dados a partir dos Termos de Uso disponíveis nos SRSO torna-se relevante realizar uma RSL para identificar nas comunicações científicas outros possíveis riscos causados à privacidade de dados a partir dos SRSO.

A proposta desta investigação é elaborar uma Revisão sistemática de Literatura (RSL) a partir da análise de comunicações científicas que abordem aspectos sobre os SRSO, a privacidade e os potenciais riscos que afetam a segurança de dados dos usuários.

1.4 Estrutura do texto da pesquisa

O texto da pesquisa está estruturado em Seções e Subseções. A Primeira Seção é composta por alguns elementos e segue a respectiva ordem sendo eles: o Problema, os Objetivos, a Justificativa, além da Estrutura da Pesquisa. A Segunda Seção traz os Procedimentos Metodológicos desenvolvidos a fim de direcionar a investigação para o alcance dos objetivos propostos, sendo selecionado para tal uma Revisão Sistemática de Literatura. A Subseção 1 da Segunda Seção traz ainda um quadro síntese com os passos e etapas seguidos no desenvolvimento da RSL. A terceira Seção é formada pelos Resultados Quantitativos, com apresentação de dados obtidos por meio da coleta de dados executada nas três bases de conhecimento sendo elas a Scientific Electronic Library Online (SciELO), Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (BRAPCI) e a Academic Search Premier (ASP-EBSCO). A Quarta Seção está constituída pelo córpus de comunicações científicas identificadas e selecionadas por meio de coleta realizada nas respectivas bases sobre os potenciais riscos que podem comprometer a privacidade dos usuários em SRSO. O córpus de comunicações científicas revisado por meio da RSL foi organizado em Subseções que vai da 4.1 a 4.20. Nestas Subseções foram evidenciados os aspectos teóricos bem como os potenciais riscos sobre a privacidade de dados em SRSO. A Quinta Seção traz a Discussão a partir dos resultados obtidos na RSL, descrevendo alguns dos potenciais riscos relacionados à privacidade. Para complementar a Seção foi elaborado um Quadro Síntese relacionando os potenciais riscos aos Grupos e Subgrupos que integram a Taxonomia da Privacidade (RODRIGUES; SANT'ANA, 2016). Por fim tem-se a Sexta Seção com as Considerações Finais do que foi observado na RSL baseado nos textos e no que foi identificado durante a análise sobre a privacidade de dados e os potenciais riscos para os usuários.

2 PROCEDIMENTOS METODOLÓGICOS

Adotou-se para esta pesquisa a RSL, baseada no *Roadmap* - um guia de fases e de etapas que orienta quanto a realização de pesquisas em áreas do conhecimento tais como as ciências exatas e que também será aplicado na CI (CONFORTO; AMARAL; SILVA, 2011).

Para se obter um embasamento teórico, ou seja, um estado da arte consistente sobre um tema, é necessário planejar e executar algumas etapas como por exemplo as de coleta, de conhecimento, de compreensão, de análise, de sintetização e de avaliação de um conjunto de artigos científicos previamente selecionados (LEVY; ELLIS, 2006).

Entretanto para o desenvolvimento desta pesquisa será utilizado o modelo de Conforto, Amaral e Silva (2011), pois entende-se que as fases e etapas propostas em seu modelo atenderá as necessidades deste estudo pois trata de uma investigação do tipo exploratória que tem como *lócus* de investigação as bases de conhecimento e as comunicações científicas produzidas no Brasil sobre os SRSO.

O modelo de RSL proposto por Conforto, Amaral e Silva (2011) é composto pelas fases de Entrada, de Processamento e de Saída. A Fase de Entrada inclui oito etapas formadas pelo problema de pesquisa, objetivos, fontes primárias, *strings* de busca, critérios de inclusão e de exclusão, critérios de qualificação, método e ferramentas e cronograma.

Adotou-se para a Fase de entrada apenas sete etapas conforme o Quadro 1, pois observa-se que a etapa do problema foi contemplada em um contexto já abordado nesta pesquisa. A Fase de Entrada apresenta os títulos das etapas (numéricos) e a descrição das atividades do roteiro.

Quadro 1 - Fase de Entrada - Roteiro de Atividades da RSL

Etapa	**Roteiro de Atividades**
Etapa 1	Definir as atividades iniciais da RSL que devem estar alinhadas com os objetivos do projeto de pesquisa. As atividades devem ser claras e possíveis de serem executadas.
Etapa 2	Selecionar fontes primárias para a pesquisa que podem ser tanto artigos de periódicos como bases de conhecimento.
	Definir critérios de seleção para as comunicações científicas.
Etapa 3	Definir os termos ou as strings de busca que serão usadas para recuperar as comunicações científicas nas bases de conhecimento. A etapa prevê a realização de um breve estudo a fim de identificar fontes seguras para definição dos termos que podem ser os Tesauros (Vocabulários controlados).
	Aplicar as regras para as strings de busca que corresponde ao uso dos operadores lógicos normalmente utilizados durante as buscas, tanto na avançada quanto na booleana.
	Realizar testes com as strings para verificar a maneira como foram aplicados os termos e os operadores de busca booleana.
	Selecionar as bases de conhecimento como por exemplo a Web of Science. Mas é

Etapa	Roteiro de Atividades
	preciso ter atenção em relação às diferenças apresentadas por cada base em relação à configuração de busca, uso dos operadores booleanos ou aos tipos de filtros disponíveis.
Etapa 4	Elaborar os critérios de inclusão e de exclusão de acordo com os objetivos e campo de investigação. Os critérios de inclusão podem ser as fontes primárias indicadas por especialistas da área, ou que estejam disponíveis em texto completo, ou a quantidade de citações dos artigos de periódicos, por exemplo.
Etapa 5	Estabelecer os critérios para verificar a qualidade das fontes primárias que serão utilizadas.
Etapa 6	Definir um método e ferramentas utilizados na realização das buscas nas bases de conhecimento estabelecendo por exemplo as etapas e critérios que podem ser utilizados.
	Estabelecer os filtros a serem aplicados durante a pesquisa nas bases de conhecimento.
	Elaborar planilhas.
	Adotar software definindo como e onde os dados coletados nas bases de conhecimento serão armazenados e processados. Este processo faz parte da seleção de ferramentas.
Etapa 7	Elaborar um cronograma para a RSL (A média de tempo para a realização da RSL é de 3 a 12 meses dependendo dos objetivos da pesquisa).
	Elencar materiais e software que irão auxiliar no processamento dos dados.

Fonte: Adaptado pela Autora (2022), a partir de Conforto, Amaral e Silva (2011).

Para a primeira etapa da Fase de Entrada estabeleceu-se: i) Identificar e registrar os aspectos teóricos que tratam da privacidade de dados em SRSO, ii) Investigar os potenciais riscos relacionados à privacidade de dados identificados na literatura científica.

Para a segunda etapa da Fase de Entrada utilizou-se como fontes primárias os artigos de periódicos e os anais de congressos. Logo, não são comunicações científicas de interesse desta pesquisa os capítulos de livros ou livros completos, patentes, artigos de revisão, resumos expandidos e outros. Além disso, adotou-se os seguintes critérios para a seleção das fontes, conforme o Quadro 2.

Quadro 2 - Fase de Entrada - Etapa 2 - Critérios para realizar seleção das comunicações científicas nas Bases de Conhecimento

#[2]	Critérios
1	Artigos de periódicos e anais de congressos
2	Idioma das publicações apenas na língua portuguesa
3	Selecionados apenas os que estiverem em texto completo
4	Disponíveis nas bases entre os anos de 2002 a 2020

Fonte: Adaptado pela Autora (2022), a partir de Conforto, Amaral e Silva (2011).

A escolha do quarto critério se justifica em função do primeiro SRSO, com características similares ao que temos atualmente, ter sido lançado no ano de 2002 que foi o *Friendster*, assim muitos outros que vieram depois como Fotolog (2002), MySpace (2003), Orkut (2004), Flickr (2004), *Facebook* (2004) possam ser recuperados durante as buscas nas bases de conhecimento (BRANCO; BARBAS, 2021; RECUERO, 2020).

[2] O símbolo # foi utilizado nos quadros para representar a palavra Ordem.

Na terceira etapa da Fase de Entrada definiu-se as *strings* de busca, ou seja, os termos ou as suas combinações, tendo como instrumento de auxílio a consulta a tesauros. Esta atividade foi necessária para que se tenha um nível de confiabilidade para a pesquisa. Portanto, foram consultados três tesauros: o Thesa, o do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) e o da United Nations Educational, Scientific and Cultural Organization (UNESCO).

O Tesauro Thesa[3] da Ciência da Informação indica, por exemplo, o uso do termo "Mídias Sociais" com a variação de Redes Sociais, trazendo como exemplos o *Facebook* e o *Myspace*. Neste Tesauro não foi retornada durante a busca o termo Site de Rede Social, que é um termo mencionado em publicações como os da Recuero (2020).

O segundo Tesauro consultado foi o do IBICT[4]. Foi realizada novamente a busca do termo "Redes Sociais", cuja nota recuperada indica que sejam "[...] redes formadas por pessoas que trocam informação entre si [...]" (PINHEIRO; FERREZ, 2014, p. 191). Na pesquisa percebeu-se que existe um outro termo indicado para o uso do que são Redes de Comunicação e Informação e que está atrelado às TIC. Uma segunda busca foi realizada, desta vez com o termo "Mídias Sociais", não sendo retornado nenhum resultado.

O terceiro Tesauro consultado foi o da UNESCO[5] retornado durante a verificação o termo "Social networks online" (Redes Sociais Online). Os demais termos adotados por alguns países são "Social Media" (Mídias Sociais) e "Redes Sociais" e equivalem ao mesmo termo.

Em seguida foram elaboradas as *strings* de buscas utilizadas para recuperar nas bases de conhecimento o quantitativo de artigos de periódicos e de anais de congressos para a realização da RSL. Definiu-se portanto que os termos utilizados nas buscas são "Redes Sociais" e "Privacidade" e suas respectivas variações e combinações conforme o Quadro 3. Nas *strings* de busca foi também acrescentado o termo booleano AND.

Quadro 3 - Fase de Entrada - Etapa 3 - *Strings* de Busca utilizadas na pesquisa

#	**Tipo**	***String* de Busca**
1	Redes sociais e variações	Redes sociais online
2		Redes sociais on-line
3		Mídias sociais

[3] THESA: tesauro Semântico Ciência da Informação - #Mídias sociais. Disponível em: https://www.ufrgs.br/tesauros/index.php/thesa/c/19126/64. Acesso em: 20 out. 2021.
[4] PINHEIRO, Lena Vania Ribeiro; FERREZ, Helena Dodd. **Tesauro Brasileiro de Ciência da Informação**. 2014. Disponível em: http://sitehistorico.ibict.br/publicacoes-e-institucionais/tesauro-brasileiro-de-ciencia-da-informacao-1/copy_of_TESAUROCOMPLETOFINALCOMCAPA24102014.pdf>. Acesso em: 3 de jul. 2020.
[5] TESAURO de la UNESCO. Disponível em: http://vocabularies.unesco.org/browser/thesaurus/en/?clang=es. Acesso em: 20 out. 2021.

#	Tipo	*String* de Busca
4	Redes sociais e a combinação com o termo Privacidade	Redes sociais AND privacidade
5		Redes sociais online AND privacidade
6		Redes sociais on-line AND privacidade
7		Mídias sociais AND privacidade

Fonte: Autora (2022).

As bases de conhecimento selecionadas para esta pesquisa foram a Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (BRAPCI)[6], base de conhecimento que tem por princípio o Open Access, ou seja a disponibilização de forma livre na internet de comunicações científicas em texto completo. A Academic Search Premier - ASP (EBSCO)[7], disponível para as instituições assinantes do Portal de Periódico Capes e respectivos usuários. E a Scientific Electronic Library Online (SciELO)[8], também com Open Acess. Depois da seleção das bases, houve a realização de pré-testes com as *strings* de busca conforme as Figuras 1, 2 e 3.

A Figura 1 apresenta a interface inicial de pesquisa da BRAPCI, onde se utilizou da delimitação de busca entre os anos de 2002 a 2020, pesquisa no texto completo, ordenados por relevância. Foram recuperadas 617 comunicações científicas. As setas em vermelho indicam as personalizações utilizadas na busca, bem como o botão de pesquisa.

[6] **Brapci - Base de Dados em Ciência da Informação**. Disponível em: <https://www.brapci.inf.br/>. Acesso em: 14 out. 2021.
[7] **EBSCOhost**. Disponível em: <https://web-b-ebscohost.ez3.periodicos.capes.gov.br/ehost/search/basic?vid=0&sid=dfc41470-add5-4bb1-8e21-a3c8d30d6f41%40sessionmgr102>. Acesso em: 14 out. 2021.
[8] **SciELO.org**. Disponível em: <https://www.scielo.org/>. Acesso em: 14 out. 2021.

Figura 1 - Exemplo de pré-teste com as strings de busca realizada na Base de Conhecimento BRAPCI.

Fonte: Elaborado pela Autora (2022), a partir de BRAPCI (2021).

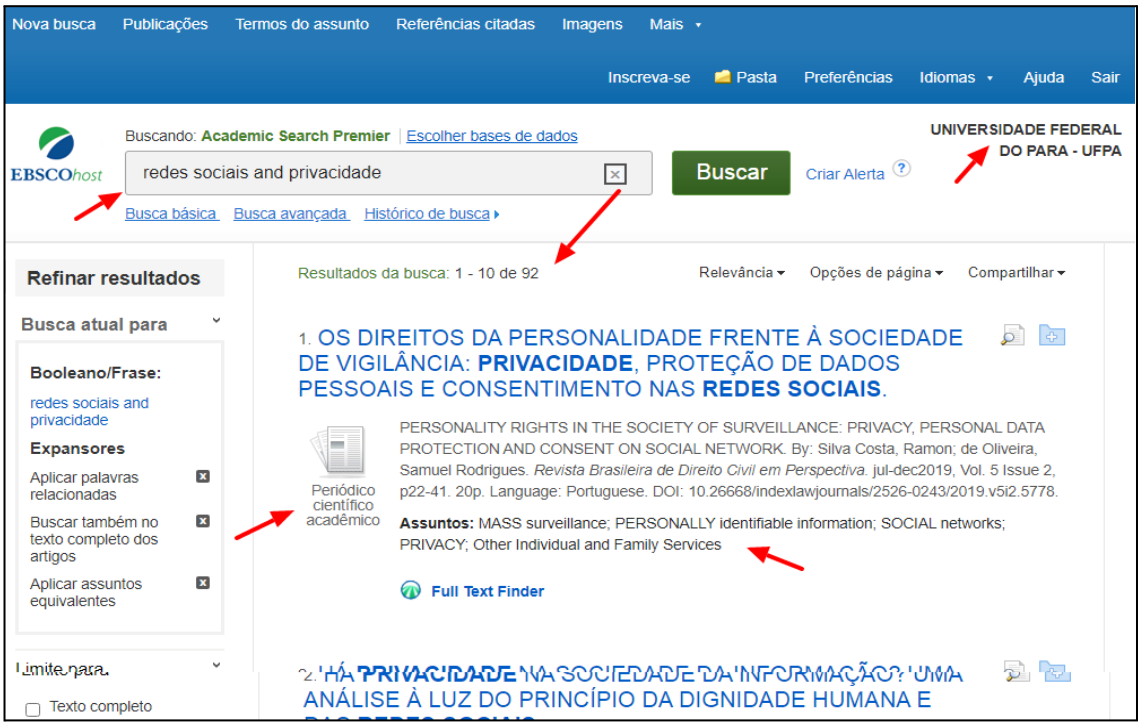
A Figura 2 apresenta o processo de busca na SciELO por resultados para a delimitação da busca entre os anos 2002 e 2020, ordenados por relevância. Foram filtradas 16 comunicações científicas. As setas em vermelho indicam as personalizações utilizadas na busca, bem como o botão de busca.

Figura 2 - Exemplo de pré-teste com as strings de busca realizada na Base de Conhecimento SciELO.

Fonte: Elaborado pela Autora (2022), a partir de SciELO (2021).

A Figura 3 apresenta o processo de busca no EBSCOhostt, por resultados para a delimitação da busca entre os anos 2002 e 2020, ordenados por relevância. Foram filtradas 16 comunicações científicas. As setas em vermelho indicam as personalizações utilizadas na busca. No caso, foi realizado o login institucional pela conta da Universidade Federal do Pará, já que é uma base de conhecimento com acesso pago.

Figura 3 - Exemplo de pré-teste com as strings de busca realizada na Base de Conhecimento EBSCOhost.



Fonte: Elaborado pela Autora (2022), a partir de EBSCOhost (2021).

A quarta etapa da Fase de Entrada consistiu na elaboração de critérios de inclusão e de exclusão conforme o Quadro 4. Os critérios de inclusão foram formulados para delimitar por exemplo os tipos de fontes primárias recuperadas: artigos e anais de congressos. A formulação dos critérios é para atender tanto aos objetivos da pesquisa quanto para recuperar as comunicações científicas que estejam alinhadas ao tema. Os critérios de exclusão foram elaborados com a finalidade de serem parâmetro para o descarte de comunicações científicas recuperadas nas bases de conhecimento, mas que não serão utilizadas nesta investigação por não atender por exemplo a aderência ao tema.

Quadro 4 - Fase de Entrada - Etapa 4 - Definição dos critérios de inclusão e de exclusão

#	Tipo de Critério	Descrição do Critério
1	Inclusão	As fontes primárias serão somente os artigos de periódicos e anais de congressos.
2		Disponibilizados em texto completo nas bases de conhecimento.

#	Tipo de Critério	Descrição do Critério
3		Produzidos no idioma da língua portuguesa.
4		Os artigos de periódicos e de anais de congressos 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.
5		Os artigos e anais de congressos vinculados ao Open Access tem por princípio a disponibilização de artigos de forma livre na internet. Os periódicos neste formato têm um nível de exigência para a submissão de produções semelhantes aos periódicos tradicionais, ou seja, os adquiridos por assinatura (O que…., 2021). O segundo recurso é recuperar os artigos e anais de congressos que estejam disponíveis para acesso via Rede Comunidade Acadêmica Federada (CAFe).
6	Exclusão	Os artigos de periódicos e de anais de congresso duplicados nas bases de conhecimento.
7		Os artigos e anais de congressos que sejam uma RSL.
8		Os textos que não tenham aderência com o tema investigado, sendo para isso adotada como estratégia a leitura técnica de alguns elementos presentes nos textos tais como título, resumo, quando houver, e na ausência deste a leitura técnica dos dois primeiros parágrafos da introdução, das palavras-chave, bem como das considerações finais. Após a verificação, os artigos e anais de congressos em que não se observe aderência com o foco da investigação não serão considerados para a RSL.

Fonte: Autora (2022).

Na quinta etapa da Fase de Entrada, adotou-se como critério de qualidade para os artigos de periódicos o estrato Qualis[9]. A última classificação dos estratos dos periódicos em vigor é a do quadriênio 2013 - 2016. Portanto, foram considerados para análise os artigos indexados em periódicos com estrato QUALIS igual ou superior a B2 (PLATAFORMA …, 2021), pois quanto mais próximo do estrato A1 mais qualidade terão os artigos revisados.

Quanto aos anais de congressos foram considerados para a RSL apenas aqueles realizados a nível nacional ou regional. Os anais de congressos locais foram desconsiderados para esta investigação.

Na sexta etapa da Fase de Entrada aplicar-se-á os filtros para a realização das buscas nas bases de conhecimento. O “Filtro 1” tem por objetivo recuperar apenas os textos em língua portuguesa, enquanto que o “Filtro 2” foi aplicado para recuperar as comunicações científicas no intervalo de tempo entre 2002 a 2020. Por fim, o "Filtro 3” foi

[9] A Plataforma Sucupira é utilizada para fins de classificação da produção científica nacional, especialmente os periódicos onde os artigos são indexados. Os periódicos podem ser avaliados e classificados em oito estratos, que variam de A1 a C, de acordo com o Quadriênio 2013 a 2016. PLATAFORMA Sucupira. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsf. Acesso em: 15 out. 2021.

aplicado para recuperar os artigos de periódicos e os anais de congressos disponibilizados em texto completo.

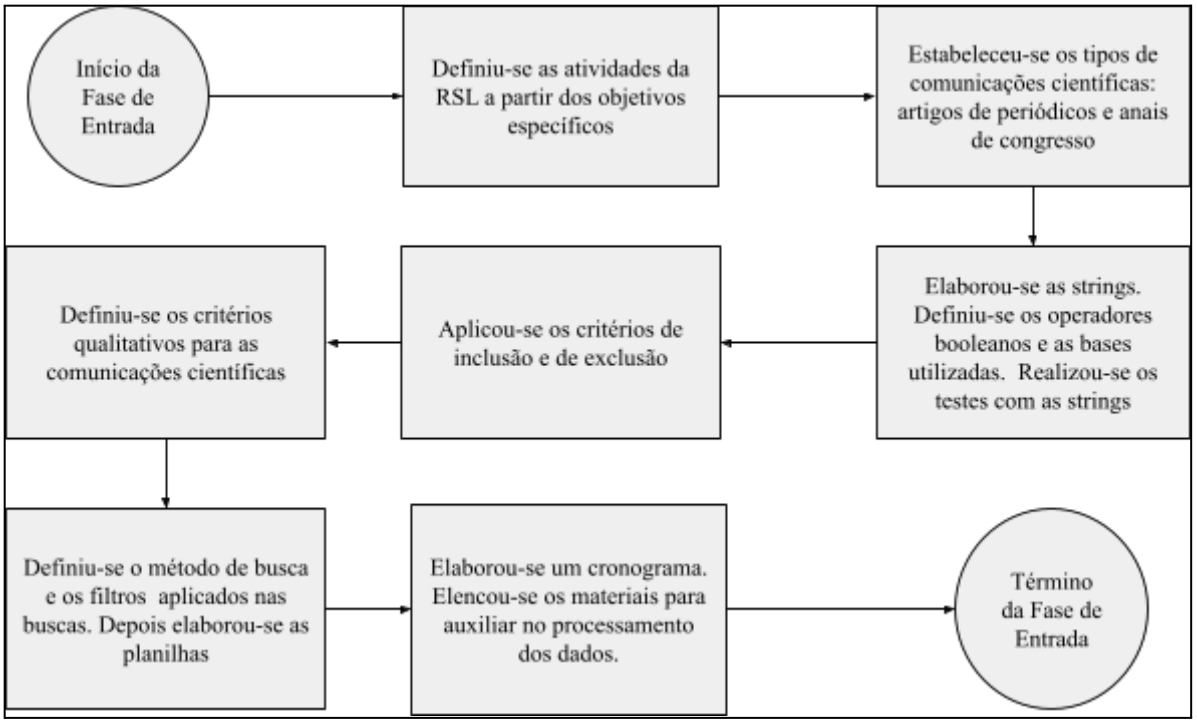
Destaca-se que a base de conhecimento SciELO não apresenta a opção para aplicação de filtro para texto completo. Entretanto, em sua página há informações que garantem que as comunicações estão disponibilizadas em texto completo ou não - esta informação será utilizada para a filtragem, de forma manual.

Posteriormente serão elaboradas planilhas eletrônicas[10] contendo os dados e os metadados dos artigos e dos anais de congressos recuperados nas bases de conhecimento. Os dados das planilhas contêm a data da coleta, o termo utilizado na recuperação, a ordem de classificação, os nomes e sobrenomes dos autores, título da comunicação científica, título do periódico, título dos anais de congresso, ano de publicação, número, volume, palavras-chave, resumo, quantidade de citações, *hyperlink* para o acesso ao texto completo, base de conhecimento e o critério de qualidade adotado nesta RSL, que é o estrato Qualis.

A sétima etapa da Fase de Entrada consistirá na realização de um levantamento para identificar os materiais que serão utilizados no processamento dos dados. Este instrumento é necessário para saber por exemplo se um artigo de periódico encontra-se duplicado nas bases de conhecimento. Em seguida foi elaborado um fluxograma como observa-se na Figura 4, cuja sintetiza as sete etapas da Fase de Entrada para a RSL.

[10] A planilha eletrônica foi elaborada por meio do Google Workspace, antigo *G-Suite,* um aplicativo utilizado para fins de produção e de colaboração. **Google Workspace: Apps empresariais e ferramentas de colaboração**. Disponível em: https://workspace.google.com/intl/pt-BR/. Acesso em: 7 jun. 2022.

Figura 4 - Etapas realizadas para a Fase de Entrada da RSL



Fonte: Autora (2022).

Outra atividade prevista para a sétima etapa da Fase de Entrada foi a organização de um cronograma, que demonstra a sequência de desenvolvimento de cada Fase, etapas e atividades planejadas para a RSL, conforme pode ser verificado no Quadro 5.

Quadro 5 - Cronograma de execução das 3 Fases da RSL

Fase	**Etapa**	**Atividade**	**Sequência de Desenvolvimento**			
			1	**2**	**3**	**4**
Entrada	1	Definição dos objetivos.	x			
	2	Definir os tipos das fontes primárias utilizadas	x			
	3	Definição das Strings de busca.	x			
	4	Estabelecimento dos critérios de inclusão e de exclusão.	x			
	5	Definir os critérios de qualidade dos artigos e dos anais de congressos.	x			
	6	Definição dos filtros de busca. Elaboração de planilhas no *G-Suíte.*	x	x	x	
	7	Elaboração de cronograma e identificação dos materiais.	x			
Processa-mento	1	Execução das buscas e adequação das *Strings* de busca.	x	x	x	
	2	Leitura e análise dos artigos de periódicos e dos anais de congressos.		x	x	
	3	Organização da documentação e compilação dos dados obtidos nas planilhas do *G- Suíte.*		x		
Saída	1	Arquivamento em *software Zotero* dos artigos e anais selecionados.		x		
	2	Síntese sobre os SRSO e os riscos referentes à privacidade de dados.			x	x
	3	Formulação dos resultados.				x

Fonte: Autora (2022).

No Quadro 6 visualiza-se as etapas da Fase de Processamento composta pela Busca, Análise e Documentação. A etapa de busca é realizada com o auxílio das *strings,* tendo o pesquisador a possibilidade de recuperar as comunicações científicas de seu interesse. Por fim, recomenda-se fazer a busca cruzada, ou seja, os autores não recuperados nas buscas, mas que foram citados nos textos analisados podem ser incluídos na RSL (CONFORTO; AMARAL; SILVA, 2011), o que não foi adotado nesta investigação.

Quadro 6 - Etapas da Fase de Processamento da RSL

Etapa	**Roteiro de Atividades**
Etapa 1	Realizar as buscas das comunicações científicas nas bases de conhecimento selecionadas utilizando-se as strings de busca. Tem-se também a opção de fazer uma busca cruzada.
Etapa 2	Registrar os dados e metadados referentes às comunicações científicas recuperadas nas bases de conhecimento, contabilizando também as duplicadas, as analisadas e as não analisadas, ou seja tudo deve estar devidamente documentado.
Etapa 3	Realizar a leitura das comunicações científicas que se fará por meio de três estágios. Estágio 1 - título, palavras-chaves e resumo; ii) Estágio 2 - Introdução e considerações; iii) Estágio 3 - Texto completo. Analisar os aspectos relativos ao tema identificados na leitura dos textos.

Fonte: Adaptado pela Autora (2022), a partir de Conforto, Amaral e Silva (2006).

Na primeira etapa da Fase de Processamento executar-se-á as buscas nas bases SciELO, Brapci e EBSCOhost. Nesta etapa serão utilizadas as strings de busca, sendo necessário fazer adaptações em relação àquilo que foi programado inicialmente, uma vez que cada base de conhecimento apresenta uma estrutura um pouco diferente uma das outras.

Na segunda etapa da Fase de Processamento os dados e metadados de cada artigo e anais de congressos recuperados nas citadas bases de conhecimento serão registrados em planilha, 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[11]. Os demais dados registrados foram os totais de:

- Artigos de periódicos e anais de congressos;
- Tipo de comunicação científica;
- Duplicados;
- Descartados que não atenderam aos critérios de inclusão;

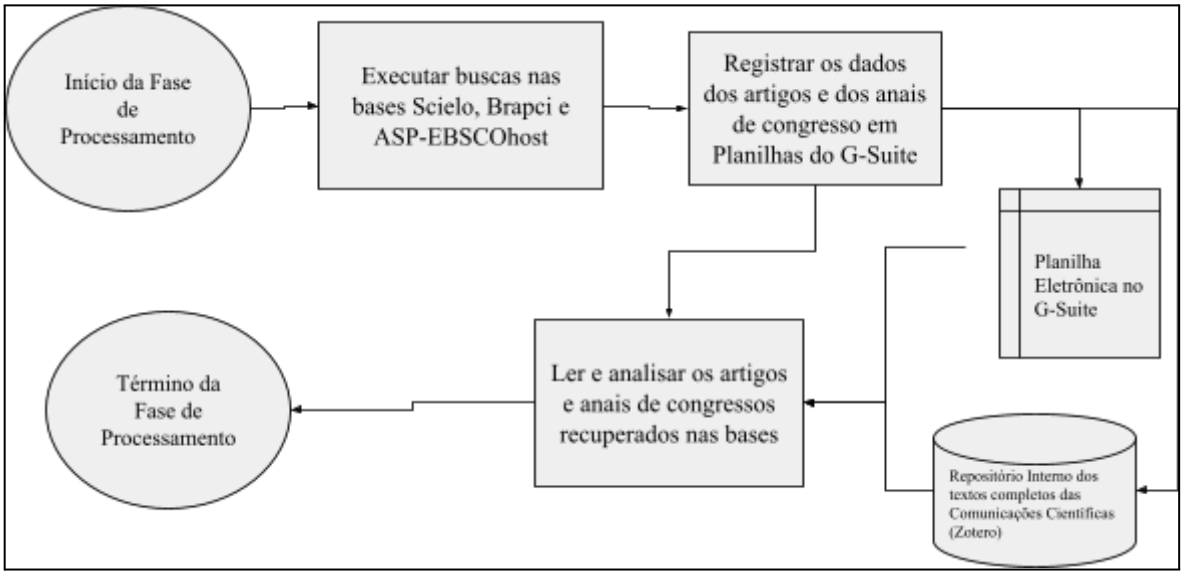
[11] A Plataforma Sucupira foi a fonte de consulta utilizada para verificação do estrato Qualis dos artigos em periódicos. PLATAFORMA Sucupira. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsf. Acesso em: 15 out. 2021.

A terceira etapa da Fase de Processamento constitui-se pela leitura e análise dos artigos de periódicos e anais de congressos registrados nas planilhas. Conforto, Amaral e Silva (2011) orientam que a leitura das comunicações científicas seja realizada a partir de elementos básicos tais como o título, resumo e palavras-chave. Quando não for identificado nesses elementos indícios sobre o tema que se está investigando, então a leitura deverá estender-se a outros elementos tais como a introdução, considerações, ou o texto completo (CONFORTO; AMARAL; SILVA, 2011).

Assim, optou-se por realizar a leitura dos artigos e anais de congresso como forma de identificar as comunicações científicas que têm aderência ao tema investigado sobre os SRSO e a privacidade de dados. A leitura foi dividida em 3 estágios: i) Estágio 1 - título, palavras-chaves e resumo; ii) Estágio 2 - Introdução e considerações; iii) Estágio 3 - Texto completo.

A seguir, foi elaborado um fluxograma que representa a Fase de Processamento, contendo as três etapas utilizadas nesta RSL como se pode observar na Figura 5.

Figura 5 - Etapas realizadas para a Fase de Processamento da RSL



Fonte: Autora (2022).

A Fase de Saída, Quadro 7 no modelo de Conforto, Amaral e Silva (2011) constitui-se pelas etapas de gerenciamento de alerta, cadastro e arquivo, síntese e resultados e modelos teóricos.

A etapa de gerenciamento de alerta é um tipo de serviço comumente oferecido por bases de conhecimento e tem por objetivo informar ao pesquisador sobre a disponibilização de novos artigos produzidos sobre o tema. No entanto esta etapa não será adotada para esta RSL.

Quadro 7 - Etapas da Fase de Saída da RSL

Etapa	Roteiro de Atividades
1	Cadastrar e arquivar as comunicações científicas
2	Sintetizar os estudos analisados
3	Formular os resultados

Fonte: Adaptado pela Autora (2022), a partir de Conforto, Amaral e Silva (2006).

Assim, a primeira etapa da Fase de Saída desta RSL compreende o cadastro e arquivo dos artigos de periódicos e dos anais de congressos selecionados na análise. Posteriormente, os arquivos em *Portable Document Format* (PDF) foram armazenados no Zotero, software[12] utilizado para organizar e elaborar as referências em vários formatos, inclusive o da Associação Brasileira de Normas Técnicas (ABNT).

A segunda etapa da Fase de Saída consistirá em produzir uma síntese a partir dos estudos analisados. Como parâmetro para o desenvolvimento da síntese da investigação utilizou-se os objetivos específicos que prevê identificar aspectos teóricos sobre SRSO, elencando-se também os principais riscos relacionados à privacidade de dados identificados nesta investigação.

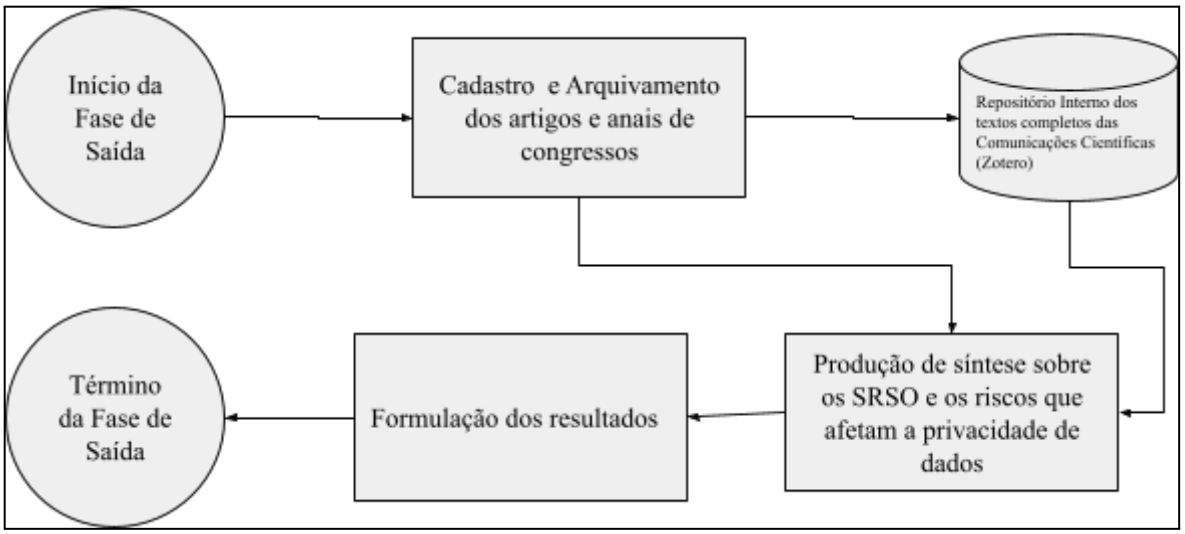
Neste caso, não será utilizado nenhum tipo de métrica tais como a quantidade de citações ou índice de performance para fins de identificação. Nesta investigação utilizar-se-á apenas a técnica de leitura de conteúdo das comunicações científicas, de forma minuciosa, identificando-se os objetivos, tema, características dos SRSO e possíveis potenciais riscos.

Por fim, os principais riscos identificados serão cruzados com os grupos e subgrupos descritos no estudo de Rodrigues e Sant'Ana (2017), que trata da Taxonomia da Privacidade. Cada potencial risco identificado sobre a privacidade de dados será analisado e relacionado a um grupo e subgrupo conforme as características apresentadas.

Para a terceira etapa da Fase de Saída serão formulados os resultados acerca dos SRSO e os potenciais riscos identificados e analisados nesta investigação. Além disso, somar-se-á aos estudos existentes uma contribuição teórica sobre o tema, evidenciando também lacunas que podem ser objetos de futuras pesquisas na CI.

[12] O Zotero é um software *Open Access* utilizado para organizar e armazenar as comunicações científicas, além de ser possível também elaborar as referências. **Zotero:** your personal research assistant. Disponível em: https://www.zotero.org/. Acesso em: 15 out. 2021.

Figura 6 - Fluxograma das Etapas da Fase de Saída da RSL



Fonte: Autora (2022).

Finalizando a Fase de Saída, elaborou-se um fluxograma para demonstrar a sequência das atividades realizadas que levam à conclusão desta RSL, conforme verifica-se na Figura 6.

2.1 Síntese da aplicação do Método de RSL e dos materiais utilizados

Esta subseção apresenta uma síntese das atividades realizadas em cada etapa de cada Fase bem como os resultados esperados a partir de sua aplicação. Destaca-se que a Etapa problema da Fase de Entrada, assim como a etapa de gerenciamento de alerta da Fase de Processamento presentes no modelo de RSL de Conforto, Amaral e Silva (2011) não foram aplicadas nesta RSL.

Na Fase de Entrada, a etapa objetivos trará como resultado a identificação dos aspectos teóricos e os riscos referentes à privacidade de dados em SRSO. Já a etapa de seleção relativa a escolha das fontes primárias trará como resultado a identificação de artigos e de anais de congressos produzidos no Brasil que abordam a temática de SRSO. A etapa de definição das strings será relevante para encontrar os termos e suas composições que auxiliaram para recuperar os artigos e os anais de congressos.

A aplicação dos critérios de inclusão e de exclusão da quarta etapa, bem como o critério de qualidade, e a aplicação dos filtros nas bases de conhecimento que correspondem respectivamente a quinta e a sexta etapa resultará em uma seleção mais rigorosa do quantitativo de artigos de periódicos e de anais de congressos recuperados nas bases *SciELO, BRAPCI e* EBSCOhost. Além disso, a última etapa da Fase de Entrada representada em forma de cronograma guia o pesquisador a executar em sequência todas as atividades previstas nas Fases de Entrada, Processamento e de Saída.

A etapa de busca da Fase de Processamento deve ter como resultado a recuperação dos artigos e de anais de congressos sobre o tema de SRSO e privacidade de dados. Já a etapa de leitura e análise permitiu identificar nos textos recuperados aspectos teóricos e os riscos que afetam a privacidade de dados. Por fim, a etapa da documentação permitirá organizar e registrar em planilhas os dados e metadados das comunicações científicas, resultando no controle quantitativo sobre os tipos de comunicações científicas que foram analisadas.

Na Fase de Saída, a etapa de cadastro e arquivamento resultará na inserção dos artigos e anais de congressos em *software* e na geração de referências dos textos analisados, uma vez que estes devem compor a lista de referência desta pesquisa.

Quadro 8 - Materiais utilizados para a RSL

RSL		**Materiais utilizados**	**Resultados**
Fase	**Etapa**		
Entrada	1	NA[1]	NA[1]
	2	Tesauros	Definição das strings de buscas.
	3	NA[1]	NA[1]
	4	Plataforma Sucupira	Identificação do estrato Qualis dos periódicos onde os artigos foram publicados
	5	*Google G-Suite*	Elaboração de planilha eletrônica no *G-Suite.*
	6	NA[1]	NA[1]
Processamento	1	*SciELO, BRAPCI e* EBSCOhost	Recuperação dos artigos e anais de congressos nas bases de conhecimento.
	2	Computador com acesso a internet	Leitura e análise dos artigos em periódicos e dos anais de congressos.
	3	Planilhas eletrônicas.	Controlar e registrar dados e metadados dos artigos e anais de congressos recuperados nas bases de conhecimento.
Saída	1	*Software Zotero,* gerenciador de referências	Cadastro e armazenamento dos artigos e anais de congressos. Pasta organizada no Gerenciador de Referências, contendo as referências e os documentos digitais das Comunicações Científicas.
	2	*Google G-Suite*	Registro da síntese sobre o tema SRSO e os potenciais riscos que afetam a privacidade de dados.
	3	*Google G-Suite*	Registro dos resultados.

Legenda: [1] NA = Não se Aplica.
Fonte: Autora (2022).

A etapa de síntese da Fase de Saída produzirá como resultado uma amostra da literatura científica produzida no Brasil de aspectos teóricos sobre a privacidade de dados e os potenciais riscos decorrentes do uso de SRSO, atendendo portanto aos objetivos desta RSL. Para finalizar, o Quadro 8 contém os materiais utilizados bem como os resultados esperados a partir do uso do modelo da RSL proposta nesta pesquisa.

3 REVISÃO SISTEMÁTICA DE LITERATURA - ANÁLISE QUANTITATIVA

As Etapas da RSL, especialmente a de Entrada e a de Processamento contribuíram para a formação de dados e de metadados. Os dados e metadados obtidos a partir das Etapas foram organizados, registrados e submetidos à análise, obtendo-se como resultados quantitativos desta seção 23 dimensões, ordenadas a seguir:

1. Quantidade de comunicações científicas analisadas e descartadas, segmentadas por Base de Conhecimento, em valores absolutos e percentuais;
2. Quantidade de comunicações científicas recuperadas para as strings, segmentadas por String, em valores absolutos e percentuais;
3. Total de ocorrências de comunicações científicas, segmentadas por base de conhecimento, incluindo comunicações científicas descartadas na análise, em valores absolutos;
4. Total de ocorrências de tipos de comunicações científicas, segmentadas por base de conhecimento, incluindo comunicações científicas totais (sem recorte) e descartadas na análise (com recorte), em valores absolutos e em percentuais;
5. Total de ocorrências de tipos de comunicações científicas, segmentadas por string, incluindo comunicações científicas totais (sem recorte) e descartadas na análise (com recorte), em valores absolutos e em percentuais;
6. Total de ocorrências de autores, segmentadas por base de conhecimento, incluindo autores descartados na análise, em valores absolutos;
7. Total de ocorrências de autores, segmentadas por string, incluindo autores descartados na análise, em valores absolutos;
8. Total de ocorrências de periódicos e anais de congresso, segmentados por Base de Conhecimento, incluindo comunicações científicas descartadas na análise, em valores absolutos;
9. Total de ocorrências de periódicos e anais de congresso, segmentados por string, incluindo comunicações científicas descartadas na análise, em valores absolutos;
10. Total de ocorrências de estratos QUALIS da CAPES, segmentados por Base de Conhecimento, incluindo comunicações científicas descartadas na análise, em valores absolutos;
11. Total de ocorrências de estratos QUALIS da CAPES, segmentados por Base de Conhecimento, excluindo as comunicações científicas descartadas na análise, em valores absolutos;

12. Total de ocorrências de estratos QUALIS da CAPES, segmentados por string, incluindo comunicações científicas descartadas na análise, em valores absolutos;
13. Total de ocorrências de estratos QUALIS da CAPES, segmentados por string, excluindo as comunicações científicas descartadas na análise, em valores absolutos;
14. Total de ocorrências de comunicações científicas, segmentados por ano e por Base de Conhecimento, incluindo as comunicações científicas descartadas na análise, em valores absolutos;
15. Total de ocorrências de comunicações científicas, segmentados por ano e por Base de Conhecimento, excluindo as comunicações científicas descartadas na análise, em valores absolutos;
16. Total de ocorrências de comunicações científicas, segmentados por ano e por string, incluindo as comunicações científicas descartadas na análise, em valores absolutos;
17. Total de ocorrências de comunicações científicas, segmentados por ano e por string, excluindo as comunicações científicas descartadas na análise, em valores absolutos;
18. Total de ocorrências de tipos de comunicações científicas, segmentados por ano e por tipo de comunicação científica, incluindo as comunicações científicas descartadas na análise, em valores absolutos;
19. Total de ocorrências de tipos de comunicações científicas, segmentados por ano e por tipo de comunicação científica, excluindo as comunicações científicas descartadas na análise, em valores absolutos;
20. Total de ocorrências de palavras-chave, segmentados por Base de Conhecimento, incluindo as comunicações científicas descartadas na análise, em valores absolutos;
21. Total de ocorrências de palavras-chave, segmentados por Base de Conhecimento, excluindo as comunicações científicas descartadas na análise, em valores absolutos;
22. Total de ocorrências de palavras-chave, segmentados por string, incluindo as comunicações científicas descartadas na análise, em valores absolutos;
23. Total de ocorrências de palavras-chave, segmentados por string, excluindo as comunicações científicas descartadas na análise, em valores absolutos

A busca por comunicações científicas sobre SRSO e a privacidade foi realizada em três bases de conhecimento: a BRAPCI, a SciELO e a EBSCOhost, conforme mencionado na Seção 2, dos Procedimentos Metodológicos, resultando em um quantitativo de 331 comunicações científicas. Destas, apenas 20 foram revisadas. A realização das buscas compreende o período entre 10 de novembro de 2021 a 13 de dezembro de 2021.

A partir da coleta de dados (Tabela 1) identificou-se que a base de conhecimento com maior ocorrência de comunicações científicas analisadas foi a EBSCOhost, seguida da SciELO. Nota-se que a Brapci teve apenas uma ocorrência. Isto pode indicar que os pesquisadores da CI têm uma baixa produção em relação à temática investigada. Entretanto há necessidade de realização de investigações em outras bases de conhecimento que corroborem ou não com este resultado.

Foram selecionadas um total de 20 comunicações científicas para a análise. Tal resultado é reflexo da aplicação dos critérios de exclusão tais como idioma, aderência ao tema ou ainda a seleção baseada no estrato Qualis dos periódicos. 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.

Tabela 1 - Quantidade de comunicações científicas analisadas e descartadas, segmentadas por Base de Conhecimento, em valores absolutos e percentuais.

Base de Conhecimento	**Quantidade de Com. Científicas Analisadas**	**Quantidade de Com. Científicas Descartadas**	**Total**		**Quantidade de Com. Científicas Analisadas (em %)**	**Quantidade de Com. Científicas Descartadas (em %)**
BRAPCI	1	55	56		1,79%	98,21%
EBSCOhost	11	130	141		7,80%	92,20%
SciELO	8	126	134		5,97%	94,03%
Total	**20**	**311**	**331**		**6,04%**	**93,96%**

Fonte: Autora (2022).

Com relação às strings utilizadas, a Tabela 2 exibe as três bases de conhecimento, com a ordem das strings em que foram realizadas as buscas. Em ordem, as strings com o maior quantitativo de comunicações científicas recuperadas foram “Mídias sociais” com (115) ocorrências, seguida de “Redes sociais AND privacidade” com (87) ocorrências, “Redes sociais online” com (76) ocorrências e “Redes sociais online AND privacidade” com (12) ocorrências. As demais strings “Redes sociais on-line AND privacidade” e "Mídias sociais AND privacidade” tiveram respectivamente (6) e (2) ocorrências.

Em relação às Bases de Conhecimento, a quantidade de comunicações científicas recuperadas na BRAPCI com as strings de “Mídias sociais” foi de (0) ocorrências; "Mídias sociais AND privacidade” com (1) ocorrência; “Redes sociais AND privacidade” com (7) ocorrências; “Redes sociais on-line com (11) ocorrências; “Redes sociais on-line AND privacidade com (3) ocorrências; “Redes sociais online” com (26) ocorrências; “Redes

sociais online AND privacidade com (8) ocorrências, totalizando 56 comunicações científicas recuperadas.

Na SciELO obteve-se as seguintes ocorrências: “Mídias sociais” com (110) ocorrências; "Mídias sociais AND privacidade” com (1) ocorrência; “Redes sociais AND privacidade” com (11) ocorrências; “Redes sociais on-line” com (4) ocorrências; “Redes sociais on-line AND privacidade” com (0) ocorrências; “Redes sociais online” com (8) ocorrências; “Redes sociais online AND privacidade” com (0) ocorrências, totalizando 134 comunicações científicas recuperadas na base.

Na EBSCOhost os resultados foram: “Mídias sociais” com (5) ocorrências; "Mídias sociais AND privacidade” com (0) ocorrência; “Redes sociais AND privacidade” com (69) ocorrências; “Redes sociais on-line” com (18) ocorrências; “Redes sociais on-line AND privacidade” com (3) ocorrências; “Redes sociais online” com (42) ocorrências; “Redes sociais online AND privacidade” com (4) ocorrências, totalizando 141 comunicações científicas recuperadas na EBSCOhost.

O resultado demonstra que existe uma diversidade de termos utilizados por pesquisadores em suas respectivas comunicações científicas para se referir ao tema de SRSO. Não é possível até o momento definir exatamente qual (is) o (s) termo (s) mais adequado (s) a ser adotado pelos pesquisadores. Entretanto, é preciso chegar a um consenso e minimizar a quantidade de termos utilizados, uma vez que isso implica diretamente na recuperação das comunicações científicas nas bases de conhecimento e cria dificuldades ao pesquisador.

Tabela 2 - Quantidade de comunicações científicas recuperadas para as strings, segmentadas por String, em valores absolutos e percentuais.

String	BRAPCI	SciELO	EBSCOhost	Total de Com. Científicas	BRAPCI (em %)	SciELO (em %)	EBSCOhost (em %)
Mídias sociais	0	110	5	**115**	0,00%	95,65%	4,35%
Mídias sociais AND privacidade	1	1	0	**2**	50,00%	50,00%	0,00%
Redes sociais AND privacidade	7	11	69	**87**	8,05%	12,64%	79,31%
Redes sociais on-line	11	4	18	**33**	33,33%	12,12%	54,55%
Redes sociais on-line AND privacidade	3	0	3	**6**	50,00%	0,00%	50,00%
Redes sociais online	26	8	42	**76**	34,21%	10,53%	55,26%
Redes sociais	8	0	4	**12**	66,67%	0,00%	33,33%

String	BRAPCI	SciELO	EBSCOhost	Total de Com. Científicas		BRAPCI (em %)	SciELO (em %)	EBSCOhost (em %)
online AND privacidade								
Total de Com. Científicas	**56**	**134**	**141**	**331**		**16,92%**	**40,48%**	**42,60%**

Fonte: Autora (2022).

Na Tabela 3 (Apêndice A) tem-se a relação das comunicações científicas ordenadas pelo número de ocorrências por base de conhecimento. A base com maior ocorrência total de títulos duplicados foi a EBSCOhost com (5) ocorrências. As bases com menores ocorrências foram a SciELO e a BRAPCI com (2) ocorrências cada.

A maior e a menor ocorrência de títulos duplicados identificados na BRAPCI foi de (4) e (2) respectivamente. Enquanto que na SciELO a maior ocorrência foi de (3) e a menor foi de (2). Já na EBSCOhost a maior ocorrência ficou em (5) e a menor em (2).

A duplicação de comunicações científicas em mais de uma base foram identificadas respectivamente nas ordens: 13 (1) ocorrência cada nas bases SciELO e na EBSCOhost; na ordem 14 com (1) ocorrência cada nas bases BRAPCI e SciELO; na ordem 15 com (1) ocorrência cada nas bases BRAPCI e SciELO; na ordem 23 com (1) ocorrência em cada uma das bases BRAPCI e na EBSCOhost; e na ordem 37 com (1) ocorrência nas bases SciELO e a EBSCOhost.

A base com maior quantitativo total de duplicações de comunicações científicas foi a EBSCOhost com (31), seguida SciELO com (20) e da BRAPCI com (15).

Os dados indicam que existe uma significativa duplicação de comunicações científicas sobre o tema em algumas bases de conhecimento e até mesmo em uma mesma base. É necessário portanto aos pesquisadores estarem atentos quanto a estes tipos de resultados. Verificou-se também que no caso das comunicações científicas analisadas, nenhuma tem duas ou mais ocorrências de duplicação.

Observou-se na coleta de dados realizada nas três bases de conhecimento que foram encontradas 267 comunicações científicas únicas.

Alguns periódicos e anais de congresso possuem um texto de apresentação. Portanto, esta somatória de ocorrência é descartada.

A Tabela 4 representa os tipos de comunicações científicas identificadas nas bases. Em ordem decrescente a EBSCOhost retornou 141 comunicações científicas, seguida da SciELO com 134 e a BRAPCI com 56.

A partir da observação da Tabela 4 é possível verificar por exemplo que a BRAPCI é a base com maior variedade de comunicações científicas, entretanto com o menor percentual de artigos em periódicos quando comparada às demais bases.

Existe uma predominância de artigos em periódicos em relação aos demais tipos de comunicações científicas identificadas. A BRAPCI possui 11,44% de artigos, a SciELO 42,81% e a EBSCOhost 45,75%. Do quantitativo de comunicações científicas selecionadas e analisadas nas 3 bases observa-se que todas são referentes a artigos em periódicos.

O resultado talvez aponte para uma tendência de preferência dos pesquisadores em publicar comunicações científicas em formato de artigo em periódico. Entretanto, é preciso que investigações futuras de múltiplas áreas do conhecimento como as Ciência Sociais Aplicadas, Ciências da Saúde dentre outras possam indicar se isso é um caminho mais apropriado ou não para a divulgação do conhecimento.

Nas comunicações científicas revisadas por base tem-se o respectivo resultado. Na BRAPCI apenas (1) artigo em periódico foi analisado, enquanto que a SciELO somam-se (8) e a EBSCOhost (11), totalizando 20 artigos. A redução na quantidade de comunicações científicas revisadas se explica pela aplicação dos critérios de exclusão, relacionados na Seção 2, dos Procedimentos Metodológicos.

Tabela 4 - Total de ocorrências de tipos de comunicações científicas, segmentadas por base de conhecimento, incluindo comunicações científicas totais (sem recorte) e descartadas na análise (com recorte), em valores absolutos e em percentuais.

Tipo de Comunicação Científica	**BRAPCI**	**SciELO**	**EBSCO host**	**Total**	**BRAPCI (em %)**	**SciELO (em %)**	**EBSCO host (em %)**	**Total (em %)**
Sem recorte								
Artigo de revisão	2	0	0	**2**	100,00%	0,00%	0,00%	**100,00%**
Artigo em Anais	2	0	1	**3**	66,67%	0,00%	33,33%	**100,00%**
Artigo em Periódico	35	131	140	**306**	11,44%	42,81%	45,75%	**100,00%**
Comunicação oral	3	0	0	**3**	100,00%	0,00%	0,00%	**100,00%**
Ensaios	1	0	0	**1**	100,00%	0,00%	0,00%	**100,00%**
Pecha Kucha	1	0	0	**1**	100,00%	0,00%	0,00%	**100,00%**
Periódico	2	0	0	**2**	100,00%	0,00%	0,00%	**100,00%**
Pesquisa em andamento	2	0	0	**2**	100,00%	0,00%	0,00%	**100,00%**
Preprints	0	3	0	**3**	0,00%	100,00%	0,00%	**100,00%**
Relato de experiência	2	0	0	**2**	100,00%	0,00%	0,00%	**100,00%**
Relato de Pesquisa	6	0	0	**6**	100,00%	0,00%	0,00%	**100,00%**
Total	**56**	**134**	**141**	**331**	**16,92%**	**40,48%**	**42,60%**	**100,00%**

Tipo de Comunicação Científica	BRAPCI	SciELO	EBSCO host	Total	BRAPCI (em %)	SciELO (em %)	EBSCO host (em %)	Total (em %)
Com recorte								
Artigo de revisão	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Artigo em Anais	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Artigo em Periódico	1	8	11	**20**	5,00%	40,00%	55,00%	**100,00%**
Comunicação oral	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Ensaios	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Pecha Kucha	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Periódico	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Pesquisa em andamento	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Preprints	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Relato de experiência	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Relato de Pesquisa	0	0	0	**0**	0,00%	0,00%	0,00%	**0,00%**
Total	**1**	**8**	**11**	**20**	**5,00%**	**40,00%**	**55,00%**	**100,00%**

Fonte: Autora.

A Tabela 5 representa a quantidade de ocorrências de tipos de comunicações científicas por strings de busca, sem recorte e com recorte. Para uma melhor compreensão dos resultados da Tabela 5, lista-se a seguir a ordem primeiramente sem recorte.

1. Artigo de revisão com 2 ocorrências, sendo (1) em “Redes sociais AND privacidade” e (1) em “Redes sociais on-line”;
2. Artigo em anais de eventos com 3 ocorrências, sendo (1) em “Redes sociais AND privacidade e (2) em “Redes sociais online”;
3. Artigo em periódicos com 306 ocorrências, sendo (112) em “Mídias sociais”, (2) em “Mídias sociais AND privacidade”, (83) em “Redes sociais AND privacidade”, (29) em “Redes sociais on-line”, (5) em “Redes sociais on-line AND privacidade”, (67) em “Redes sociais online”, e (8) em “Redes sociais online AND privacidade”;
4. Comunicação oral com 3 ocorrências, sendo (1) em “Redes sociais on-line” e (1) em “Redes sociais online”, e (1) em “Redes sociais online AND privacidade”;
5. Ensaios com (1) ocorrência em “Redes sociais AND privacidade”;
6. Pecha Kucha apenas com (1) ocorrência em “Redes sociais online”;
7. Periódico teve 2 ocorrências, com (1) em “Redes sociais AND privacidade” e (1) “Redes sociais online AND privacidade”;

8. Pesquisa em andamento com 2 ocorrências (1) em “Redes sociais on-line” e (1) em “Redes sociais online”;
9. Preprints com (3) ocorrências em “Mídias sociais
10. Relatos de experiência com 2 ocorrências em “Redes sociais online”;
11. Relatos de pesquisa com 6 ocorrências, sendo (1) em “Redes sociais on-line”. (1) em “Redes sociais on-line AND privacidade”, (2) em “Redes sociais online” e (2) em “Redes sociais online AND privacidade”.

Se comparados os tipos de comunicações recuperadas nas bases de conhecimento temos como as maiores ocorrências de strings os artigos em periódicos e os relatos de pesquisa. Observou-se também que todas as strings utilizadas recuperaram algum tipo de comunicação científica sobre o tema investigado, embora em menor quantidade se comparado aos artigos em periódicos.

Sobre os resultados com recorte da Tabela 5 (Apêndice B) tem-se um total de 20 comunicações científicas, relacionadas também por número de ocorrências.

1. Artigo de revisão, assim como artigo em anais de eventos; comunicação oral, ensaios, pecha kucha, periódico, pesquisa em andamento, preprints, relato de experiência e relato de pesquisa não tiveram nenhuma ocorrência;
2. Os artigos em periódicos tiveram 20 ocorrências sendo (2) em "Mídias sociais”, (0) em “Mídias sociais AND privacidade”, (12) em “Redes sociais AND privacidade”, (2) em “Redes sociais on-line”, (0) em “Redes sociais on-line AND privacidade”, (4) em “Redes sociais online” e (0) em “Redes sociais online AND privacidade”.

A Tabela 6, traz autores recuperados nas bases de conhecimento com o número de ocorrência igual ou superior a 3. A Tabela é formada pela relação dos autores incluídos e não incluídos na revisão. Sendo que os autores com maior frequência identificados foram Sant’Ana, com (8), seguido de Oliveira com (7), Silva e Streck com (5) cada e Assumpção, Furtado, Oliveira, Passos e Rodrigues com (4) ocorrências cada.

Percebe-se que há autores recuperados em apenas uma base de conhecimento como é o caso de Sant’Ana cuja ocorrência indica apenas para a base BRAPCI. Outros autores como Oliveira, L. foi identificado nas três bases, embora esta não seja a dinâmica predominante da Tabela 6.

Observa-se no recorte desta pesquisa que cada autor possui apenas uma comunicação científica selecionada e analisada, não sendo portanto necessária a elaboração de tabela.

Tabela 6 - Total de ocorrências de autores, segmentadas por base de conhecimento, incluindo autores descartados na análise, em valores absolutos (n >= 3).

Autor	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
SANT'ANA, RICARDO CÉSAR GONÇALVES	8	0	0	**8**
OLIVEIRA, LÍDIA	3	2	2	**7**
VASCONCELLOS-SILVA, PAULO ROBERTO	0	6	0	**6**
SILVA, ARMANDO MALHEIRO DA	0	0	5	**5**
STRECK, MELISSA	0	0	5	**5**
ASSUMPÇÃO, FABRÍCIO SILVA	4	0	0	**4**
FURTADO, CASSIA	3	1	0	**4**
OLIVEIRA, LEONARDO PESTILLO DE	2	0	2	**4**
PASSOS, JASILAINE ANDRADE	0	4	0	**4**
RODRIGUES, FERNANDO DE ASSIS	4	0	0	**4**
SANTOS, PLÁCIDA LEOPOLDINA VENTURA AMORIM DA COSTA	4	0	0	**4**
ALBUQUERQUE, JOÃO PEDRO SILVA	3	0	0	**3**
BRAGA, DENISE BÉRTOLI	0	0	3	**3**
FONSECA, FERNANDA SANTOS	0	0	3	**3**
FURTADO, CASSIA CORDEIRO	3	0	0	**3**
HJORT, RODRIGO	0	0	3	**3**
KADOOKA, ALINE	0	0	3	**3**
LEPRE, RITA MELISSA	0	0	3	**3**
LUCENA, TIAGO FRANKLIN RODRIGUES	2	0	1	**3**
MAIA, JUNOT DE OLIVEIRA	0	0	3	**3**
PALETTA, FRANCISCO CARLOS	0	0	3	**3**
PELLANDA, EDUARDO CAMPOS	0	0	3	**3**
PINHO, VIVIANE DIAS MALHEIROS DE	0	0	3	**3**
PURIM, KÁTIA SHEYLLA MALTA	0	3	0	**3**
SANTOS, PAULA WIVIANNE QUIRINO DOS	3	0	0	**3**
SOUZA FILHO, JOSÉ RONALDO AGRA DE	0	0	3	**3**
TIZZOT, EDISON LUIZ ALMEIDA	0	3	0	**3**
Total de Ocorrências	**39**	**19**	**45**	**103**

Fonte: Autora (2022).

A Tabela 7 representa o quantitativo de autores segmentadas por strings. Definiu-se a inclusão na tabela de ocorrências maiores ou iguais a 3. A Tabela 7 contém tanto o nome dos autores incluídos como dos não incluídos na RSL.

As maiores ocorrências totais de strings foram verificadas em "Redes sociais online" com (25) ocorrências, "Redes sociais on-line" com (24) ocorrências, "Redes sociais AND privacidade" com (16) ocorrências e "Redes sociais online AND privacidade" com (14) ocorrências. E as menores foram identificadas em "Redes sociais on-line AND privacidade" com (10) ocorrências, "Mídias sociais AND privacidade" com (2) ocorrências e "Mídias sociais" com (12) ocorrências.

Percebe-se ainda que há uma prevalência de autores recuperados com as strings de “Redes sociais” e com as suas respectivas variações. Por outro lado, este resultado pode indicar que exista um cuidado maior por parte dos autores com a utilização da string de "Mídias sociais”.

Tabela 7 - Total de ocorrências de autores, segmentadas por string, incluindo autores descartados na análise, em valores absolutos (n >= 3).

Autor	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais on-line AND privacidade	Redes sociais online AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
SANTANA, RICARDO CÉSAR GONÇALVES	3	1	0	1	3	0	0	**8**
OLIVEIRA, LÍDIA	1	6	0	0	0	0	0	**7**
VASCONCELLOS-SILVA, PAULO ROBERTO	0	0	0	0	0	0	6	**6**
SILVA, ARMANDO MALHEIRO DA	0	1	3	1	0	0	0	**5**
STRECK, MELISSA	1	1	1	1	1	0	0	**5**
ASSUMPÇÃO, FABRÍCIO SILVA	1	1	0	1	1	0	0	**4**
FURTADO, CASSIA	1	3	0	0	0	0	0	**4**
OLIVEIRA, LEONARDO PESTILLO DE	1	2	0	0	1	0	0	**4**
PASSOS, JASILAINE ANDRADE	0	0	0	0	0	0	4	**4**
RODRIGUES, FERNANDO DE ASSIS	2	0	0	0	2	0	0	**4**
SANTOS, PLÁCIDA LEOPOLDINA VENTURA AMORIM DA COSTA	1	1	0	1	1	0	0	**4**
ALBUQUERQUE, JOÃO PEDRO SILVA	3	0	0	0	0	0	0	**3**
BRAGA, DENISE BÉRTOLI	1	0	1	0	1	0	0	**3**
FONSECA, FERNANDA	0	1	1	1	0	0	0	**3**

Autor	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais on-line AND privacidade	Redes sociais online AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
SANTOS								
FURTADO, CASSIA CORDEIRO	1	2	0	0	0	0	0	**3**
HJORT, RODRIGO	0	1	1	1	0	0	0	**3**
KADOOKA, ALINE	1	0	1	0	1	0	0	**3**
LEPRE, RITA MELISSA	1	0	1	0	1	0	0	**3**
LUCENA, TIAGO FRANKLIN RODRIGUES	2	0	0	0	1	0	0	**3**
MAIA, JUNOT DE OLIVEIRA	1	0	1	0	1	0	0	**3**
PALETTA, FRANCISCO CARLOS	0	1	1	1	0	0	0	**3**
PELLANDA, EDUARDO CAMPOS	1	1	1	0	0	0	0	**3**
PINHO, VIVIANE DIAS MALHEIROS DE	0	1	1	1	0	0	0	**3**
PURIM, KÁTIA SHEYLLA MALTA	0	0	1	0	0	1	1	**3**
SANTOS, PAULA WIVIANNE QUIRINO DOS	3	0	0	0	0	0	0	**3**
SOUZA FILHO, JOSÉ RONALDO AGRA DE	0	1	1	1	0	0	0	**3**
TIZZOT, EDISON LUIZ ALMEIDA	0	0	1	0	0	1	1	**3**
Total de Ocorrências	**25**	**24**	**16**	**10**	**14**	**2**	**12**	**103**

Fonte: Autora (2022).

A Tabela 8 representa a quantidade de ocorrências de títulos de periódicos ou anais de congressos identificados na análise dos dados. Dentre os títulos de periódicos recuperados por base de conhecimento foram relacionados os que obtiveram ocorrência maior ou igual a 3.

Nota-se que foram recuperados alguns títulos de periódicos com foco em CI com ocorrências significativas nesta análise. Dos títulos de periódicos recuperados relaciona-se:

“Perspectiva em Ciência da Informação” com (10) ocorrências, “Em Questão” com (5) ocorrências, “Informação & Informação” (4), “Informação & Tecnologia”(3), “Pesquisa Brasileira em Ciência da Informação e Biblioteconomia” (3), "Revista Ibero-Americana de Ciência da Informação” (3) e “Transinformação” (3), totalizando 7 periódicos com 31 ocorrências.

No caso do recorte analisado, a única reincidência de periódico é o “Sessões do Imaginário” que possui 3 ocorrências na análise, todas sendo vinculadas à base de conhecimento EBSCOhost[13]. Portanto, é preciso que os pesquisadores fiquem atentos aos títulos de periódicos que tenham uma tendência no aceite de comunicações científicas com temas relacionados às TIC, especialmente sobre SRSO.

Tabela 8 - Total de ocorrências de periódicos e anais de congresso, segmentados por Base de Conhecimento, incluindo comunicações científicas descartadas na análise, em valores absolutos (n >= 3).

#	Título do Periódico ou Título dos Anais	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências	#	Título do Periódico ou Título dos Anais	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
1	REVISTA COMPOLÍTICA	0	0	20	**20**	18	SAÚDE E PESQUISA	0	0	4	**4**
2	PRISMA.COM	3	0	14	**17**	19	SAÚDE EM DEBATE	0	4	0	**4**
3	SESSÕES DO IMAGINÁRIO	0	0	14	**14**	20	UNIVERSITAS: ARQUITETURA E COMUNICAÇÃO SOCIAL	0	0	4	**4**
4	CIÊNCIA & SAÚDE COLETIVA	0	12	0	**12**	21	COMUNICAÇÃO E SOCIEDADE	0	2	1	**3**
5	PERSPECTIVAS EM CIÊNCIA DA INFORMAÇÃO	3	7	0	**10**	22	ESPAÇO E CULTURA	0	0	3	**3**
6	CADERNOS DE SAÚDE PÚBLICA	0	8	0	**8**	23	FÓRUM LINGÜÍSTICO	0	0	3	**3**
7	INTERFACE - COMUNICAÇÃO, SAÚDE, EDUCAÇÃO	0	6	0	**6**	24	GALÁXIA (SÃO PAULO)	0	3	0	**3**
8	REVISTA BRASILEIRA DE ADMINISTRAÇÃO CIENTÍFICA	0	0	6	**6**	25	INFORMAÇÃO & TECNOLOGIA	3	0	0	**3**
9	EM QUESTÃO	5	0	0	**5**	26	INTERCOM: REVISTA BRASILEIRA DE CIÊNCIAS DA COMUNICAÇÃO	0	3	0	**3**

[13] Ressalta-se que não há necessidade de elaboração de tabela para o registro de uma única ocorrência.

#	Título do Periódico ou Título dos Anais	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências	#	Título do Periódico ou Título dos Anais	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
10	OBSERVATORIO (OBS*)	0	2	3	**5**	27	LETRÔNICA	0	0	3	**3**
11	PERSPECTIVAS EM GESTÃO & CONHECIMENTO	5	0	0	**5**	28	MEDIA & JORNALISMO	0	3	0	**3**
12	RECIIS - REVISTA ELETRÔNICA DE COMUNICAÇÃO, INFORMAÇÃO E INOVAÇÃO EM SAÚDE	5	0	0	**5**	29	PESQUISA BRASILEIRA EM CIÊNCIA DA INFORMAÇÃO E BIBLIOTECONOMIA	2	0	1	**3**
13	REVISTA DE PSICOLOGIA DA CRIANÇA E DO ADOLESCENTE	0	0	5	**5**	30	REVISTA BRASILEIRA DE ENFERMAGEM	0	3	0	**3**
14	SAÚDE E SOCIEDADE	0	5	0	**5**	31	REVISTA IBERO-AMERICANA DE CIÊNCIA DA INFORMAÇÃO	3	0	0	**3**
15	INFORMAÇÃO & INFORMAÇÃO	4	0	0	**4**	32	SIGNÓTICA	0	0	3	**3**
16	INTRATEXTOS	0	0	4	**4**	33	TRANSINFORMAÇÃO	0	3	0	**3**
17	REVISTA BRASILEIRA DE EDUCAÇÃO MÉDICA	0	4	0	**4**	**Total de Ocorrências**		**25**	**44**	**66**	**135**

Fonte: Autora (2022).

A Tabela 9 traz um total de 186 ocorrências de títulos de periódicos recuperados com a utilização das *strings* de busca definidas na Seção 2, dos Procedimentos Metodológicos.

As maiores ocorrências de títulos recuperados foram com as strings "Mídias Sociais", "Redes sociais AND privacidade", "Redes sociais online" e "Redes Sociais On-line". E as menores ocorrências de títulos recuperados foram com as strings "Redes Sociais Online AND Privacidade", "Redes Sociais On-line AND Privacidade" e "Mídias sociais AND Privacidade".

Considera-se que as strings utilizadas para a recuperação das comunicações científicas em periódicos se mostraram bastante eficazes, graças à consulta prévia dos vocabulários controlados mencionados nos Procedimentos Metodológicos da Seção 2.

No caso do recorte analisado, a única reincidência de periódico é o “Sessões do Imaginário” que possui 3 ocorrências na sua análise, sendo todas vinculadas às strings “Redes sociais AND privacidade” com (2) ocorrências, e “Redes Sociais Online” (1) com ocorrência[14].

Tabela 9 - Total de ocorrências de periódicos e anais de congresso, segmentados por string, incluindo comunicações científicas descartadas na análise, em valores absolutos (n >= 3).

#	Título do Periódico ou Título dos Anais	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
1	REVISTA COMPOLÍTICA	12	6	2	0	0	0	0	**20**
2	PRISMA.COM	4	2	7	1	1	0	2	**17**
3	SESSÕES DO IMAGINÁRIO	2	1	9	1	1	0	0	**14**
4	CIÊNCIA & SAÚDE COLETIVA	0	0	2	0	0	0	10	**12**
5	PERSPECTIVAS EM CIÊNCIA DA INFORMAÇÃO	2	2	0	0	0	0	6	**10**
6	CADERNOS DE SAÚDE PÚBLICA	0	0	0	0	0	0	8	**8**
7	INTERFACE - COMUNICAÇÃO, SAÚDE, EDUCAÇÃO	0	0	2	0	0	0	4	**6**
8	REVISTA BRASILEIRA DE ADMINISTRAÇÃO CIENTÍFICA	1	1	2	1	1	0	0	**6**
9	EM QUESTÃO	2	1	0	1	1	0	0	**5**
10	OBSERVATORIO (OBS*)	1	2	2	0	0	0	0	**5**
11	PERSPECTIVAS EM GESTÃO & CONHECIMENTO	1	2	0	1	1	0	0	**5**
12	RECIIS - REVISTA ELETRÔNICA DE COMUNICAÇÃO, INFORMAÇÃO E INOVAÇÃO EM SAÚDE	2	1	0	1	1	0	0	**5**
13	REVISTA DE PSICOLOGIA DA	1	0	3	1	0	0	0	**5**

[14] Neste caso não é necessário a elaboração de Tabela para o registro de um único resultado.

#	Título do Periódico ou Título dos Anais	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
	CRIANÇA E DO ADOLESCENTE								
14	SAÚDE E SOCIEDADE	0	0	0	0	0	0	5	**5**
15	INFORMAÇÃO & INFORMAÇÃO	2	1	1	0	0	0	0	**4**
16	INTRATEXTOS	0	0	4	0	0	0	0	**4**
17	REVISTA BRASILEIRA DE EDUCAÇÃO MÉDICA	0	0	1	0	0	1	2	**4**
18	SAÚDE E PESQUISA	2	2	0	0	0	0	0	**4**
19	SAÚDE EM DEBATE	0	0	0	0	0	0	4	**4**
20	UNIVERSITAS: ARQUITETURA E COMUNICAÇÃO SOCIAL	2	0	2	0	0	0	0	**4**
21	COMUNICAÇÃO E SOCIEDADE	1	0	0	0	0	0	2	**3**
22	ESPAÇO E CULTURA	0	0	3	0	0	0	0	**3**
23	FÓRUM LINGÜÍSTICO	3	0	0	0	0	0	0	**3**
24	GALÁXIA (SÃO PAULO)	0	0	0	0	0	0	3	**3**
25	INFORMAÇÃO & TECNOLOGIA	2	0	0	1	0	0	0	**3**
26	INTERCOM: REVISTA BRASILEIRA DE CIÊNCIAS DA COMUNICAÇÃO	0	0	0	0	0	0	3	**3**
27	LETRÔNICA	0	0	3	0	0	0	0	**3**
28	MEDIA & JORNALISMO	2	0	1	0	0	0	0	**3**
29	PESQUISA BRASILEIRA EM CIÊNCIA DA INFORMAÇÃO E BIBLIOTECONOMIA	1	1	1	0	0	0	0	**3**
30	REVISTA	0	0	0	0	0	0	3	**3**

#	Título do Periódico ou Título dos Anais	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
	BRASILEIRA DE ENFERMAGEM								
31	REVISTA IBERO-AMERICANA DE CIÊNCIA DA INFORMAÇÃO	1	0	1	1	0	0	0	**3**
32	SIGNÓTICA	1	0	1	1	0	0	0	**3**
33	TRANSINFORMAÇÃO	0	0	0	0	0	0	3	**3**
Total de Ocorrências		**45**	**22**	**47**	**10**	**6**	**1**	**55**	**186**

Fonte: Autora (2022).

Os resultados da Tabela 10 foram obtidos a partir de pesquisa realizada na Plataforma Sucupira[15] e representam o quantitativo de ocorrências dos estratos Qualis por periódicos recuperados nas bases de conhecimento. O quantitativo de comunicações científicas recuperadas nas 3 bases foram: “A1” com (29) ocorrências no total, “A2” com (56) ocorrências, “B1” com (91) ocorrências, “B2” com (44) ocorrências, “B3” com (29) ocorrências, “B4” com (13) ocorrências, “B5” com (35) ocorrências, “C”com (7) ocorrências (7) e “Nenhum” com (27) ocorrências.

Quando se compara as 3 bases de conhecimento na Tabela 10 verifica-se por exemplo que a SciElo possui nos três primeiros estratos Qualis um quantitativo maior de comunicações científicas em “A1”, “A2” e “B1” em relação a BRAPCI e a EBSCOhost, o que reflete um nível mais elevado de qualidade das comunicações científicas disponibilizadas na base SciELO, referentes a esta investigação.

Ainda sobre a SciElo a maior concentração de periódicos com estrato Qualis foi em “A2” e a menor em “B4” e “B5”, sendo que em “C” não houve nenhum registro.

Já na EBSCOhost, a grande concentração de periódicos foi em “B1” e a menor em “A1”. Igualmente a BRAPCI com maior concentração em “B1” e “B5” e a menor em “C”.

Tabela 10 - Total de ocorrências de estratos QUALIS da CAPES, segmentados por Base de Conhecimento, incluindo comunicações científicas descartadas na análise, em valores absolutos.

QUALIS	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
A1	3	24	2	**29**
A2	9	40	7	**56**

[15] A avaliação por meio do extrato Qualis dos periódicos recuperados nas bases de conhecimento.

QUALIS	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
B1	13	38	40	**91**
B2	0	13	31	**44**
B3	2	8	19	**29**
B4	6	2	5	**13**
B5	13	2	20	**35**
C	1	0	6	**7**
NENHUM	9	7	11	**27**
Total de Ocorrências	**56**	**134**	**141**	**331**

Fonte: Autora (2022).

A Tabela 11 traz a ordem dos estratos Qualis apenas dos artigos em periódicos revisados, sendo observado as seguintes ocorrências: “A1” com (2) ocorrências no total, “A2” com (6) ocorrências sendo o maior quantitativo da SciELO, o “B1” com (10) ocorrências sendo a maior na EBSCOhost, “B2” com (2) ocorrências, da base SciELO.

Quando observadas as bases de conhecimento verifica-se por exemplo que a BRAPCI teve apenas uma ocorrência de comunicação científica em “A2”. A SciELO por sua vez tem ocorrências nos estratos “A1”, “A2”, “B1”e “B2”. Enquanto que a EBSCOhost obteve ocorrências de comunicação científica em “A1”, “A2” e “B1”, este último com o maior quantitativo de comunicações científicas revisadas dentre todas as bases. A SciELO continua a ter um destaque em relação às outras bases, apresentando um equilíbrio na qualidade das comunicações científicas revisadas.

Tabela 11 - Total de ocorrências de estratos QUALIS da CAPES, segmentados por Base de Conhecimento, excluindo as comunicações científicas descartadas na análise, em valores absolutos.

QUALIS	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
A1	0	1	1	**2**
A2	1	3	2	**6**
B1	0	2	8	**10**
B2	0	2	0	**2**
Total de Ocorrências	**1**	**8**	**11**	**20**

Fonte: Autora (2022).

A Tabela 12 traz o estrato Qualis dos periódicos por strings. O que se pode perceber observando a Tabela é que as maiores ocorrências de string por estrato Qualis foram identificadas em “A2”, “B1” e em “B2”.

Em “A2” a maior ocorrência foi verificada em "Mídias sociais” e a menor em “Redes sociais online AND privacidade”, e a única strings sem nenhuma ocorrência foi em "Mídias sociais AND privacidade”. Em “B1” o uso de todas as strings recuperaram algum tipo de comunicação científica, sendo a maior ocorrência "Mídias sociais” com (29)

e as menores “Redes sociais on-line AND privacidade” com (2) ocorrências e "Mídias sociais AND privacidade” com (2) ocorrências.

Em “B2” a maior ocorrência registrada foi em “Redes sociais online” com (17) ocorrências e a menor foi em “Redes sociais on-line” com (7) ocorrências. Destaca-se ainda que algumas comunicações científicas foram publicadas em periódicos sem “Nenhum” estrato Qualis. Apesar de terem sido poucos, isto pode representar aos autores e as suas pesquisas pouca visibilidade e credibilidade quanto à questão da qualidade das comunicações científicas.

Tabela 12 - Total de ocorrências de estratos QUALIS da CAPES, segmentados por string, incluindo comunicações científicas descartadas na análise, em valores absolutos.

QUALIS	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
A1	2	3	3	0	0	0	21	**29**
A2	4	3	10	1	1	0	37	**56**
B1	18	10	27	3	2	2	29	**91**
B2	17	7	10	0	0	0	10	**44**
B3	6	2	11	1	1	0	8	**29**
B4	7	3	0	2	1	0	0	**13**
B5	12	3	12	4	1	0	3	**35**
C	0	1	6	0	0	0	0	**7**
NENHUM	10	1	8	1	0	0	7	**27**
Total de Ocorrências	**76**	**33**	**87**	**12**	**6**	**2**	**115**	**331**

Fonte: Autora (2022).

As maiores concentrações de estrato da Tabela 13 foram percebidas nas strings “Redes sociais online” com (4) ocorrências, “Redes sociais on-line” com (2) ocorrências, “Redes sociais AND privacidade” com (12) ocorrências e “Mídias sociais” com (2) ocorrências. Este resultado indica que a associação de termos como “Redes sociais AND privacidade” para a realização da busca nas bases de conhecimento foi um recurso eficiente para a recuperação de comunicações científicas sobre o tema.

Não há ocorrência de nenhuma comunicação científica incluída na RSL com as strings de “Redes sociais online AND privacidade”, “Redes sociais on-line AND privacidade”, “Mídias sociais AND privacidade” nos 4 níveis de estratos adotados nesta investigação.

Tabela 13 - Total de ocorrências de estratos QUALIS da CAPES, segmentados por string, excluindo as comunicações científicas descartadas na análise, em valores absolutos.

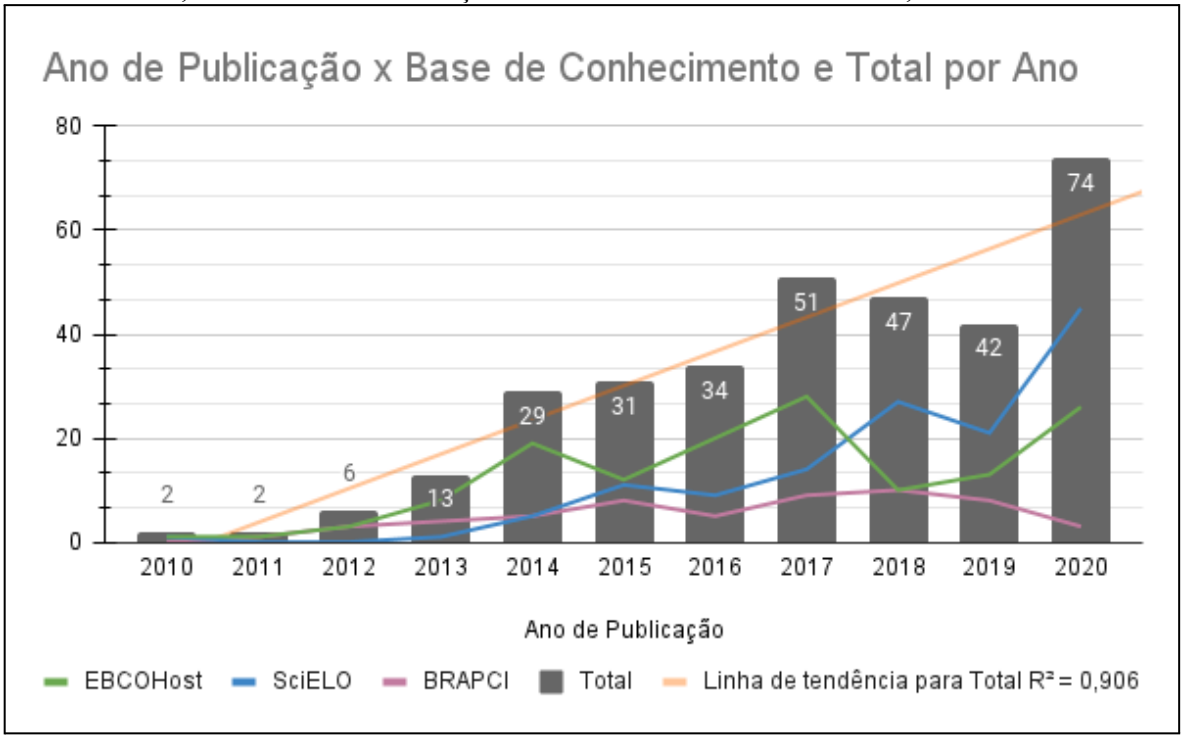
QUALIS	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
A1	0	0	2	0	0	0	0	**2**
A2	1	1	4	0	0	0	0	**6**
B1	2	1	5	0	0	0	2	**10**
B2	1	0	1	0	0	0	0	**2**
Total de Ocorrências	**4**	**2**	**12**	**0**	**0**	**0**	**2**	**20**

Fonte: Autora (2022).

O Gráfico 1 mostra primeiramente um quantitativo tímido de comunicações científicas recuperadas nas bases de conhecimento. O intervalo de tempo com menor número de comunicações científicas recuperadas foi registrado entre os anos de 2010 a 2013, sendo (2) em 2010 e (2) em 2011, (6) em 2012 e (13) em 2013. Entre o período de 2014 a 2016 houve um aumento no número de comunicações científicas com um certo equilíbrio na produção, com valores que variam de 29 a 34. No período que compreende o intervalo entre os anos de 2017 a 2020 percebe-se um aumento no número de comunicações por ano de ocorrência seguida de uma pequena queda nos anos seguintes, 2018 e 2019. Em 2020 foi registrado o maior número de comunicações conforme mostra o Gráfico.

Dentre as bases investigadas nota-se que a BRAPCI é a que teve menor desempenho de produção de comunicações. A EBSCOHost teve um pico de produção em 2017. Já a SciELO apresentou equilíbrio com uma pequena queda em 2019, mas com um aumento no ano seguinte. É preciso saber quais os fatores contribuíram para um aumento de comunicações científicas sobre a temática, de forma mais evidente entre os anos de 2014 a 2020.

Gráfico 1 - Total de ocorrências de comunicações científicas, segmentados por ano e por Base de Conhecimento, incluindo as comunicações científicas descartadas na análise, em valores absolutos.



Fonte: Autora (2022).

O Gráfico 2 traz as comunicações científicas incluídas na RSL por ano de produção. A primeira observação feita a partir do gráfico indica que a comunicação mais antiga analisada é a do ano de 2010, identificada na base SciELO. Após a primeira ocorrência houve mais (7) ocorrências distribuídas entre os anos de 2015 a 2020, totalizando (8) ocorrências de artigos em periódicos revisados.

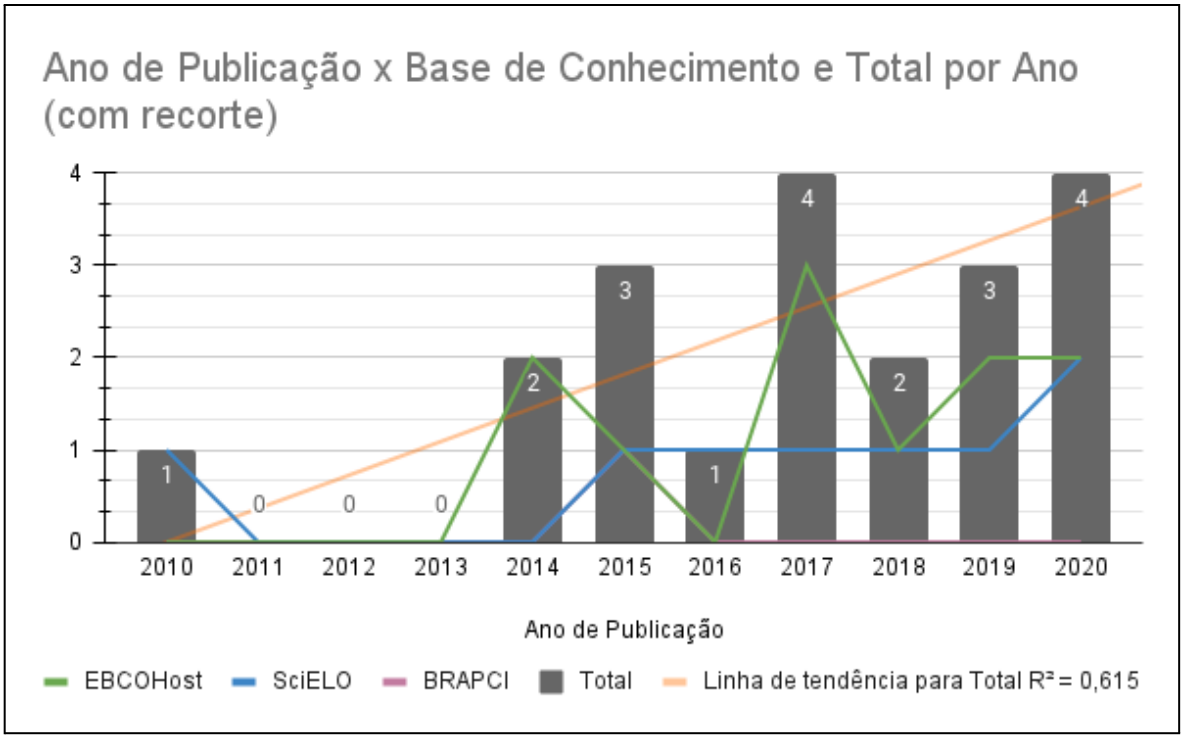
Entre os anos de 2011 a 2013 não foi incluída nenhuma comunicação científica na RSL. Após esse intervalo foram incluídas na RSL comunicações científicas da base EBSCOhost, sendo identificadas (2) ocorrências do ano de 2014, (1) ocorrência de 2015, (3) ocorrências de 2017, (1) ocorrência de 2018, (2) ocorrências de 2019 e (2) ocorrências de 2020, totalizando 11 comunicações revisadas referentes a esta base. A EBSCOhost foi a base com o maior quantitativo de comunicações incluídas na RSL devido à aderência ao tema.

Observa-se também no Gráfico 2 que foi analisado apenas 1 artigo em periódico da base BRAPCI referente ao ano de 2015. Posteriormente a isso houve uma estagnação de produções sobre a temática de SRSO, enquanto que as outras duas bases conseguiram manter ou aumentar a quantidade de comunicações científicas por ano.

Isso pode indicar que os pesquisadores da CI no Brasil necessitem voltar um pouco mais suas investigações para a temática, uma vez que esta ciência prioriza a organização e

o fluxo da informação. Destaca-se que a CI pode atuar em problemas relacionados às TIC, SRSO e à privacidade de dados e de informações da sociedade em diversas fontes e ambientes tanto offline como online, uma vez que ela possui “[...] uma forte dimensão social e humana que ultrapassa a tecnologia [...]” (SARACEVIC, p. 42, 1995).

Gráfico 2 - Total de ocorrências de comunicações científicas, segmentados por ano e por Base de Conhecimento, excluindo as comunicações científicas descartadas na análise, em valores absolutos.

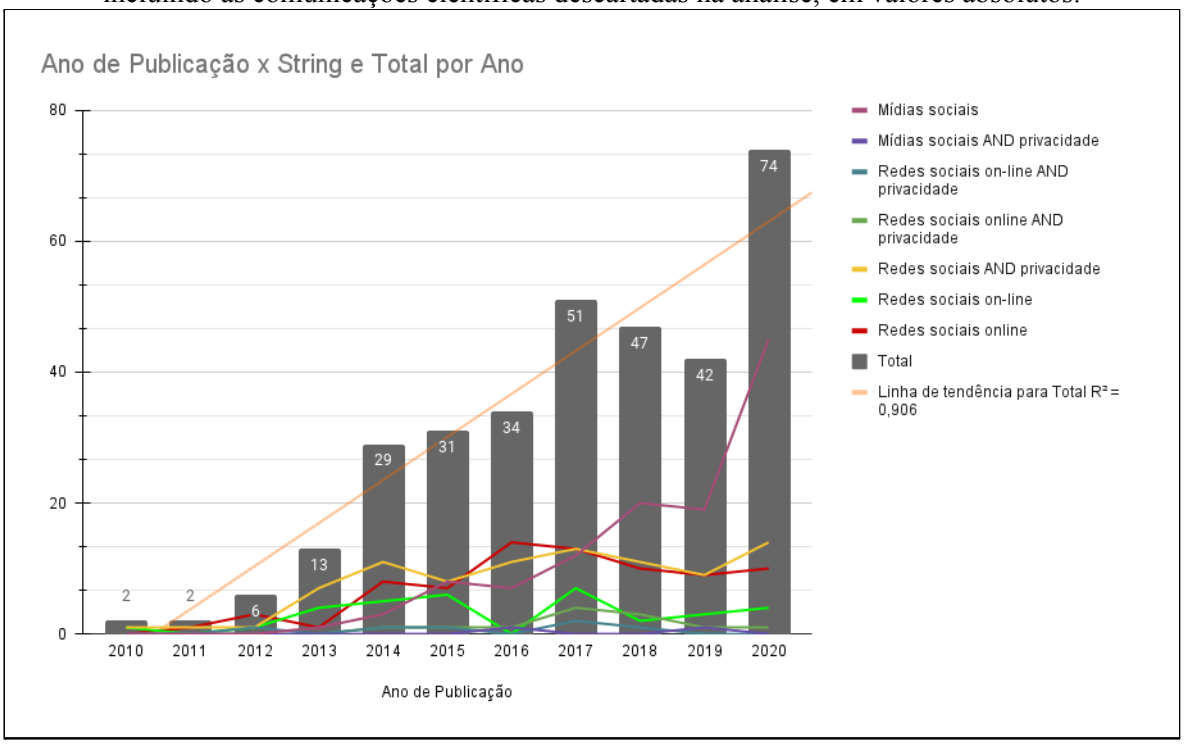


Fonte: Autora (2022).

O Gráfico 3 indica que a maior concentração de comunicações científicas recuperadas por ano foram as recuperadas com a string de "Mídias sociais”, “Redes sociais AND privacidade”, “Redes sociais online” e “Redes sociais on-line”, esta última com oscilações entre alta nos anos de 2013, 2014, 2015 e 2017 e queda observadas nos anos de 2016 e 2018.

O quantitativo de comunicações científicas recuperadas do ano de 2020 foi bem maior que dos anos anteriores, chegando a um total de 74 comunicações científicas. As menores concentrações de comunicações científicas recuperadas foram com as strings de “Redes sociais AND privacidade”, “Redes sociais online”, “Redes sociais online AND privacidade”, “Redes sociais on-line AND privacidade” e "Mídias sociais AND privacidade”.

Gráfico 3 - Total de ocorrências de comunicações científicas, segmentados por ano e por string, incluindo as comunicações científicas descartadas na análise, em valores absolutos.



Fonte: Autora (2022).

O Gráfico 4 apresenta o total de ocorrências das comunicações científicas revisadas nesta RSL segmentadas por string e por ano. Os anos de 2015, 2017, 2019 e 2020 representam as maiores ocorrências de comunicações científicas incluídas na RSL pela pela somatória das strings.

Apenas (1) comunicação científica com a string “Redes sociais AND privacidade” foi incluída na RSL referente ao ano de 2010. E apenas (2) comunicações científicas com a string “Redes sociais AND privacidade” foram na RSL referente ao ano de 2014.

Referente ao ano de 2015 foram incluídas na RSL (3) comunicações científicas com as somatórias das strings “Redes sociais online”, “Redes sociais on-line” e “Redes sociais AND privacidade”. E apenas (1) comunicação foi incluída com a string “Redes sociais AND privacidade” do ano de 2016,.

E do ano de 2017 foram incluídas na RSL (4) comunicações científicas com as somatórias das strings “Redes sociais online”, “Redes sociais on-line”, “Redes sociais AND privacidade”. De 2018 foram incluídas mais (2) comunicações científicas com as somatórias das strings “Redes sociais AND privacidade” e "Mídias sociais”.

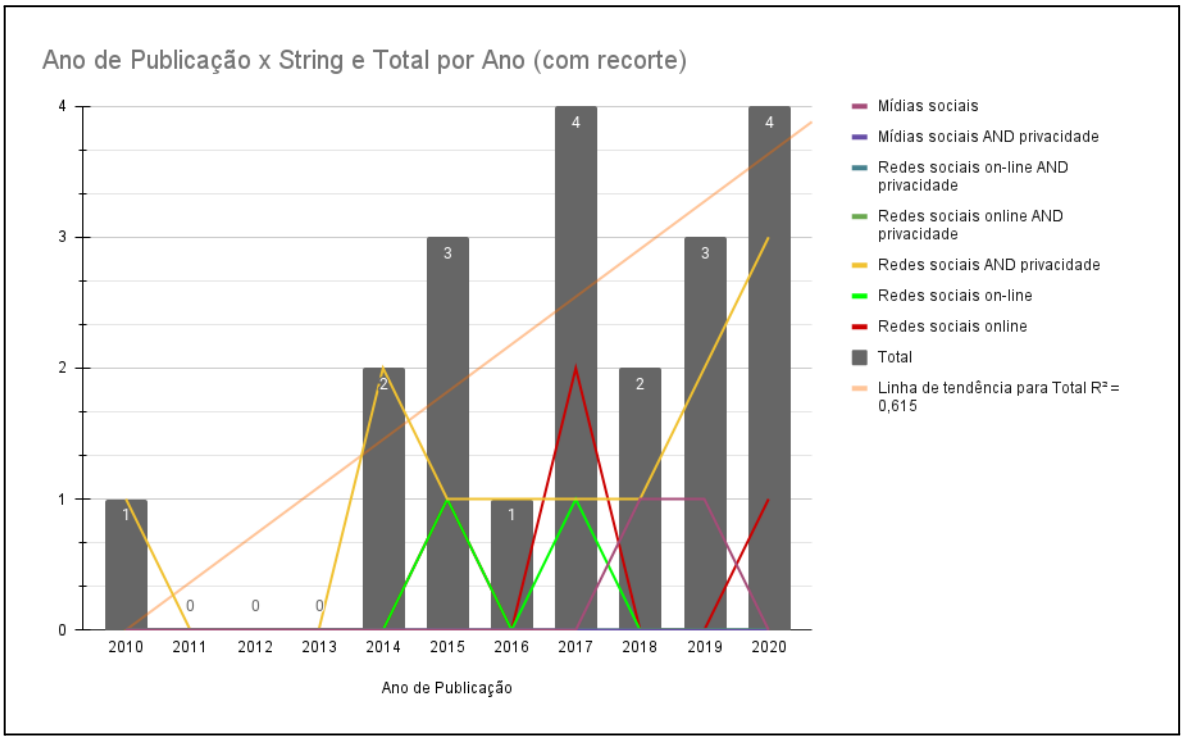
Referente ao ano de 2019 foram incluídas mais (3) com as somatórias das strings “Redes sociais AND privacidade” e "Mídias sociais”. E do ano de 2020 mais (4)

comunicações científicas foram incluídas na RSL com as somatórias das strings "Redes sociais online" e "Redes sociais AND privacidade".

A string "Redes sociais AND privacidade" foi dentre todas as outras a que mais conseguiu incluir comunicações científicas na RSL. De 2010 a 2020, os únicos anos não incluídos na RSL com essa string foram dos anos 2011 a 2013, indicando assim um certo equilíbrio no uso dessa string.

Portanto, a utilização das strings atendeu de forma satisfatória e contribui na recuperação das comunicações científicas nas bases de conhecimento. Entretanto é preciso saber quais os fatores interferiram para que as strings não conseguissem recuperar as comunicações científicas referentes aos anos de 2011 a 2013.

Gráfico 4 - Total de ocorrências de comunicações científicas, segmentados por ano e por string, excluindo as comunicações científicas descartadas na análise, em valores absolutos.



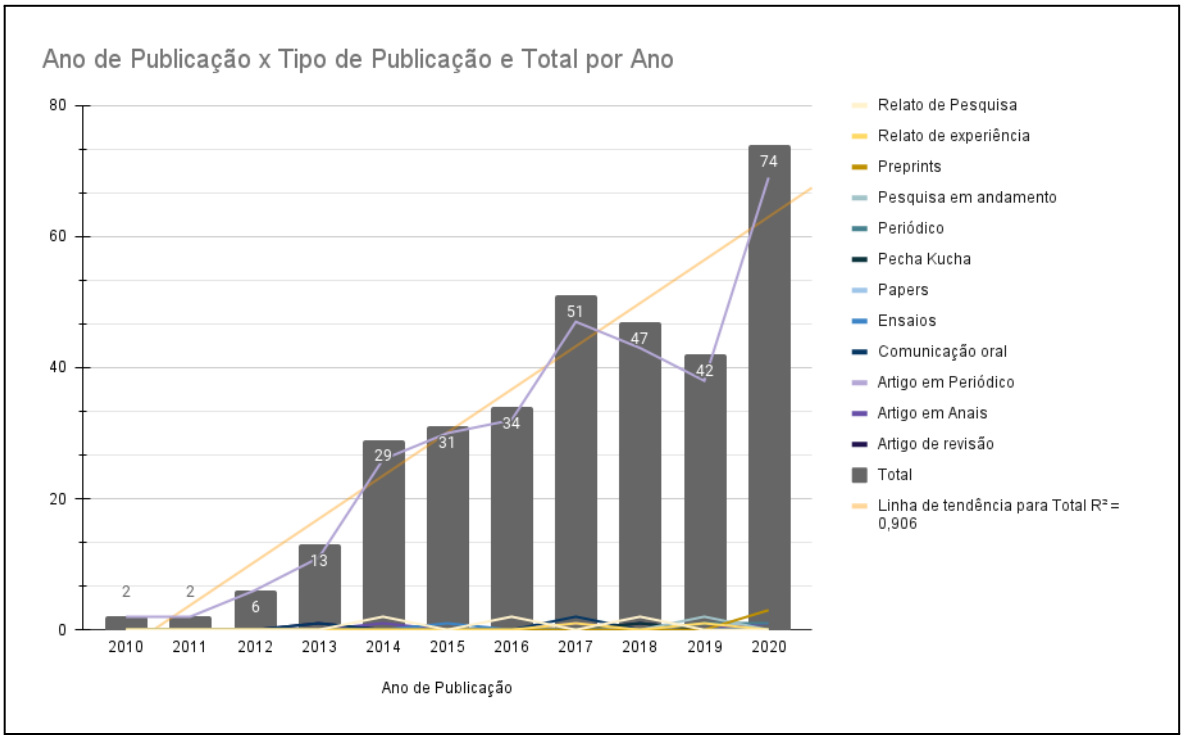
Fonte: Autora (2022).

O Gráfico 5 demonstra o quantitativo de tipos de comunicações científicas incluídas e não incluídas na RSL, e que estão distribuídas por ano. Nota-se que poucas comunicações científicas foram recuperadas sobre o tema entre os anos de 2010 a 2012. A partir de 2013 a 2014 houve um salto significativo de produção de comunicações científicas sobre o tema, indo da quantidade 13 em 2013 para 29 comunicações recuperadas em 2014. De 2014 a 2016 foi percebido também um certo equilíbrio de comunicações científicas recuperadas sobre o tema.

A partir de 2017 percebe-se um aumento e ligeira queda nos anos seguintes de 2018 e 2019. No ano de 2020 foi retomado o crescimento, sendo o ano com maior quantidade de tipos de comunicações científicas recuperadas sobre o tema.

Observando o gráfico é perceptível que o interesse pelo tema vem aumentando a cada ano. É importante destacar que futuras investigações possam ser realizadas a partir deste fator para saber quais os principais temas abordados pelos autores em suas investigações, visto que isso pode indicar tendências por temas. Além disso, os artigos em periódicos são os tipos de comunicações científicas preferidas pelos autores para divulgar suas pesquisas sobre o tema.

Gráfico 5 - Total de ocorrências de tipos de comunicações científicas, segmentados por ano e por tipo de comunicação científica, incluindo as comunicações científicas descartadas na análise, em valores absolutos.



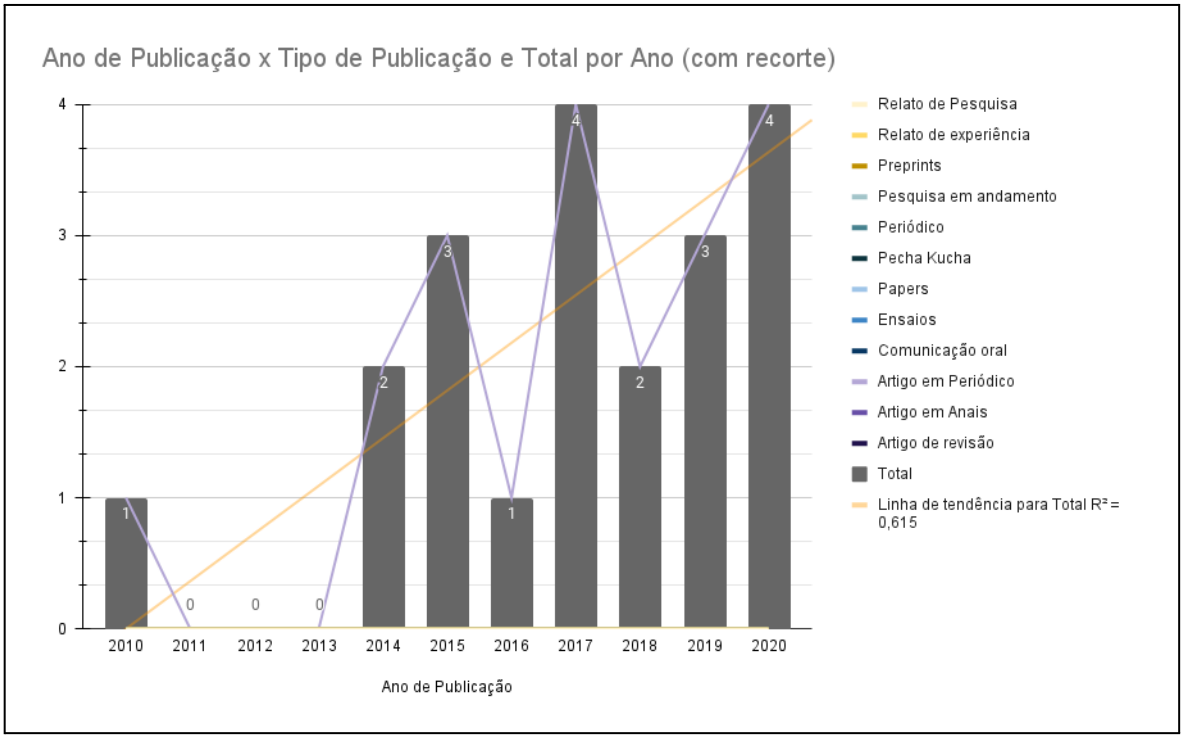
Fonte: Autora (2022).

O Gráfico 6 representa os tipos de comunicações científicas incluídas na RSL. Entre elas relaciona-se: Relato de pesquisa, Relato de experiência, Preprints, Pesquisa em andamento, Periódico, Pecha Kucha, Papers, Ensaios, Comunicação oral, Artigo em periódico, Artigo em anais e Artigo de revisão. Entretanto, o único tipo de comunicação inserida na RSL foram os Artigos em periódicos por atenderem aos critérios de inclusão e de exclusão definidos nos procedimentos metodológicos.

Portanto, foram 20 Artigos em periódicos revisados com ocorrências nos anos de: I) 2010 com (1) ocorrência, 2014 com (2) ocorrências, 2015 com (3) ocorrências, 2016 com

(1) ocorrência, 2017 com (4) ocorrências, 2018 com (2) ocorrências, 2019 com (3) ocorrências e 2020 com (4) ocorrências. A partir do Gráfico 6 é possível perceber oscilações no quantitativo de comunicações científicas revisadas, percebendo-se quedas nos anos de 2016 e 2018 e altas em 2019 e 2020 Ainda assim, este quantitativo foi satisfatório para a realização da RSL.

Gráfico 6 - Total de ocorrências de tipos de comunicações científicas, segmentados por ano e por tipo de comunicação científica, excluindo as comunicações científicas descartadas na análise, em valores absolutos.



Fonte: Autora (2022).

A Tabela 14 é referente à ocorrência de palavras-chave identificadas nas comunicações científicas e foram segmentadas por base de conhecimento. Ressalta-se que as comunicações científicas em que não foi possível identificar as palavras-chave foram excluídas dos resultados.

Para esta análise foram consideradas as ocorrências totais maiores ou iguais a 10. As 836 palavras-chaves identificadas nas comunicações científicas foram segmentadas entre as 3 bases de conhecimento, BRAPCI, SciELO e EBSCOhost. As palavras-chave com as maiores ocorrências totais foram: “Rede” total de 117, “Mídia” total de 93, “Mídias sociais" total de 79, “Redes sociais” com total de 72 ocorrências. Percebe-se que essas palavras-chave assim como as palavras-chaves “Rede social” com um total de 35 ocorrências, “Redes sociais online” com um total de 21 ocorrências e “Privacidade” com um total de 18 ocorrências tem alguma similaridade com as strings definidas nos

Procedimentos Metodológicos, embora estas últimas com um menor quantitativo de ocorrências em relação ao primeiro grupo de palavras-chaves.

Baseado nesta observação e na posição que a palavra-chave “Privacidade” ocupa na Tabela 14 é possível perceber que o tema não apareceu entre as palavras-chave com as maiores ocorrências. Isso pode indicar a necessidade de mais pesquisas relacionadas ao tema, especialmente no Brasil. Entretanto é necessário realizar outros estudos a partir desta observação a fim de comprovar ou não esta percepção inicial.

Tabela 14 - Total de ocorrências de palavras-chave, segmentados por Base de Conhecimento, incluindo as comunicações científicas descartadas na análise, em valores absolutos (n >= 10).

Palavras-Chave	**BRAPCI**	**SciELO**	**EBSCOhost**	**Total de Ocorrências**
REDE	29	40	48	**117**
MÍDIA	6	77	10	**93**
MÍDIAS SOCIAIS	1	72	6	**79**
REDES SOCIAIS	8	27	37	**72**
INFORMAÇÃO	28	15	20	**63**
SAÚDE	4	29	6	**39**
COMUNICAÇÃO	7	14	15	**36**
INTERNET	1	24	11	**36**
REDE SOCIAL	20	9	6	**35**
FACEBOOK	16	9	8	**33**
TECNOLOGIA	1	10	17	**28**
POLÍTICA	2	9	12	**23**
CIÊNCIA DA INFORMAÇÃO	21	0	0	**21**
REDES SOCIAIS ONLINE	4	6	11	**21**
PRIVACIDADE	4	9	5	**18**
EDUCAÇÃO	1	13	3	**17**
CONHECIMENTO	6	2	5	**13**
MEDIA	5	5	3	**13**
BRASIL	4	5	3	**12**
COMPORTAMENTO	2	5	5	**12**
TECNOLOGIAS	0	3	9	**12**
BIBLIOTECONOMIA	7	1	3	**11**
LAR	0	2	9	**11**
TECNOLOGIA DA INFORMAÇÃO	1	5	5	**11**
ÉTICA	0	8	2	**10**
Total de Ocorrências	**178**	**399**	**259**	**836**

Fonte: Autora (2022).

A Tabela 15 é referente a ocorrências de palavras-chave apenas das comunicações científicas incluídas na RSL, sendo analisadas as ocorrências de palavras-chave com resultado total: maior ou igual a 2.

Enfatiza-se que as comunicações científicas que não possuem palavras-chave foram excluídas dos resultados apresentados nesta Tabela. A descrição do resultado será igual ao

da Tabela anterior sendo portanto destacadas as palavras-chaves com maiores ocorrências sendo elas: “Rede” com um total de (13) ocorrências, “Redes sociais” com um total de (11) ocorrências, “Privacidade” com um total de (8) ocorrências e “Facebook” com um total de (4) ocorrências.

Essas palavras-chaves têm relação de forma mais direta com o tema investigado, embora as demais com um quantitativo menor de ocorrência também tenham relação direta ou indireta com o tema, sendo portanto um dos fatores que levou a incluir as comunicações científicas na RSL.

Tabela 15 - Total de ocorrências de palavras-chave, segmentados por Base de Conhecimento, excluindo as comunicações científicas descartadas na análise, em valores absolutos (n >= 2).

Palavras-Chave	BRAPCI	SciELO	EBCOHost	Total de Ocorrências
REDE	0	6	6	12
REDES SOCIAIS	0	6	5	11
PRIVACIDADE	1	4	2	7
FACEBOOK	1	0	3	4
INFORMAÇÃO	1	1	1	3
INTERNET	0	2	1	3
TECNOLOGIA	0	2	1	3
CONFIDENCIALIDADE	0	2	0	2
DIREITOS	0	1	1	2
EDUCAÇÃO	0	2	0	2
ÉTICA	0	1	1	2
INSTAGRAM	0	0	2	2
JOVENS	0	1	1	2
SEGURANÇA	0	1	1	2
TECNOLOGIAS	0	2	0	2
Total de Ocorrências	**3**	**31**	**25**	**59**

Fonte: Autora (2022).

A Tabela 16 apresenta as ocorrências de palavras-chaves segmentadas por string, sendo consideradas as ocorrências de palavras-chaves com resultado total maior ou igual a 10. A Tabela 16 inclui as comunicações científicas descartadas na análise. É importante salientar que foram excluídos os resultados de comunicações científicas em que não foi possível identificar as palavras-chave.

A palavra-chave “Rede” foi recuperada com a utilização de todas as strings, tendo o maior quantitativo de ocorrências dentre as palavras-chave da Tabela 16 com (117) ocorrências no total. Portanto este é um termo de recuperação de comunicações científicas a ser incluído nas pesquisas em bases de conhecimento. Bem como as palavras-chaves similares tais como: “Redes sociais”, “Rede social”, “Redes sociais online”, "Mídia" e "Mídias sociais”.

É relevante dizer que os SRSO têm relação com outros termos tais como Informação, Ciência da Informação, TIC, Ética, Comportamento, Comunicação, Saúde, Política, Internet e Privacidade. Portanto, este é um tema que é discutido em vários segmentos da ciência, tanto social como da saúde e da educação.

Em ordem decrescente as palavras-chaves com as maiores ocorrências foram

1. “Rede” com 117 ocorrências no total;
2. “Mídia” com 93 ocorrências no total;
3. “Mídias sociais” com 79 ocorrências no total;
4. “Redes sociais” com 72 ocorrências no total.

Os resultados por palavras-chave com as menores ocorrências identificadas com alguma relação direta com o tema foram:

1. “Rede social” com 35 ocorrências no total;
2. “Redes sociais online” com 21 ocorrências no total;
3. “Privacidade” com 18 ocorrências no total.

Tabela 16 - Total de ocorrências de palavras-chave, segmentados por string, incluindo as comunicações científicas descartadas na análise, em valores absolutos (n >= 10).

Palavras-Chave	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
REDE	37	17	29	6	3	1	24	**117**
MÍDIA	9	0	4	1	0	1	78	**93**
MÍDIAS SOCIAIS	4	0	1	0	0	1	73	**79**
REDES SOCIAIS	23	7	23	3	1	1	14	**72**
INFORMAÇÃO	15	11	13	6	4	0	14	**63**
SAÚDE	4	3	1	1	1	0	29	**39**
COMUNICAÇÃO	13	8	3	1	1	0	10	**36**
INTERNET	2	1	11	0	0	2	20	**36**
REDE SOCIAL	12	9	4	3	1	0	6	**35**
FACEBOOK	14	6	3	3	2	0	5	**33**
TECNOLOGIA	3	5	10	1	1	0	8	**28**
POLÍTICA	6	5	5	0	0	0	7	**23**
CIÊNCIA DA INFORMAÇÃO	9	4	2	4	2	0	0	**21**
REDES SOCIAIS ONLINE	17	0	2	2	0	0	0	**21**
PRIVACIDADE	1	1	14	1	1	0	0	**18**
EDUCAÇÃO	1	2	3	0	0	1	10	**17**
CONHECIMENTO	2	2	5	1	1	0	2	**13**
MEDIA	4	1	4	0	0	0	4	**13**

Palavras-Chave	Redes sociais online	Redes sociais on-line	Redes sociais AND privacidade	Redes sociais online AND privacidade	Redes sociais on-line AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total de Ocorrências
BRASIL	3	3	1	1	0	0	4	**12**
COMPORTAMENTO	2	1	4	1	0	0	4	**12**
TECNOLOGIAS	3	3	5	1	0	0	0	**12**
BIBLIOTECONOMIA	3	5	1	1	1	0	0	**11**
LAR	1	2	5	1	0	0	2	**11**
TECNOLOGIA DA INFORMAÇÃO	0	2	2	0	1	0	6	**11**
ÉTICA	2	0	5	0	0	0	3	**10**
Total de Ocorrências	**190**	**98**	**160**	**38**	**20**	**7**	**323**	**836**

Fonte: Autora (2022).

Por fim, a Tabela 17 trata das ocorrências de palavras-chave por strings e inclui apenas os resultados referentes às comunicações científicas incluídas na RSL, sendo relacionadas na Tabela as com ocorrências totais maiores ou igual a 2. É importante destacar que foram excluídos os resultados de comunicações científicas em que não foi possível identificar as palavras-chave.

Seguindo a mesma base das Tabelas anteriores destaca-se aqui apenas as palavras-chaves com as maiores ocorrências totais e com alguma similaridade com as strings definidas no Procedimento Metodológicos, sendo elas:

1. “Rede” 12 com ocorrências no total;
2. “Redes sociais” com 11 ocorrências no total;
3. “Privacidade” com 7 ocorrências no total.

Analisando a Tabela 17 percebe-se que as comunicações científicas revisadas trouxeram o tema de SRSO e privacidade dentro do enfoque do “Direito”, da “Ética”, da “Educação”, da “Informação”, da “Tecnologia”, da “Internet”, da “Segurança”, da “Confidencialidade”, assim como as outras palavras-chave relacionados na Tabela 17, notando-se assim uma relação direta e indireta das comunicações científicas com o tema de SRSO e os potenciais riscos para a privacidade.

Tabela 17 - Total de ocorrências de palavras-chave, segmentados por string, excluindo as comunicações científicas descartadas na análise, em valores absolutos (n >= 2).

Palavras-Chave	**Redes sociais online**	**Redes sociais on-line**	**Redes sociais AND privacidade**	**Redes sociais online AND privacidade**	**Redes sociais on-line AND privacidade**	**Mídias sociais AND privacidade**	**Mídias sociais**	**Total de Ocorrências**
REDE	1	1	9	0	0	0	1	**12**
REDES SOCIAIS	1	1	8	0	0	0	1	**11**
PRIVACIDADE	1	0	6	0	0	0	0	**7**
FACEBOOK	1	1	2	0	0	0	0	**4**
INFORMAÇÃO	1	0	2	0	0	0	0	**3**
INTERNET	0	1	1	0	0	0	1	**3**
TECNOLOGIA	0	1	2	0	0	0	0	**3**
CONFIDENCIALIDADE	0	0	2	0	0	0	0	**2**
DIREITOS	0	0	2	0	0	0	0	**2**
EDUCAÇÃO	0	1	0	0	0	0	1	**2**
ÉTICA	0	0	2	0	0	0	0	**2**
INSTAGRAM	1	0	1	0	0	0	0	**2**
JOVENS	0	1	1	0	0	0	0	**2**
SEGURANÇA	0	0	2	0	0	0	0	**2**
TECNOLOGIAS	0	1	1	0	0	0	0	**2**
Total de Ocorrências	**6**	**8**	**41**	**0**	**0**	**0**	**4**	**59**

Fonte: Autora (2022).

4 REVISÃO SISTEMÁTICA DE LITERATURA - ANÁLISE QUALITATIVA

Nesta seção são detalhadas as características de cada uma das comunicações científicas, de forma individual, dividida em subseções. Para cada comunicação científica construiu-se uma síntese, observando-se como os autores tratam o tema de privacidade e de SRSO.

4.1 Sociedade de controle e redes sociais na internet: #saúde e #corpo no Instagram, por Leitzke e Rigo

O estudo discute aspectos teóricos no campo das TIC, enfatizando tópicos tais como: a) a sociedade de controle, b) o biopoder, c) a vigilância, d) a regulação das informações, e) o computador como instrumento de poder, f) a internet e redes de relacionamentos, g) as redes sociais, h) a saúde e corpo (LEITZKE; RIGO, 2020).

A fonte de pesquisa utilizada pelos autores foram algumas publicações coletadas no *Instagram,* com imagens de homens e de mulheres em suas atividades físicas e de seus resultados. O estudo buscou evidenciar a "[...] operacionalização dos mecanismos de governamentalidade no contexto da sociedade de controle" (LEITZKE; RIGO, 2020, p. 3).

Os autores identificaram nas postagens coletadas do *Instagram* fatos sobre a existência de uma sociedade de controle baseada em práticas e estratégias (LEITZKE; RIGO, 2020) tais como:

a) Confissão, intervenção e manipulação do corpo;
b) Relações entre corpo, saúde e beleza;
c) Uso de estratégias tanto para a manutenção de saúde como da "normalização dos sujeitos";
d) Prescrição;
e) Responsabilização;
f) Criação de desejos.

A existência de relações de poder e de uma sociedade de controle se faz presente por meio de opiniões e discursos de vigilância divulgados em SRSO. As publicações feitas por indivíduos, partes dessa sociedade de controle, sustentam a ideia de corpos sem defeitos, conseguidos por meio de dietas, de procedimentos estéticos ou de rotinas diárias nas academias. As referidas publicações são vendidas como fórmulas milagrosas para o alcance de um corpo ideal a ser aceito pela sociedade (LEITZKE; RIGO, 2020).

As próprias características estruturais dos SRSO, segundo Leitzke e Rigo (2020), permitem que os usuários criem estratégias de confissões em que eles demonstrem como

eles estão se saindo em seus treinos nas academias ou para revelem dietas que deram certo. Portanto, a pesquisa conclui que a exibição do corpo saudável é o resultado ou a comprovação que os usuários estão no caminho certo para se ter o corpo perfeito.

4.2 As redes sociais na internet e suas apropriações por jovens brasileiros e portugueses em idade escolar, por Rosado e Tomé

A utilização dos SRSO e a produção de dados por estudantes portugueses e brasileiros é o ponto central das discussões do estudo de Rosado e Tomé (2015)**.** Os autores afirmam, por exemplo, que os SRSO funcionam como uma rede paralela à internet (ROSADO; TOMÉ, 2015).

Essa "rede paralela" cresce à medida em que se oferta aplicativos para *download* direto em dispositivos móveis, fazendo com que os usuários possam permanecer muito mais tempo logados (ROSADO; TOMÉ, 2015).

O tempo de permanência dos usuários em SRSO pode ser um fator em potencial para a ocorrência de riscos relacionados à privacidade de dados, pois quanto maior é a sua permanência maior será o tempo de exposição e consequentemente de produção de conteúdo de dados e de coleta por terceiros (ROSADO; TOMÉ, 2015).

A associação da educação de jovens ao fenômeno de SRSO oportuniza novas formas de aprendizagem, de comunicação e de interação. Os autores argumentam que os SRSO são extensões das relações sociais presenciais vividas no espaço físico da escola, o que está sustentado com dados estatísticos no artigo (ROSADO; TOMÉ, 2015).

Os SRSO são nutridos diariamente com a produção de conteúdos, tais como comentários, vídeos e fotografias. Também servem como meio de compartilhamento de links. Além disso, os SRSO são como tipos de *websites ou gêneros de websites*, constituído por redes coletivas de participantes que produzem conteúdos variados (ROSADO; TOMÉ, 2015).

Os autores definem os SRSO enquanto estruturas em que a unidade básica está configurada em nós. Os nós representam cada indivíduo ou instituição, podendo ser ligados uns aos outros, formando novos nós dentro de uma rede de relações. Em geral, cada perfil representa um indivíduo, embora cada indivíduo possa ter mais de um perfil (ROSADO; TOMÉ, 2015).

Diante desses conceitos e aspectos debatidos no estudo, os autores desenvolveram uma investigação a respeito do processo de domínio de jovens sobre os SRSO e a aprendizagem e de como eles se comportam em relação a esses fatores. Para os autores, a

“[...] educação cuja referência é a cultura constituída com os suportes analógicos, impressos ou eletrônicos de transmissão massiva, voltada à memorização, ao uso de testes e ensino passo a passo, não compatíveis com esse novo modo de agir e pensar dos nativos” (ROSADO; TOMÉ, 2015, p. 16).

O estudo conclui que o uso de dispositivos móveis com acesso à internet e, por conseguinte, aos SRSO é uma tendência entre estudantes brasileiros e portugueses, embora perceba-se que os estudantes brasileiros acessem mais os SRSO por meio de dispositivos móveis do que os portugueses, conforme observa-se no Quadro 9 (ROSADO; TOMÉ, 2015).

Quadro 9 - Variação cultural quanto ao uso de SRSO.

Uso de SRSO	**Estudantes**	
	Brasileiros	**Portugueses**
Uso diário e elevado de SRSO (Facebook, Orkut, Youtube)	Sim	Sim
Diversidade de uso de dispositivos tecnológicos (smartphones, computador pessoal, ou da família ou de amigos) para acesso aos SRSO.	Sim	Sim
Maior acesso aos SRSO por meio de dispositivos móveis (smartphones).	Sim	Não
Uso simultâneo de diferentes SRSO.	Sim	Sim
Uso de multiperfis de usuários.	Sim	Sim
Divulgam dados mais de terceiros do que de si mesmos	Não	Sim
Não têm problemas com a revelação de dados pessoais. Assim divulgam seu nome completo e nome da escola que frequentam.	Sim	Não
Tem preferência em postar imagem do próprio rosto, seja individualmente ou com amigos ou familiares em seus perfis.	Sim	Não
Quanto mais a idade avança, menos os indivíduos se preocupam com a privacidade de dados (exposição de fotografias), por exemplo.	Não	Sim

Fonte: Adaptado pela Autora de Rosado e Tomé (2015).

Embora as conexões estabelecidas nos dois países sejam equilibradas, foi observado que conforme a idade avança, mais amigos são conectados às suas redes de relacionamentos. Outro ponto de equilíbrio percebido no público investigado são as relações distantes que preferem manter com seus familiares ou professores de escola (ROSADO; TOMÉ, 2015).

A revelação de dados por estudantes está diretamente ligada ao fator idade, é o que afirma Rosado e Tomé (2015). Quanto maior a idade dos investigados de Portugal, mais dados tendem a revelar sobre si sendo, portanto, eventuais usuários passíveis de coleta de dados pelas empresas.

> Existe uma forte influência do fator idade para a definição do aprofundamento nos usos das redes sociais on-line pelos jovens. À medida que vão amadurecendo, mais amigos são feitos (laços fracos),

> mais amizades fora do espaço de convivência presencial são tecidas, diminuindo a comunicação com pais e professores. Eles vão se tornando mais independentes e passam a acessar as redes via celular e computador pessoal, entrando aos poucos na lógica do multiacesso e da mobilidade e publicando conteúdos próprios com maior frequência (ROSADO; TOMÉ, 2015, p. 22).

Existem dois tipos de usuários de SRSO. Os primeiros são os nativos digitais, denominados assim devido ao alto grau de participação no uso de SRSO, cuja comunicação e relação ocorre em sua maioria com indivíduos que a priori têm a mesma idade do que eles (ROSADO; TOMÉ 2015).

Os autores alertam para a criação de perfis por públicos menores de 13 anos. Segundo Rosado e Tomé (2015, p. 20)

> Apesar de a criação de perfil no Facebook (e em outras redes como Orkut e Linkedin) ser permitida apenas a maiores de 13 anos de idade, muitos jovens brasileiros e portugueses afirmaram terem criado seus perfis com 12 anos ou menos (alguns chegam aos sete anos de idade), evidenciando que os controles formais nesses sites não são eficazes a ponto de inibir o acesso de adolescentes e crianças.

O segundo tipo de usuário são denominados de migrantes digitais, que podem ser tanto os familiares dos estudantes (nativos digitais) quanto a escola (instituição). Este tipo de usuário tem baixa interação com os estudantes devido à pouca frequência de acesso e uso dos SRSO (ROSADO; TOMÉ, 2015).

As semelhanças entre esses dois grupos mostraram que tanto os estudantes do Brasil quanto os de Portugal são usuários em potencial dos SRSO. Em geral, os SRSO são utilizados pelos estudantes como forma de conectar relações sociais e de produzir conteúdo de dados (ROSADO; TOMÉ, 2015).

4.3 Protagonismo dos estudantes de medicina no uso do Facebook na graduação, por Purim e Tizzo

Este estudo trata de aspectos sobre uso de SRSO enquanto tecnologias que podem auxiliar no processo de aprendizagem. Por outro lado, essas mesmas tecnologias levantam discussões relativas à ética, à segurança e à privacidade no campo da saúde, especificamente da medicina (PURIM; TIZZOT, 2019).

O estudo investigou como os estudantes do curso de medicina da Universidade Federal do Paraná (UFPR) utilizam o *Facebook* para a atividade de aprendizagem. Para isso foram abordadas algumas questões na investigação tais como: a adesão dos estudantes aos SRSO, a frequência de uso, as vantagens ou desvantagens observadas pelos estudantes

e a verificação de conhecimento dos estudantes sobre a conduta ética quanto ao uso dos SRSO (PURIM; TIZZOT, 2019).

A investigação dos autores resultou em informações sobre o uso de SRSO. A primeira delas é que a grande maioria dos estudantes de graduação em medicina indicaram algum tipo de vantagem no uso de SRSO, dentre elas cita-se: formação de grupos, compartilhamento de informações, interação entre as pessoas, rapidez e democracia, facilidade, rapidez e compartilhamento (PURIM; TIZZOT, 2019).

Outros estudantes relataram em suas respostas desvantagens sobre o uso do SRSO *Facebook*, indicando em primeiro lugar na pesquisa a falta de privacidade, com (34,5%), seguidos da distração e perda de foco (19,7%), questões éticas (11%), dificuldade de inclusão digital (4,2%), disponibilidade de tempo dos professores (3,5%), vício e dependência da internet (1,6%) e conteúdos duvidosos (1,3%) (PURIM; TIZZOT, 2019).

As ferramentas mais utilizadas do *Facebook* pelos estudantes foram os documentos (84,2%), o mural (55%), o bate-papo (50%) e os eventos (49%). No aspecto finalidade, o estudo indica que os estudantes utilizam o SRSO *Facebook* para: a) verificar avisos com representantes e atualizar cronograma, b) resolver e/ou tirar dúvidas para fazer trabalho *on-line,* c) obter matéria dada em aula; d) discutir casos clínicos (PURIM; TIZZOT, 2019).

Outro ponto relevante no estudo é o debate que se faz sobre a privacidade. Purim e Tizzot afirmam que “Debater casos clínicos respeitando a privacidade e o anonimato inerentes ao ato médico é uma das estratégias que permitem análise crítica e interdisciplinar de diversas situações que ocorrem no cotidiano” (PURIM; TIZZOT, 2019, p. 193) .

Dentre os achados sobre a privacidade no estudo relacionado ao uso do *Facebook* pelos estudantes de graduação verifica-se a existência dos chamados dilemas sobre os: I) Limites da vida privada; II) Limites da confidencialidade de informações, alcançadas tanto dentro como fora dos ambientes médicos (PURIM; TIZZOT, 2019).

Além disso, foi abordado no estudo o papel das Normas Profissionais no uso de SRSO no que diz respeito à divulgação de imagens. Em relação a isso os autores detectaram que a grande maioria dos estudantes desconhecem as normas que são emitidas sobre a divulgação de imagens (PURIM; TIZZOT, 2019).

Sobre essa ausência de conhecimento sobre as “Recomendações éticas” por parte dos estudantes, Purim e Tizzot argumentam que é necessário realizar ações de cunho formativo tanto aos discentes quanto aos docentes, pois na visão dos autores isso poderia

minimizar as questões de segurança, ética e de educação no curso de medicina (PURIM; TIZZOT, 2019).

Os autores apresentam como proposta para a segurança dos dados quanto ao uso de SRSO: a) a aplicação de investimentos e treinamento de docentes e estudantes; b) a implantação de regras quanto ao uso de SRSO pelos estudantes de medicina; c) o uso de sistemas como BMJ Learning para a formação médica; d) o desenvolvimento de uma rede inter colaborativa formada por docentes e estudantes voltada para a realização de monitoramento e privacidade.

4.4 Pesquisando co-viewing em redes sociais e aplicativos de mensagem instantânea: ética e desafios, por Sá

A principal discussão do estudo foi verificar quais são as "[...] preocupações e os desafios éticos que devem ser considerados durante o estudo da prática de covisualização (televisão social) dos conteúdos audivisuais [...]" em SRSO (SÁ, 2018, p. 391).

Foi mencionado que os ambientes digitais são relevantes fontes de pesquisas e se mostram presentes no dia a dia dos indivíduos. Apesar disso, trazem a estes vantagens e desvantagens, e uma das vantagens é o menor tempo gasto na realização de pesquisas (SÁ, 2018).

Pode se dizer que o fenômeno da covisualização conectada ou da televisão social que ocorre por meio dos SRSO é algo novo a ser considerado. O fenômeno pode ser observado na interação dos indivíduos com outros indivíduos por meio de dispositivos tecnológicos. Essa interação de acordo com Sá é diversificada (SÁ, 2018) e pode ocorrer com

a) Indivíduos sozinhos fisicamente, podem estar conectados coletivamente com outros indivíduos *online;*
b) Indivíduos podem estar acompanhados de outros indivíduos offline e on-line;
c) E, de maneira tradicional, em que os indivíduos assistem juntos seu programa televisivo.

A covisualização se dá por meio de instrumentos tecnológicos, seja um aparelho de televisão ou seja por meio de *smartphones*, ou ainda de interfaces de SRSO. O que se ressalta é que todos esses instrumentos são capazes de promover a interação entre os indivíduos. Mas ao mesmo tempo a covisualização em SRSO deixam rastros de dados (SÁ, 2018).

Aspectos sobre a privacidade são elencados no estudo. O primeiro deles é a exigência de fornecimento de metadados como critério para acesso aos SRSO, tais como: endereço de email, nome e CPF (SÁ, 2018).

A "[...] percepção de privacidade não é absolutamente evidente" (SÁ, 2018, p. 400). E quando o autor destaca este ponto, é porque mesmo diante de tantas pesquisas já realizadas sobre o tema e de tantas perguntas feitas com os usuários sobre o assunto, ainda sim não há um entendimento definido sobre o que seja privacidade ou de como se possa preservar os dados (SÁ, 2018).

A percepção dos usuários sobre a privacidade pode estar relacionada com a possível ausência de preocupação com o que está descrito nos Termos e nas Condições de Uso em SRSO (SÁ, 2018).

Características referentes aos SRSO também são mencionadas no estudo. Discute-se por exemplo se o *Facebook* é uma plataforma pública ou não. Devido às suas configurações entende-se que se trata de uma plataforma pública, mas que pode ser também privada. O *status* de um perfil de público ou privado é normalmente definido pelo indivíduo no ato de criação de seu registro de acordo com as configurações disponíveis nas plataformas de SRSO (SÁ, 2018).

Na visão de Sá, as páginas de grupos fechados criadas no *Facebook* são investigadas no estudo e foram consideradas semi públicas, uma vez que as postagens feitas por um membro ou outro podem ser visualizadas apenas por seus integrantes (SÁ, 2018).

4.5 A publicitação do privado na era da pós-verdade: uma exploração às redes sociais dos líderes políticos portugueses, por Barriga

A questão central do estudo foi determinar "[...] a centralidade e a visibilidade que os líderes políticos dão à exposição de outras mensagens que estão além do discurso público e do debate político", tendo como fonte de investigação o *Twitter,* o *Facebook* e o *Instagram* (BARRIGA, 2020, p. 58).

A proposta do autor foi realizar uma investigação exploratória em SRSO a fim de verificar tipos de participações políticas por meio de conteúdos publicados por políticos de diferentes partidos pertencentes à [...] Assembleia da República portuguesa [...] (BARRIGA, 2020, p. 58).

No que diz respeito aos aspectos teóricos discutidos no estudo sobre os SRSO e sobre a privacidade, foi possível observar a partir do entendimento de Barriga (2020) sinais da existência de uma dicotomia entre o público x privado.

Existem outras dicotomias observadas e identificadas no uso de SRSO como por exemplo, a divulgação de dados (usuários) x apropriação de dados (empresas) ou mesmo o uso de SRSO como meio de comunicação x ou para uso recreativo. E por fim, o uso de SRSO com a intenção de Vigiar x Ser vigiado (BARRIGA, 2020).

A divulgação de dados pelos usuários muitas vezes são realizadas de forma deliberada, sem cuidado algum. A vigilância sobre os usuários e de seus passos nos SRSO é uma consequência desse processo. “Em nome da melhoria de qualidade do serviço, desenvolvem-se formas de vigilância mais sofisticadas que o panóptico de Bentham [...]" (BARRIGA, 2020, p. 62).

Em nome da interação e do uso recreativo é que se afirma que a privacidade pode estar desaparecendo ou pode estar bastante comprometida, afinal os SRSO são ambientes gratuitos, que coletam qualquer rastro deixado por um indivíduo (BARRIGA, 2020).

Para Barriga (2020), a privacidade de dados explicita outros aspectos presentes nos SRSO que envolvem a:

1. Consolidação de uma sociedade de controle (com ações de vigilância, de manipulação, de apropriação de dados), análoga à sociedade de vigilância de Michel Foucault, na qual os indivíduos eram controlados por paranópticos;
2. Desvalorização da privacidade. A inovação tecnológica modifica a sociedade com o uso por exemplo de SRSO, principalmente quanto à concepção de valor;
3. Apropriação de dados pelas empresas, indicando ainda que esse processo é pouco conhecido pelos indivíduos;
4. Visibilidade desejada, ou seja tudo ou quase tudo que um indivíduo expõe, publiciza nos SRSO de sua vida íntima é feito de forma voluntária e deliberada.

Se constata sobre as empresas de TIC que elas criam formas variadas de vigilância, contribuem para a formação de uma sociedade em rede e ao mesmo tempo exercem controle sobre essa mesma sociedade (BARRIGA, 2020).

Diante disso, o autor faz uma analogia entre a sociedade observada na microfísica do poder de Foucault controlada por meio de panóptico e o novo tipo de controle exercido pelas TIC, simbolizado pela internet. O poder colocado em foco, nesta nova sociedade tem

a capacidade de não somente controlar, mas de envolver o "corpo social" por meio de seduções que os SRSO (produto das TIC) oferecem (BARRIGA, 2020).

Os dispositivos móveis contribuem para que os indivíduos possam ser controlados e vigiados dentro de suas próprias moradias ou em qualquer lugar uma vez que os Apps, como o *FaceApp* podem ser instalados e armazenados em *smartphone*, sendo segundo Barriga uma provável vulnerabilidade para a privacidade dos usuários (BARRIGA, 2020).

O uso de dispositivos móveis e de SRSO está relacionado com a dicotomia público x privado e é um assunto ainda muito difícil de se entender mesmo porque a forma como os usuários se comportam quando utilizam os SRSO e o que estes significam para eles tornam essa distinção ainda mais difícil de ser compreendida (BARRIGA, 2020).

Os SRSO colaboram para a proliferação de potenciais riscos para a privacidade. Em primeiro lugar eles são utilizados de forma intensa pelos indivíduos. São projetados para atender aos interesses de empresas de TIC, de governos, de organizações políticas e terroristas. Em segundo lugar, são fontes de disseminação de notícias falsas (*fake news*), intensificam o populismo e dão chance também à desinformação (BARRIGA, 2020, p. 62).

Sobre a vigilância, Barriga menciona ainda que tanto o Estado, quanto as organizações "[...] detêm grandes quantidades de dados [...]" (2020, p. 62). Mas o problema é ainda mais preocupante quando se descobre que este tipo de domínio não acontece apenas nessas instâncias, mas também na relação entre os indivíduos, em que um um exerce poder sobre o outro (Barriga, 2020).

Mas existem contrapontos sobre a vigilância. Se as TIC, representada neste estudo pelos SRSO obtém vantagens a partir da prática de vigilância de dados dos usuários, estes por sua vez são ao mesmo tempo vigiadas e sofrem penalidades quando enfrentam escândalos de vazamento de dados como no caso do Facebook (BARRIGA, 2020).

Em relação aos reflexos do uso dos SRSO pelos políticos e a exposição da privacidade observou-se no estudo que: I) o conteúdo produzido pode ser produzido não somente pelos políticos mas por seus assessores de comunicação dos partidos políticos e até mesmo de maneira articulada entre os dois; II) comentários feitos por jornalistas sobre os *tweets* postados por políticos são desviados do assunto político, os quais deveriam ser o foco para assuntos estritamente privados, e que deveriam dizer respeito somente aos políticos; III) sobre o *Twitter* existe uma mescla de configurações que fazem perceber que não existem características únicas e bem definidas, sendo considerados ambientes híbridos,

uma vez que não há distinção entre o que é público e o que se pode ser considerado privado. Nos SRSO são tratados assuntos desde questões políticas até algo do cotidiano (BARRIGA, 2020).

O autor analisou no estudo alguns tipos de postagens realizadas pelos políticos nas campanhas eleitorais em alguns SRSO. De maneira geral foi constatado sobre as postagens que (BARRIGA, 2020):

a) As lideranças políticas pouco realizaram postagens sobre suas vidas particulares;
b) Apesar de existir uma preocupação com a exposição da vida privada de políticos, percebeu-se no estudo que isto não é tão recorrente quanto em outras mídias como a televisão;
c) Uma vantagem percebida é que os SRSO possibilitam uma autonomia e ao mesmo controle sobre aquilo que é publicado, protegendo assuntos privados e a própria imagem dos políticos;
d) A estrutura dos SRSO permite por outro lado uma "sobre-exposição" da imagem dos políticos e também proporciona a "personalização da política".

Diante de tudo isso Barriga afirma que "A internet apresenta-se como "democratizadora" e promotora de igualdade; mas os algoritmos que controlam e manipulam também perpetuam a desigualdade social" (BARRIGA, p. 68, 2020).

4.6 Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no Facebook, por Martorell, Nascimento e Garrafa

Percebe-se uma preocupação nas investigações sobre situações que coloquem em risco a privacidade de pacientes, como a exposição de imagens. São situações que estão diretamente ligadas com a quebra de confidencialidade. É o que o estudo de Martorell, Nascimento e Garrafa (2016) busca explicar.

Os escândalos envolvendo o acesso e o uso de informações chamaram a atenção de pesquisadores na área da saúde. Sobre isso, no que diz respeito à preservação de dados observou-se que é algo que faz parte da natureza ética e profissional e é também algo que os pacientes esperam (MARTORELL; NASCIMENTO; GARRAFA, 2016).

Essa preocupação ocorre devido ao aumento do uso de SRSO por profissionais de saúde. "[...] há uma crescente popularização do uso de redes sociais virtuais entre os profissionais de saúde, que passam a usar tal ferramenta publicando na internet informações sobre suas rotinas profissionais" (MARTORELL; NASCIMENTO; GARRAFA, 2016, p. 14).

Assim, os autores contribuem com o tema quando propõe no estudo identificar algumas situações que podem desencadear pelos profissionais da área da saúde a quebra de confidencialidade ou de privacidade em publicações de imagens no *Facebook* relacionadas a pacientes, de forma direta ou não (MARTORELL; NASCIMENTO; GARRAFA, 2016).

As imagens foram coletadas dos álbuns dos usuários, coletâneas de imagens publicadas no SRSO por um longo período pelos usuários. Para identificação e análise dos dados, as imagens foram divididas em grupos, Quadro 10. Sobre a análise realizada pelos autores é possível detectar alguns riscos relacionados à exposição de dados de pacientes pelos profissionais de saúde (MARTORELL; NASCIMENTO; GARRAFA, 2016). O primeiro deles é a revelação. No estudo os autores identificaram imagens de pacientes mas também de pessoas que não tinham relação com os profissionais.

Quadro 10 - Revelação de imagens postadas por profissionais de Saúde no *Facebook.*

Imagens por grupo	**Situação**	**O que foi revelado**
Grupo I	Postagens de pacientes.	Rostos completos de pacientes.
	Postagens de grupos de pacientes em atividades de saúde.	Rostos de crianças.
Grupo II	Imagens em centros cirúrgicos ou em consultórios dentários.	Parte dos rostos de pacientes.
Grupo III	Imagens de exames complementares como um exame radiológico de paciente foram publicadas pelo profissional de saúde.	Dados pessoais como nome completo do paciente foi exposto, tanto diretamente na fonte, neste caso no exame radiológico como no comentário do profissional.

Fonte: Adaptado pela Autora, a partir de Martorell, Nascimento e Garrafa (2016).

Os autores afirmaram que mesmo não sendo revelada a imagem de um rosto por completo de um paciente como acontece por exemplo em centros cirúrgicos, isso pode ocorrer por meio da associação de imagem por relativização, é o que empresas de SRSO fazem (MARTORELL; NASCIMENTO; GARRAFA, 2016).

A revelação de rostos de crianças, Grupo I, em imagens primárias de pacientes é um dos muitos perigos para a privacidade de indivíduos que talvez nem sequer tenham um registro em um SRSO, como é o caso de crianças. Assim, percebe-se que há uma dupla exposição: a de imagens de pacientes e a de imagens de indivíduos que por acaso foram captadas e publicadas (MARTORELL; NASCIMENTO; GARRAFA, 2016).

Os profissionais de saúde divulgam imagens de seus feitos possivelmente sem autorização dos pacientes como forma de validar o serviço realizado (MARTORELL; NASCIMENTO; GARRAFA, 2016), e isso tem se tornado uma prática cada vez mais comum, principalmente por dentistas que realizam procedimentos estéticos.

Os dados de uma senhora do Grupo 3 foram expostos a partir da publicação de um exame radiológico da paciente, revelando seu nome sem o menor cuidado com a preservação de dados.

> [...] uma paciente exposta em duas instâncias: na própria imagem do exame e no comentário do médico responsável. Com o nome da paciente revelado, o título dado para esta imagem era: "Image challenge: o que será q é isso no peito da dona [nome da paciente]". O caso constava de uma fotografia de radiografia de tórax com uma imagem radiolúcida incomum, que incluía um rosário que a paciente esqueceu-se de retirar para fazer o exame, conforme, posteriormente, revelou o próprio médico. Com esse desafio lançado, houve 26 comentários para a fotografia, destacando-se dois deles: "Caraca! Primeiro, ela tem cardiomegalia... chumbinhos????"; "Nossa...expondo a bichinha desse jeito...ainda dá o last name...achei q era chumbinho tb...dona danada que gosta de matar passarinho" (MARTORELL; NASCIMENTO; GARRAFA, 2016, p. 16)

Os autores enfatizam sobre o direito de pacientes à privacidade que a) tanto o Estado quanto os Conselhos Profissionais devem garantir a proteção dos indivíduos, combatendo com o uso de meios legais a exposição indevida de imagens e de dados; b) o direito à privacidade é inalienável (MARTORELL; NASCIMENTO; GARRAFA, 2016).

Existem outras reflexões tratadas no estudo sobre as atitudes dos profissionais de saúde em relação à exposição de dados de pacientes. A primeira delas é saber se os pacientes receberam esclarecimentos dos profissionais sobre uso de imagem e o segundo é se consentiram que suas imagens fossem divulgadas (MARTORELL; NASCIMENTO; GARRAFA, 2016).

A exposição dos pacientes em situações de vulnerabilidade e sem poder de decisão sobre a divulgação de imagens é algo preocupante e deveria ser acompanhada mais de perto pelos conselhos éticos. A consequência que a exposição de dados dos pacientes pode trazer aos profissionais de saúde impacta diretamente na confiança que a sociedade deposita sobre eles. Os profissionais até podem divulgar seus feitos em SRSO desde que estejam seguros de que a privacidade dos usuários seja mantida na íntegra (MARTORELL; NASCIMENTO; GARRAFA, 2016).

O estudo apresentou também potenciais riscos para a privacidade de dados, descritos no Quadro 11.

Quadro 11 - Situações de risco à privacidade de dados.

Casos	**Situações**	**Risco a privacidade**
Caso 1	Identificação de imagens de crianças	Exposição de vulneráveis (crianças) dando margem ao uso da imagem por pedófilos.

Casos	Situações	Risco a privacidade
Caso 2	Identificação de nomes de pacientes a partir de divulgação de uma imagem radiológica. A imagem mostrava que a paciente havia esquecido de retirar seu escapulário para a realização do exame, e isso gerou alguns comentários.	Ridicularização e Associação. Foram emitidos comentários insinuando que talvez se tratasse de uma matadora de passarinho, pois a paciente poderia ter engolido chumbinho ou que a paciente pudesse ser uma de traficante de drogas.
Caso 3	Imagem de um paciente com bigode	Impossibilidade de controle do profissional sobre comentários maldosos. Um indivíduo por exemplo mencionava que deveria ser ateado fogo no bigode do paciente.

Fonte: Adaptado pela Autora, a partir de Martorell, Nascimento e Garrafa (2016).

A publicização por profissionais de saúde de imagens de pacientes em cenários de hospitais ou em outras situações de atendimento, caso 1, pode permitir que outros indivíduos como as crianças sejam identificáveis. As imagens de crianças obtidas a partir das imagens publicadas de pacientes originais podem ser alvos de utilização por pedófilos (MARTORELL; NASCIMENTO; GARRAFA, 2016).

O caso 2 tem relação com o subgrupo “Distorção” do Grupo Disseminação de Informações (RODRIGUES; SANT'ANA, 2016). Neste caso a imagem foi distorcida de seu contexto original, levando usuários a terem várias interpretações sobre o ocorrido, levando a paciente a ser confundida com uma traficante de drogas, o que acarreta à paciente já fragilizada um enorme constrangimento por meio de chamados “[...] dano extensivo, já que se trata de uma rede social leiga, onde as imagens são acessadas por usuários que não detêm informações adequadas, muito menos formação na área e, com frequência, interagem com as imagens por meio de comentários pejorativos e desrespeitosos [...]” (MARTORELL; NASCIMENTO; GARRAFA, 2016, p. 18).

O caso 3 de exposição de imagem de um paciente com bigode pode ser um reflexo da banalização de rotinas profissionais divulgadas em SRSO sem qualquer tipo de controle por esses profissionais. Por tudo isso, Martorell, Nascimento e Garrafa afirmam que os pacientes já estão vulneráveis pela própria condição em que se encontram e expô-los em um SRSO os tornam mais vulneráveis ainda (MARTORELL; NASCIMENTO; GARRAFA, 2016).

Por isso os autores alertam que existem leis que visam proteger dados como a identidade e a privacidade dos indivíduos. E a violação dessas leis pode acarretar danos criminais e éticos a profissionais que desrespeitarem a privacidade de pacientes ou

qualquer forma de exposição de dados (MARTORELL; NASCIMENTO; GARRAFA, 2016).

Portanto, não há qualquer fundamento que justifique as publicações de pacientes em SRSO por profissionais de saúde ou que [...] relativizem seu dever de respeito à privacidade e confidencialidade com relação aos seus pacientes (MARTORELL; NASCIMENTO; GARRAFA, 2016, p. 21).

4.7 Análise de mecanismos de controle de acesso nas redes sociais, por Santos, Porto e Alturas

Os autores discutem uma série de elementos disponíveis para a proteção a dados e relacionam visões identificadas sobre os SRSO. A primeira visão é que as empresas de SRSO deveriam fornecer aos usuários segurança, pois muitas vezes os usuários desejam apenas compartilhar dados a quem concedeu permissão para acessar a sua rede. A proposta é que as empresas deveriam fazer isso de forma fácil e ao mesmo tempo eficaz (SANTOS; PORTO; ALTURAS, 2010).

O estudo buscou saber se os mecanismos de controle de dados oferecidos aos usuários em SRSO são flexíveis a ponto de proporcionarem a eles facilidade de acesso e controle sobre seus dados. E ao mesmo tempo saber se os mecanismos de controle são ao mesmo tempo suficientemente rígidos a ponto de oferecer garantias de confidencialidade e de privacidade de dados (SANTOS; PORTO; ALTURAS, 2010).

A segunda visão é sobre a proteção de dados em SRSO. Para isso, os autores elencaram aspectos sobre a integridade de dados. O primeiro aspecto é sobre a autentificação individual. Um usuário ao se registrar em uma conta está de certa forma obtendo uma garantia de integridade para alguns dados. O segundo aspecto sobre a proteção de dados mostra que a grande maioria dos SRSO concede apenas ao proprietário da conta uma autorização única para alterar ou excluir dados, o que não é permitido a outros usuários, uma vez que isso é apenas possível ao titular da conta, feito por meio de login e senha pessoal (SANTOS; PORTO; ALTURAS, 2010).

Quando trata-se sobre integridade de origem, refere-se à autenticidade do conteúdo ou dos usuários que o apresentam. “Sobre integridade de origem, em redes de relacionamento populares como o Orkut, é comum a criação de falsos profiles, principalmente de usuários que se fazem passar por empresas ou pessoas famosas, com o intuito de disseminar spam ou vírus” (SANTOS; PORTO; ALTURAS, 2010, p. 55).

A utilização de perfis falsos são usados para o envio de mensagens a outros usuários com a intenção de fazer com que eles abram *hyperlinks* contendo vírus, por exemplo. Nas mensagens o usuário com perfil falso afirma ter uma possível relação com outro usuário, mencionando que o conhece de algum lugar ou descreve fotos de um possível evento em que ambos participaram. A intenção do emissor da mensagem é a de obter confiança do usuário receptor da mensagem (SANTOS; PORTO; ALTURAS, 2010).

A criação de perfis falsos tem por objetivo a captura de informações por meio da chamada engenharia social. Muitos dos perfis falsos criados podem obter informações sigilosas de indivíduos e até mesmo de empresas (SANTOS; PORTO; ALTURAS, 2010).

A confidencialidade é um aspecto dos SRSO que garante que os dados dos usuários fiquem visíveis apenas a quem tenha autorização de acesso (SANTOS; PORTO; ALTURAS, 2010).

Os autores afirmam que para que um SRSO seja confiável e os dados fiquem seguros é preciso existir um nível de controle obtido por meio da autorização dos usuários, que é um dos principais critérios de confiança no controle de acesso a dados. O segundo critério é o nível de relacionamento que um usuário possui com o outro usuário (SANTOS; PORTO; ALTURAS, 2010), registrado no Quadro 12.

Quadro 12 - Confidencialidade de dados em SRSO

Nível de relacionamento de um usuário	
Acesso a dados	**Nível de relacionamento**
Privado (somente para acesso pelo titular da conta)	Todos
	Amigo de amigo
	Amigo

Fonte: Adaptado pela Autora, a partir de Santos, Bezerra e Alturas (2010).

Essa configuração da confidencialidade de dados é considerada pelos autores como fácil e flexível pois possibilita a liberdade de escolha aos usuários. Entretanto ressaltam que apesar desse recurso, os SRSO não fazem distinção entre aquele que é amigo e o que foi aceito e, portanto faz parte de sua rede de relacionamento aquele amigo que não faz parte de sua rede mais íntima (SANTOS; PORTO; ALTURAS, 2010).

A ausência de distinção no nível de confidencialidade impacta na questão do compartilhamento de dados uma vez que existem dados e informações às vezes até sigilosos, que só se quer compartilhar apenas com amigos. Portanto, se um usuário não restringir o nível de acesso a dados apenas para os reais amigos pode acontecer de qualquer indivíduo visualizar e até utilizar os dados que a princípio deveriam ser privados aos amigos de sua rede de relacionamento (SANTOS; PORTO; ALTURAS, 2010).

A ambiguidade de acesso a dados é outro aspecto abordado no estudo. Um indivíduo que é amigo de seu chefe em um determinado SRSO pode, por exemplo, optar em não querer compartilhar dados com ele, mesmo que seja seu amigo. Talvez o usuário prefira manter privacidade dos dados em relação ao seu chefe, mas não em relação a um outro amigo (SANTOS; PORTO; ALTURAS, 2010).

Alguns SRSO tais como o *Orkut* ou *Facebook* possuem uma estrutura diferente em relação ao acesso a dados como por exemplo de um álbum de fotos. No *Orkut* os usuários podiam optar por criar álbuns com várias fotos e em seguida fazer a seleção de amigos com quem queriam compartilhar (SANTOS; PORTO; ALTURAS, 2010).

O *Facebook* oferece também a opção de seleção dos amigos que podem visualizar as fotos. Mas oferece também uma outra opção aos usuários que é a restrição de acesso às fotos a amigos específicos, ou seja, o usuário pode não querer compartilhar as fotos com todos os amigos de sua rede (SANTOS; PORTO; ALTURAS, 2010).

O *Twitter* possui uma única opção de controle quanto o acesso a dados que é "[...] Protect my updates (proteger minhas actualizações) [...]" (SANTOS; PORTO; ALTURAS, 2010, p. 56). Esse tipo de controle permite ao usuário titular da conta conceder acesso para acompanhamento de *post* apenas aos indivíduos indicados pelos usuários, sendo uma boa forma de restrição (SANTOS; PORTO; ALTURAS, 2010).

O *Twitter* é um SRSO popular porque possui uma interface simples. As mensagens postadas por um usuário podem ser vistas apenas por seus seguidores, Entretanto as mensagens podem ser retweetadas com outros usuários (SANTOS; PORTO; ALTURAS, 2010).

O retuíte é uma forma de recompartilhamento de dados que a princípio foram compartilhados com um determinado usuário ou grupo restrito ganhando assim uma amplitude maior de alcance, uma vez que os dados serão vistos e comentados por indivíduos que nem sequer são seus seguidores, perdendo assim o controle sobre os dados e sobre a privacidade (SANTOS; PORTO; ALTURAS, 2010).

A compreensão que Santos, Porto e Alturas têm sobre os SRSO é que o mais importante é disseminar uma grande quantidade de dados o mais rápido possível (SANTOS; PORTO; ALTURAS, 2010).

Quanto ao acesso a dados compartilhados tanto no *Youtube* como no *Flickr* apresentam um mecanismo bem simples de ser compreendido pelos usuários. No *Youtube*, por exemplo, um vídeo pode ser configurado como privado. Neste caso, apenas o usuário

pode visualizá-lo. A segunda opção é a configuração de listados na qual apenas os usuários que receberam o *hyperlink* terão acesso ao vídeo. A terceira opção de acesso a dados no *Youtube* é de tornar o vídeo público cujo todos podem visualizá-lo (SANTOS; PORTO; ALTURAS, 2010).

O Flickr oferece três tipos de formatos de acesso a dados que vai depender da configuração que o usuário irá adotar em seu perfil. Quando um perfil é configurado como público significa dizer que qualquer indivíduo terá acesso aos dados daquele usuário. O segundo tipo é parcialmente restrito. Significa que um usuário pode ter acesso a dados, desde que ele seja aceito em um determinado grupo por meio de convite. O terceiro tipo é ainda mais restrito, uma vez que apenas indivíduos convidados pelo dono do perfil podem visualizar dados como uma foto, o que dá ao usuário uma liberdade maior ainda (SANTOS; PORTO; ALTURAS, 2010).

Há um problema quanto à questão da privacidade de dados relacionada aos tipos de perfis e de acesso a dados. Uma foto postada por um usuário em seu perfil pode ser adicionada a uma galeria de fotos de um grupo do qual ele faça parte. Assim a foto que deveria ser vista apenas por amigos, tendo o caráter de privada passará a ter o caráter de pública, pois todos do grupo poderão visualizá-la (SANTOS; PORTO; ALTURAS, 2010).

Diante de tudo isso, Santos, Porto e Alturas (2010) elencam aspectos sobre o controle de acesso a dados em SRSO:

1. Os usuários têm meios disponíveis para proteção de dados nos próprios ambientes de SRSO;
2. A mesma proteção disponibilizada aos usuários, titulares dos perfis, para tornar seus dados mais privados, estão também disponíveis a outros usuários com interesses obscuros. Portanto é mais difícil identificar usuários que usam os SRSO apenas para acessar dados e aqueles que querem cometer algum tipo de delito como a homofobia, o racismo, uma vez que eles se utilizam do anonimato;
3. A popularização cada vez maior dos SRSO requer que os mecanismos de controle de acesso a dados sejam mais flexíveis e mais fáceis de serem utilizadas pelos usuários, quando o que está em questão é a privacidade de dados e a segurança dos usuários;
4. Existe ainda uma tendência para que se crie automaticamente tipos de permissões, retirando dos usuários a capacidade de configurar os mecanismos de controle

disponíveis, pois entende-se que são complexos e extensos, e portanto isso seria uma atribuição do próprio sistema.

Os mecanismos de controle de acesso a dados são até certo ponto simples, contudo não são suficientemente flexíveis a ponto de atenderem os usuários em suas necessidades de segurança de dados e de privacidade. Além disso, os mecanismos de controle atuais são complexos para que possam ser utilizados de forma adequada pelos usuários (SANTOS; PORTO; ALTURAS, 2010).

4.8 O excesso no discurso de ódio dos haters, por Rebs

O objetivo desta investigação foi o de identificar e também de compreender as marcas deixadas pelo discurso de ódio dos haters possibilitado pelo uso de SRSO como grande força propulsora da "[...] difusão da informação [...]" (REBS, 2017, p. 2512)

Uma das características marcantes dos SRSO é o tipo de linguagem utilizada pelos usuários no momento de interação. Apesar de existirem outros tipos de linguagens utilizadas como as chamadas de vídeo, o que prevalece na comunicação em SRSO é a forma escrita da linguagem. Uma outra característica é a possibilidade de anonimato dos usuários, de uma não presença física (REBS, 2017), de usuários imperceptíveis, escondidos em perfis nem sempre reais.

O que os usuários buscam por meio dos SRSO é o reconhecimento e uma boa reputação. Eles querem ser conhecidos por aquilo que divulgam ou pelo aquilo que pensam. Isso só é possível quando apresentam ao mundo o seu discurso, o que lhes garante um alto grau de visibilidade (REBS, 2017).

Ao mesmo tempo que os SRSO facilitam a interação entre os indivíduos por meio da comunicação explicitam também a "violência simbólica" como o discurso de ódio, que antes não era tão visível assim em ambientes físicos (REBS, 2017).

As características estruturais dos SRSO deixam claro que os indivíduos que propagam discursos de ódio ficam invisíveis pois existem facilidades para que se execute este tipo de ação. A primeira delas é a utilização do anonimato, ou seja, não há um indivíduo físico presente nas interações. A segunda facilidade é a ausência de leis referentes aos SRSO sobre comportamentos considerados agressivos. Na verdade entende-se que a violência, o discurso de ódio fazem parte da sociedade, mas o que os SRSO permitem é uma potencialização dos discursos graças as suas interfaces (REBS, 2017).

O estudo apresenta como exemplo de um discurso de ódio um caso de racismo ocorrido no *Facebook* com a atriz Taís Araújo. Foi observado durante a análise do caso que a propagação do discurso de ódio parece ser um dos objetivos dos *hater* - o odiador ou aquele que odeia. A intenção dos *haters* é provocar um grande choque ou humilhar as vítimas por meio de palavras ofensivas (REBS, 2017).

Apesar de serem criticados por outros usuários de SRSO ainda sim o conteúdo agressivo é possível de ser pesquisado, compartilhado, fotografados ou printados, ficando armazenados na internet, o que se caracteriza como uma ação de persistência do discurso do ódio (REBS, 2017).

Além do excesso de violência que os *haters* impregnam nos SRSO cometidos contra os afrodescentes, por exemplo, eles também tem o propósito de alcançar valores que os próprios SRSO potencializam que são a

> "[...] visibilidade, a popularidade (entre integrantes das redes e a própria mídia), a autoridade e a reputação (ainda que apenas dentro do grupo de pertença do hater), afinal, eles reconhecem os comentários e os apoiam por meio das "curtidas" ou mesmo "respostas" que funcionam como reforço aos seus ideais" (REBS, 2017, p. 2521).

4.9 Instagram como interface da comunicação móvel e ubíqua, por Streck e Pellanda

O *Instagram* foi analisado na investigação para exemplificar um meio de comunicação utilizado pelos usuários para tipicamente postar imagens. As postagens de imagens realizadas por meio da plataforma acontecem quase que instantaneamente (STRECK; PELLANDA, 2017).

A publicação de dados como fotos e vídeos é uma forma de interação ou de memorização de algum lugar que se tenha visitado. Um dos riscos quanto a publicação deste tipo de dados é que eles podem ficar armazenados em um SRSO permanentemente ou até que o usuário faça a sua exclusão ou ainda que o definam como privados (STRECK; PELLANDA, 2017).

No *Instagram* as imagens publicadas são "rememorizadas". Isso significa que os usuários podem revê-las quando quiserem em sua página pessoal (STRECK; PELLANDA, 2017). Este é um recurso utilizado pelo *Facebook* ou pelo *Instagram* para fazer com que os usuários publiquem cada vez mais imagens, uma vez que a rememorização pode mexer com os sentimentos dos usuários.

Outro ponto relevante relacionado às TIC e de sua evolução foi citado na investigação de Streck e Pellanda (2017). O acesso aos *smartphones* tornam a vida dos indivíduos mais fácil. Antes ao saírem para um passeio os indivíduos levavam suas

câmeras fotográficas pesadas e caras e mais um celular. Agora as câmeras já vêm acopladas aos *smartphones* (STRECK; PELLANDA, 2017), o que em tese é mais acessível para uma boa parte da sociedade e torna a publicação de fotos muito mais rápida.

O *Instagram* é uma plataforma cujo prefixo Insta está diretamente relacionada à captação de informações em tempo real pelo usuário" (STRECK; PELLANDA, 2017, p. 13), é o tempo presente, o agora, significando que os dados disponibilizados pelos usuários são feitos no exato momento em que cada postagem acontece (STRECK; PELLANDA, 2017).

O *Instagram* é um SRSO que serve para capturar fatos do cotidiano bem como para armazenar e compartilhar "[...] memórias e interações sociais" (STRECK; PELLANDA, 2017, p. 13).

O *Instagram* oferece aos usuários recursos para marcação de locais, registrando de onde as fotos foram capturadas ou a marcação de amigos que podem visualizar as imagens e vídeos, além das curtidas (STRECK; PELLANDA, 2017).

Outras funcionalidades do *Instagram* são disponibilizadas aos usuários para a criação de histórias em fotos ou em vídeos desde 2016. Os recursos incluem a inserção de *emojis*, de textos ou de criação de desenhos à mão livre ou com auxílio de ferramentas gráficas existentes na plataforma (STRECK; PELLANDA, 2017).

Dados como os comentários podem ser produzidos a partir das funcionalidades e da criação de histórias que segundo Pellanda retratam "micromomentos" de fatos do cotidiano do usuário. As histórias produzidas por um usuário ficam expostas por um período de 24 horas revelando portanto o momento atual vivido a seguidores (STRECK; PELLANDA, 2017).

Um outro fator relevante considerado característico dos SRSO é a quantidade de fotos que podem ser publicadas. Não existe limite para a quantidade de fotos que um mesmo usuário pode publicar (STRECK; PELLANDA, 2017), o que aumenta a capacidade de coleta de informações sobre um mesmo indivíduo e de amigos com quem ele interage.

Outro aspecto que os autores chamam a atenção em relação aos SRSO é para o uso de recursos de alteração de imagens ou do uso de filtros. O usuário ao aplicar um filtro em uma imagem pode tirá-la do contexto real em que foi captada, levando a uma mudança de detalhes que podem confundir o usuário que esteja visualizando a imagem ou o cenário que foi modificado (STRECK; PELLANDA, 2017).

4.10 (In)visibilidade algorítmica no "Feed de Notícias" do Facebook, por Jurno e D'Andréa

Os autores discutem em seu estudo questões relacionadas às publicações visiveis e invisiveis geridas no Facebook no Feed de Notícias tendo como foco saber se as publicações são de origem humana ou não humana (JURNO; D'ANDRÉA, 2017).

O *Facebook* assim como outros SRSO funcionam por meio da produção de conteúdos de dados provenientes de várias naturezas como as que convergem pelo Feed de Notícias (FN). O FN acontece de maneira personalizada para cada usuário (JURNO; D'ANDRÉA, 2017).

A personalização segundo Jurno e D'Andréa é "[...] dinâmica e heterogênea [...]". É dinâmica porque muda de forma frequente como acontece por exemplo em um status de relacionamento de um indivíduo que hoje pode estar solteiro e amanhã pode estar em um relacionamento sério. É heterogênea porque é composta por uma variedade de dados tais como posts, o próprio status de relacionamento, selfies ou fotos com familiares, parentes ou amigos de trabalho, vídeos e outros dados do tipo textual (JURNO; D'ANDRÉA, 2017, p. 464).

A organização da personalização do FN é feita pelos algoritmos. São eles que realizam o agenciamento dos posts, ou seja, são os responsáveis por selecionar aquilo que os usuários podem ou não ver em seu FN (JURNO; D'ANDRÉA, 2017).

É notório que os usuários deixam rastros ao utilizarem os ambientes de SRSO como o *Facebook*. Isso ocorre quando, por exemplo, os usuários curtem um post. Esta ação dos usuários desencadeiam várias outras ações que se ramificam e influenciam na formação de outros FN (JURNO; D'ANDRÉA, 2017).

O estudo avaliou 34 *posts* publicados no *Facebook* a fim de verificar como acontece o processo de personalização a partir do FN, principalmente aqueles identificados no "[...] NewsFeed FYI em um site Newsroon [...]" (JURNO; D'ANDRÉA, 2017, p. 463).

O FN é um conjunto formado por variados tipos de dados pertencentes a um usuário [...] que conformam textos e sentidos a partir das nossas próprias experiências" (JURNO; D'ANDRÉA; 2017, p. 466).

O FN de um usuário se forma primeiramente por meio de um registro e do acesso a um SRSO, e sem registro não há como um usuário ter um FN próprio. Outro fator importante sobre o FN é que ele nunca se repete, ele está sempre em constante transformação (JURNO; D'ANDRÉA, 2017).

O agenciamento feito no *Facebook* ocorre com a realização de ações que são movimentadas pelos usuários. Primeiro o usuário cria um perfil. Em seguida é necessário que ele realize atualizações em sua conta pessoal e por fim forme uma lista de amigos. As curtidas, os compartilhamentos e os comentários fazem parte dos dados que podem ser agenciados pelo *Facebook* (JURNO; D'ANDRÉA, 2017).

Outro tipo de agenciamento é a partir de dados de empresas e/ou de instituições. Os representantes desses segmentos também compartilham dados, assim como os usuários comuns e até interagem com os usuários. A diferença neste tipo de agenciamento empresarial é que as empresas pagam para o *Facebook* para que fiquem visíveis no FN dos usuários (JURNO; D'ANDRÉA, 2017).

As *hashtags* são formas de agenciamento que recuperam na verdade "[...] redes textuais temáticas [...]". Além disso, os usuários podem melhorar seus FNs incluindo novos amigos e incluindo páginas às suas listas de seguidos (JURNO; D'ANDRÉA, 2017, p. 466).

Outro tipo de agenciamento identificado em SRSO é o de marcação direta de perfis de um usuário ou de uma página em uma postagem. Ao ser marcado em uma postagem o usuário titular do perfil é informado sobre isso (JURNO; D'ANDRÉA, 2017).

Todas essas articulações e formas de agenciamento são desenvolvidas pelos algoritmos e que têm como base os banco de dados. No banco de dados ficam armazenados todo tipo de dados coletados por meio de publicações selecionadas a partir dos acessos feitos aos SRSO por meio do perfil dos usuários (JURNO; D'ANDRÉA, 2017), o que é fundamental para a sobrevivência do *Facebook.*

A seleção de um conjunto de dados é realizada pelos algoritmos por meio de rotinas de programação. Essas rotinas incluem a identificação de assuntos considerados relevantes, extraídos dos rastros digitais, ou de opções ou de preferências sinalizadas pelos usuários quando utilizam um SRSO (JURNO; D'ANDRÉA, 2017).

Os dados reunidos pelo *Facebook* por meio da ação dos algoritmos são processados e transformados em informações. As informações são compartilhadas com outras empresas que as utilizam conforme seus objetivos sejam comerciais ou apenas para fins de divulgação de serviços (JURNO, D'ANDRÉA, 2017).

> Assim, todas essas informações geradas nos nossos acessos são computadas junto com as de milhares de outros usuários e usadas para criar "perfis de público", prever comportamentos e, assim, vender espaços de publicidade personalizada, relatórios de marketing para

> empresas interessadas ou sistemas de vigilância, dentre outros. Sob essa perspectiva, o rastreamento das ações na internet constitui supostamente uma via privilegiada de acesso aos desejos e a alguns traços de personalidade dos usuários (JURNO, D'ANDRÉA, 2017, p. 468).

Além de realizarem a coleta de dados, os algoritmos são responsáveis também em fazer com que uma publicação paga de uma empresa apareça no FN do perfil de um usuário (JURNO; D'ANDRÉA, 2017).

Os algoritmos atuam também no engajamento de publicações. Para que as publicações tenham um grande alcance é necessário que sejam curtidas, comentadas e compartilhadas por um grande número de usuários (JURNO; D'ANDRÉA, 2017).

A quantidade de interações de um usuário é também levada em consideração pelos algoritmos. Isso significa dizer que quanto mais publicações de um usuário são exibidas, mais ele se torna prioritário e mais frequentemente suas publicações aparecerão no FN de outros usuários com quem ele interage (JURNO; D'ANDRÉA, 2017).

O uso de códigos para a execução de agenciamento é também uma atividade executada pelos algoritmos. Quando um usuário "segue" ou deixa de "seguir" um outro está na verdade permitindo ou não que sua publicação possa ser exibida (JURNO; D'ANDRÉA, 2017).

A visibilidade de dados é algo relevante no contexto de SRSO e para a ação dos algoritmos. Ao utilizar um SRSO o usuário tem a opção de configurar suas publicações como privadas ou públicas, conforme o Quadro 13.

Quadro 13 - Opções de configurações para acesso às publicações.

Ordem	**Tipo**	**Permissão de acesso às publicações**
1	Públicas	O usuário permite que todos os usuários daquele SRSO possam visualizar suas publicações.
2	Todos os amigos	Todos os selecionados como amigos podem ver as publicações.
3	Amigos dos amigos	Amigos em comum de seus amigos podem visualizar as publicações.
4	Somente amigos	Não inclui conhecidos.
5	Listas personalizadas	São listas elaboradas pelos usuários contendo os nomes de familiares ou de amigos. Somente os que constam na listagem podem ter acesso às suas publicações.

Fonte: Adaptado pela Autora, a partir de Jurno e D'Andréa (2017).

Os usuários podem definir as configurações de acesso às suas publicações. O próximo passo é dado pelos algoritmos que escolhem, por exemplo, qual a ordem ou quais as publicações do usuário serão exibidas para seus amigos (JURNO; D'ANDRÉA, 2017).

Uma série de ações são executadas pelos algoritmos e impactam no direito de escolha dos usuários. Se por um lado eles podem configurar suas permissões de acesso às suas publicações, por outro lado eles não têm direito de escolha sobre quais publicações gostariam de exibir em seu FN. Para Jurno e D'Andréa (2017, p. 469), o "[...] Facebook nos passa a impressão de que são apenas os próprios usuários que escolhem os posts que serão exibidos no FN, ou que os posts selecionados seriam simplesmente os que mais importam para esses usuários".

As mais recentes atualizações de publicações de um usuário com registro no *Facebook* são feitas de forma contínua e cronológica segundo Jurno e D'Andréa (2017). No *Facebook* é possível que um usuário consiga visualizar todas as ações realizadas por seus amigos. É possível saber por exemplo quem curtiu a sua publicação, ou quem fez algum comentário sobre uma foto, ou mesmo quem teve acesso a sua publicação. Esse mesmo usuário pode ser notificado pelo *Facebook* quando há novas interações em sua publicação ou quando há novas publicações ou de um perfil ou de uma página (JURNO; D'ANDRÉA, 2017).

As publicações são organizadas conforme sua relevância. Não há uma ordem cronológica e sim temporal de como e quando as publicações podem ser exibidas. Os algoritmos fazem a seleção e ditam a circulação das publicações nos FN (JURNO; D'ANDRÉA, 2017).

Em 2013, o *Facebook* fez o anúncio de que publicaria informações para os usuários de como os algoritmos funcionam. A partir dessas informações, tanto os usuários como as empresas puderam adquirir "[...] espaços de marketing e publicidade no ambiente" (JURNO; D'ANDRÉA; 2017, p. 472).

Informações com alterações sobre o *modus operandi* dos algoritmos foram lançadas pelo *Facebook* em agosto de 2016, sendo publicados 34 textos pertencentes a categoria NewsFeed FY referentes ao FN (JURNO; D'ANDRÉA, 2017).

A identificação de variáveis do *Facebook* claramente influencia na formação do FN. Dentre os elementos que formam o aparato técnico necessário para o *Facebook* estão uma conexão mais rápida da internet ou os tipo de conteúdos que foram publicados, sendo os vídeos os de maior preferência, ou mesmo "[...] quando o conteúdo foi publicado e como o usuário interagiu com os posts" (JURNO; D'ANDRÉA; 2017, p. 474).

Alguns aspectos sobre o FN referentes a ação dos algoritmos e a privacidade de dados foram identificados nesta pesquisa. Existe uma real pressão sobre o *Facebook* e uma

preocupação dos usuários e da imprensa em especial sobre o que acontece no FN e sobre o papel dos algoritmos ou de sua influência em ambientes de SRSO (JURNO; D'ANDRÉA, 2017).

A análise realizada a partir do Newsroom referente a categoria NewsFeed FYI foi considerada por Jurno e D'Andréa como o acesso a caixa preta do *Facebook*, por meio do qual foram identificados um conjunto de algoritmos que exercem o agenciamento no *Facebook* (JURNO; D'ANDRÉA, 2017).

O *Facebook* pode ainda camuflar algumas publicações pois podem conter conteúdos considerados inadequados, uma vez que não se encaixam nas condições descritas nos Termos de Uso da plataforma (JURNO; D'ANDRÉA, 2017).

Os algoritmos parecem conduzir os trajetos dos usuários em SRSO, assim como coletam, manipulam e processam dados. Para Jurno e D'Andréa (2017), os algoritmos gerenciam a sociedade, as organizações, geram rendimentos e regulam espaços.

4.11 Diretrizes para aperfeiçoamento e interpretação da Lei do Marco Civil da internet com vistas à garantia do direito à privacidade nas redes sociais, por Lima

Ao mesmo tempo em que os SRSO promovem uma melhoria no processo de comunicação e de interação, são também associados a uma crescente preocupação com a violação de privacidade. Para controlar ações de violação de privacidade na internet foram criados mecanismos jurídicos, tais como o Marco Civil da Internet (LIMA, 2018). O objetivo deste estudo foi verificar se o referido instrumento jurídico pode não ser utilizado no contexto de problemas relacionados à privacidade em SRSO. Assim, foi baseado em premissas que abordam desde o contexto de SRSO e sua relação com as TIC, até o direito à privacidade e de suas garantias (LIMA, 2018).

As TIC impulsionam novas formas de comunicação, que de certa maneira provocaram efeitos tanto positivos quanto negativos aos indivíduos (LIMA, 2018). Para Lima (2018), os efeitos negativos no uso dessas novas formas de comunicação incluem o vazamento de dados, o compartilhamento, além da exposição de dados e da renúncia da privacidade, seja feita de forma consciente ou não consciente.

Acrescenta que os avanços provenientes de tecnologias como as relacionadas com a comunicação produzem um efeito na vida dos indivíduos e em suas ações, tendo como foco a busca pela "hiperinformação" e de sua inclusão em meios online (LIMA, 2018).

A busca pela informação, a convergência, a virtualização do mundo e o indivíduo conectado ditam o ritmo da sociedade digital e nesse contexto surgem os SRSO na Internet (LIMA, 2018).

O cenário mais recente dos SRSO indica uma nova versão sendo utilizada que é a versão 3.0. Diferentemente das versões anteriores, esta versão mais recente tem como foco a interação entre os indivíduos, a produção de dados, e o seu uso de forma multimodal, facilitada pela disponibilização de internet via *wireless* e da utilização de dispositivos móveis (LIMA, 2018).

Sobre os SRSO, Lima afirma que os usuários têm um papel crucial nos problemas relacionados à privacidade. Primeiro porque os usuários dão condições de serem vigiados. A realização de um registro, por si só, já produz dados, uma vez que são solicitados para a realização do acesso. Segundo, o ato de expor publicações produz outros conjuntos de dados e esta ação realizada soma-se às iniciais como se fosse um círculo vicioso sem fim, e quanto mais publicam, mais se expõe e mais vulnerável deixam a sua privacidade (LIMA, 2018). Lima traduz bem isso quando afirma que "[...] é preciso ser visto para existir." Se um usuário não publica não existe, embora tenha um registro (LIMA, 2018, p. 64).

Outro problema relativo à privacidade é o de não conseguir de forma segura atribuir o seu verdadeiro conceito e valor, justificado por ser um tema muito amplo. Na perspectiva do ordenamento jurídico brasileiro a privacidade é considerada como um direito de personalidade e reconhecido como um direito fundamental, previsto na Constituição de 1988 (LIMA, 2018).

O direito à privacidade passa a ser tratado no contexto do Marco Civil da Internet, o qual dialoga com questões de privacidade no cenário virtual do qual fazem parte os SRSO. Lima considera os SRSO como *Facebook* como provedores uma vez que possibilitam a realização de ações por meio de um terminal conectado à internet (LIMA, 2018).

Na medida do possível, jurisprudências como o Marco Civil da Internet têm conseguido contemplar questões relativas à violação da privacidade em SRSO, embora sua aplicação de forma isolada não consiga garantir que todos os direitos sobre a privacidade sejam atendidos, pois segundo Lima os SRSO acontecem em um contexto virtual e complexo (LIMA, 2018).

Em síntese, Lima afirma que o Marco Civil da Internet é um mecanismo jurídico que pode ser aplicado em casos de violação de privacidade ocorridos em SRSO. Mas é

preciso ter ciência de que os ambientes virtuais são complexos, e que portanto necessitam de ações conjuntas e efetivas para o combate às violações de privacidade.

4.12 A questão do direito à privacidade no Facebook: um estudo à luz da ética da informação, por Fugazza e Saldanha

O direito à privacidade foi investigado sob o foco da ética da informação e por meio de estudo de caso sobre os SRSO, especificamente do *Facebook*, evidenciando problemas relativos à democracia dentro do contexto da liberdade e privacidade, objetivo deste estudo. Para isso foi considerado [...] a cultura digital de transparência em uma época de "supercompartilhamento" de dados pessoais nas plataformas da Internet" (FUGAZZA; SALDANHA, 2018, p. 463).

A ética informacional é um instrumento moral. Portanto, sempre que os indivíduos forem agir ou tomar algum tipo de decisão devem antecipadamente refletir e se basear em parâmetros e princípios considerados éticos (FUGAZZA; SALDANHA, 2018).

A ética informacional e a reflexão que é feita sobre as ações e decisões dos indivíduos na contemporaneidade originam-se por meio da evolução e do uso intenso das TIC e de forma mais preocupante dos produtos e serviços que a internet oferece (FUGAZZA; SALDANHA, 2018), assim como os SRSO.

A respeito da privacidade, Fugazza e Saldanha argumentam que é um tema bastante valorizado nas culturas ocidentais uma vez que está atrelada a princípios democráticos da autonomia e da liberdade (FUGAZZA; SALDANHA, 2018).

Mencionam ainda que o problema da privacidade é tão urgente quanto a questão da ampliação do acesso à internet e citam casos de violação ocorridos no Brasil como foi o da atriz Carolina Dieckmann que resultou na criação da Lei "Carolina Dieckmann", Nº 12.737/2012. Os autores ressaltam que a privacidade não tem a mesma atenção que foi dada ao direito de acesso livre à informação, não sendo portanto uma prioridade nas discussões (FUGAZZA; SALDANHA, 2018).

Questiona-se no estudo se pode ser atribuído aos usuários e as suas experiências os princípios da autonomia e liberdade quando estão conectados em ambientes digitais, já que a privacidade dos usuários não é importante para as empresas. As empresas estão preocupadas com o desenvolvimento e com o uso de estratégias de marketing e com a lucratividade, em que o que pesa é a transparência dos dados e não a privacidade (FUGAZZA; SALDANHA, 2018).

A publicação de dados e a velocidade com que são compartilhados por meio das conexões são por si só fatores preocupantes, mas isso não seria apenas uma prática de empresas. Usuários que tenham o hábito de investigar dados considerados privados estariam de alguma forma exercendo atividades de vigilância em SRSO (FUGAZZA; SALDANHA, 2018).

Baseado nessa premissa de vigilância em SRSO também por usuários é que Fugazza e Saldanha realizaram uma investigação com discentes de cursos de graduação e de pós-graduação de áreas do conhecimento ofertados pela UNIRIO para saber a visão deles sobre a transparência e a privacidade em SRSO, sintetizadas no Quadro 14 (FUGAZZA; SALDANHA, 2018).

Quadro 14 - Resultado do estudo de caso sobre *Facebook* a partir da premissa de vigilância, transparência e privacidade.

Perguntas feitas aos discentes baseadas nas variáveis elaboradas	**Resultado em %**	**Declaração de Direitos e Responsabilidades - DDR, do Facebook**
1 Você assinaria um contrato em 2016 autorizando a concessão de suas imagens e vídeos pessoais para uma empresa privada internacional?	60% do total dos discentes talvez forneceriam seus dados se tivessem retorno financeiro, 33% não forneceriam e 6,7% forneceriam gratuitamente.	Sobre a concessão de dados, o artigo 2.1 da, DDR do Facebook deixa claro que a Meta Platforms, Inc., proprietária do Facebook tem livre e amplo acesso a um conjunto de dados (incluindo os dados pessoais) dos usuários, sendo possível a partir da criação de conta na plataforma.
2 Você seria capaz de ceder seus dados pessoais, imagens e vídeos para amigos?	60% do total dos discentes disseram que cederiam gratuitamente dados tais como imagens e vídeos a amigos. Enquanto 40% não cederiam seus dados.	Não é somente as empresas que têm acesso livre e gratuito a dados de um usuário. Outros usuários que integram a sua rede de relacionamento ou que fazem parte de seus contatos têm acesso a dados. Fica claro na DDR que os dados de um usuário podem ser acessados também por qualquer outro usuário, com conta no Facebook. Isso pode ocorrer caso não sejam alteradas as configurações de perfil para privados.
3 Você produziria conteúdo intelectual textual para uma empresa internacional de forma gratuita?	76,7% do total dos discentes disseram que talvez produzissem de forma gratuita. 23,3% disseram que não produziriam conteúdo intelectual. E nenhum dos	O artigo 2.5 da DDR esclarece que o Facebook pode utilizar a produção intelectual, ou seja, as sugestões e comentários dos usuários sem que tenham que remunerá-los por isso. Deixa claro ainda que os usuários não

Perguntas feitas aos discentes baseadas nas variáveis elaboradas	**Resultado em %**	**Declaração de Direitos e Responsabilidades - DDR, do Facebook**
	discentes assinalou a opção "SIM".	são obrigados a produzir sugestões ou comentários. Entretanto, a empresa não deixa claro o que faz ou de que maneira utiliza essa produção intelectual.
4 Você tem o direito de usar espaço publicitário do Facebook para fazer propaganda de sua empresa familiar pelo fato de ter cedido suas imagens a empresa de SRSO?	76,7% dos discentes disseram que sim, acham que têm direito, mas 23,3% disseram que não têm direito.	O artigo 3.1 da DDR do Facebook, diz que é estritamente proibido a publicação de quaisquer comunicações comerciais não autorizadas pelo SRSO.
5 Alguém da empresa onde você trabalha está ameaçando você e usando seus dados de forma indevida. você seria capaz de tentar identificar dados desse indivíduo, como forma de se proteger?	43,3% dos discentes disseram que não iriam identificar os dados daquele que o estava ameaçando. Mas 6,7% disseram que iriam buscar meios legais para obter dados desse usuário.	O artigo 3.2 da DDR do Facebook deixa claro que não há permissão para que usuários coletem dados de quaisquer outros usuários. Assim como não é permitido também acessar o perfil de qualquer usuário por meios automatizados tais como bots de coleta, robôs etc., sem que antes a empresa seja comunicada.
6 Os discentes tiveram que responder se baseando em algum motivo foram levados a consultar dados: endereço, imagens, áudios, vídeos de um indivíduo por meio por exemplo da rede mundial de computadores (Internet)?	83,3% do total disseram que já acessaram, através da rede mundial de computadores, dados particulares de outros usuários da Internet. 16,7% do total, afirmaram nunca fizeram isso.	Não há no termo de uso do Facebook artigos que se refiram a esta variável.
7 Baseado em objetivos e interesses específicos você criaria mais de um perfil de usuário, por exemplo, para o trabalho, para a família, para o entretenimento?".	60% dos respondentes disseram que Não criariam mais de um perfil. E 40% disseram que Sim.	O artigo 4.2 da DDR do Facebook diz que é proibido a criação de mais de um perfil pessoal na plataforma, sem que haja uma autorização prévia. Entretanto, o dilema ético da universalidade em contraste com as contingências de um plano intercultural ético pode levar um usuário a criar um ou mais perfis para fins, por exemplo, de

Perguntas feitas aos discentes baseadas nas variáveis elaboradas	**Resultado em %**	**Declaração de Direitos e Responsabilidades - DDR, do Facebook**
		denúncia contra a violação de direitos humanos, é a priori destituído por uma universalidade do ethos normativo da empresa.
8 Você seria capaz de omitir uma informação pessoal para conseguir fazer parte de uma empresa privada?".	46,7% disseram que "NÃO" omitiriam qualquer informação pessoal, Mas 8, 53,3% responderam que "SIM" omitiriam alguma informação.	Segundo o artigo 4.1 da DDR, é proibido ao usuário fornecer informações falsas no Facebook.

Fonte: Adaptado pela Autora, a partir de Fugazza e Saldanha (2018).

Toda e qualquer produção intelectual dos usuários tais como fotos e vídeos pessoais, textos particulares publicados no Facebook que deveriam pertencer a eles na verdade pertencem à *Meta Platforms, Inc*.[16]. Isto está descrito nos Termos de Uso do *Facebook*. Outro aspecto levantado pelos autores é de que a publicação de dados não gera remuneração aos usuários, e sim lucro para as empresas envolvidas diretamente ou indiretamente no processo. Na opinião dos autores tudo isso é uma forma de opressão (FUGAZZA; SALDANHA, 2018).

Outra forma de arrecadação de lucro pelas empresas parceiras de SRSO é por meio do marketing. O primeiro passo é personalizar os perfis dos usuários, o que é realizado pelos algoritmos. Depois que os perfis são personalizados eles são utilizados como base para o desenvolvimento de estratégias de marketing. O objetivo das empresas é o de impulsionar as vendas de produtos e serviços por meio de anúncios. Os anúncios são realizados enquanto o usuário acessa sua página e os conteúdos publicados (FUGAZZA; SALDANHA, 2018).

Isso indica que os indivíduos integram a sociedade de controle ou vivem numa fase "[...] pós-panopticom [...]" (FUGAZZA; SALDANHA, 2018, p. 485). Os usuários são cuidadosamente vigiados. Seus dados são rastreados, coletados e são direcionados para finalidades pré-definidas. Esse poder de controle e de vigilância não estaria mais restrito apenas às empresas, mas estaria entre os próprios usuários que são fontes de vigilância (FUGAZZA; SALDANHA, 2018).

[16] A Meta Platforms, Inc, é o novo nome dado à empresa proprietária pelo Facebook. O nome da empresa foi alterado em 2021. O criador do *Facebook* é o empresário Mark Zuckerberg.

A vigilância permite que as empresas possam coletar metadados dos perfis de milhões de usuários cadastrados em um SRSO. Isto seria uma rotina para as empresas, uma vez que elas registram e documentam tudo aquilo o que seus usuários fazem, como se comportam e as suas preferências, sendo portanto considerada como uma nova forma de vigilância. Essa mesma liberdade de acesso a dados que é dada a empresas é dada também a outros usuários, pois podem julgar opiniões, investigar dados e utilizar dados também de forma indevida (FUGAZZA; SALDANHA, 2018).

Tudo isso contribuiria para a perda de privacidade. Ter privacidade na cultura ocidental significa dizer que um indivíduo possa ter autonomia sobre as suas escolhas, incluindo o direito de escolha sobre os dados que podem ou não ser publicados em um SRSO, por exemplo (FUGAZZA; SALDANHA, 2018).

É muito difícil entender quais são os limites entre o "[...] direito à privacidade no ambiente digital em coexistência à privacidade no ambiente físico" (FUGAZZA; SALDANHA, 2018, p. 484).

Sobre isso se discute que os ambientes on-line são um reflexo mais elaborado daquilo que é vivido nos ambientes físicos. Isso na percepção dos autores facilitaria a ocorrência de crimes digitais tais como a invasão de privacidade ou o "hackeamento" de dados, e que seriam mais eficazes do que os próprios crimes ocorridos em ambientes físicos. Além disso, a criação de multiperfis pelos usuários e o fato de alguns omitirem informações pessoais pode ser associada à falsidade ideológica (FUGAZZA; SALDANHA, 2018, p. 487).

Tais informações colocam os usuários em uma situação de alto risco. Primeiro porque os dados publicados pelos usuários ficam disponíveis para acesso público e de forma não autorizada. Depois, mesmo que um usuário configure suas publicações para acesso privado, as empresas têm acesso porque foi concedido o direito a elas no momento do aceite do usuário às condições das empresas, o que torna isso uma decisão sem volta. As empresas trazem em seus Termos de Uso e Condições informações limitadas aos usuários (FUGAZZA; SALDANHA, 2018), portanto tais documentos não são uma fonte segura aos usuários em relação à privacidade, coleta e uso de dados.

Para Fugazza e Saldanha (2018, p. 488),

> A utilização indiscriminada dos dados pessoais dos usuários não é claramente comunicada aos mesmos por parte das empresas digitais, exceto por meio dos termos de uso do site. Estes, além das políticas de privacidade e de cookies, são os documentos legais para justificar os usos dos dados pessoais dos usuários para as mais diversas finalidades.

Nas plataformas de SRSO existem uma quantidade e diversidade de perfis que representam os indivíduos. Por meio das conexões desses perfis ocorrem as interações sociais que são repletas de opiniões e verdades divergentes, levando a uma socialização narcisista, uma vez que cada um tende a defender seus interesses (FUGAZZA; SALDANHA, 2018).

Violar a privacidade do outro impacta diretamente na violação também de sua identidade. Para os autores, essa violação pode estar associada à cultura de transparência de dados, justificada como sendo um ato de cidadania. A absorção dessa cultura pelos usuários desestimula discussões mais profundas sobre a privacidade (FUGAZZA; SALDANHA, 2018).

4.13 Mercado, vigilância e Facebook na era do espetacular integrado, ou *inside us all there is a code*, por Borges

O estudo propôs analisar fenômenos culturais e sua relação com a internet. Para isso os autores elencaram o *Facebook como fonte de investigação.* Acrescentaram a investigação outros elementos tais como os algoritmos e o big data, além das contribuições do espetacular integrado do autor Guy Debord (1988), o que não será enfatizado nesta RSL (BORGES, 2020).

O uso da tecnologia algorítmica por empresas de SRSO é algo comum, mas que exige técnicas relevantes que são o uso da vigilância sobre os dados dos usuários e o direcionamento de marketing (BORGES, 2020).

Os algoritmos representam a inteligência artificial e são desenvolvidos com objetivo de aprenderem a linguagem de máquinas bem complexas. Sua função é a de coletar e detalhar "[...] uma massa de dados [...]" a fim de identificar padrões a partir de estatística, que posteriormente são transformados em um modelo [...]" (BORGES, 2020, p. 147).

O governo dos Estados Unidos justificou a coleta de dados de cidadãos estadunidenses como forma de proteger o país de novos ataques terroristas como o que aconteceu com as Torres do Gêmeas no dia 11 de setembro de 2001. Este episódio marcou uma nova fase para a privacidade de dados. Assim, o governo passou a reunir dados de seus cidadãos para elaborar dossiês. Os dados eram coletados de diversas fontes tais como saúde pública, justiça ou de pagamento de impostos. O fato é que isso gerou um número elevado de dados nunca antes acessíveis e abriu um precedente para que empresas privadas

como o *Facebook* pudessem fazer o mesmo, só que agora de forma descontrolada (BORGES, 2020).

Afirma-se que as ações dos algoritmos no *Facebook* são obscuras. Tal afirmação se baseia na ideia de que não se sabe como eles organizam o ranking de conteúdo. Além disso, a empresa proprietária do *Facebook* parece dar preferência para publicações patrocinadas em vez das gratuitas. Mas a "[...] a gratuidade do uso se paga com nossa ignorância com relação aos modelos e com nossos próprios dados" (BORGES, 2020, p. 151).

Para os algoritmos os usuários são um aglomerado de códigos sem estrutura alguma. O que os algoritmos fazem é coletar, decifrar, organizar e transformar essa "massa de dados" em algo lucrativo para as empresas. Diante disso, compara-se um usuário a uma mercadoria geradora de dados (BORGES, 2020).

As interações realizadas em SRSO desencadeiam uma sequência de ações e de prováveis consequências aos usuários. Quanto mais os usuários interagem no *Facebook, mais* dados são gerados. E quanto mais visíveis se tornam para os algoritmos melhor como por exemplo no "[...] feed de notícias dos amigos [...]" (BORGES, 2020, p. 155).

Quanto mais visíveis os usuários se tornam, mais empolgante será para ele utilizar um SRSO, aumentando assim o tempo de permanência e a quantidade de dados gerados (BORGES, 2020).

Não existe um limite de dados coletados, mas existem padrões de dados sujeitos a coleta e as imagens são um exemplo disso. Para a coleta de dados são utilizadas as tecnologias de reconhecimento facial, capazes de obter lucros elevados às empresas como o *Facebook*. Elas funcionam como potentes scanners que realizam em pouco tempo a captura de uma grande quantidade de fotos tanto de usuários como de amigos (BORGES, 2020).

Para evidenciar o *modus operandi* e a Política de Privacidade sobre o Facebook, Borges apresenta aspectos importantes de seu funcionamento, incluindo informações sobre o marketing e também o da vigilância. Borges considera que a Política de Privacidade é muito ofensiva e traz preocupações e uma delas fere os "[...] direitos humanos básicos" (BORGES, 2020, p. 157).

O primeiro aspecto apresentado por Borges é o uso de dados pelo *Facebook*. Eles são a mercadoria mais valiosa e são comercializados com terceiros, ou seja com outras

empresas, representantes de produtos ou de serviços, como os da publicidade. Os dados são negociados e dessa transação resultam lucros exorbitantes (BORGES, 2020).

Para aumentar ainda mais seus lucros, o *Facebook* desde 2012 vem realizando parcerias com empresas tais como a data brokers. Essa empresa tem como função coletar dados tanto *on-line* como *off-line* para comercializá-los com empresas como a *Meta Platforms, Inc.* - *Facebook* (BORGES, 2020).

O segundo aspecto são os Termos de Uso do *Facebook* referente a uma de suas cláusulas que é a modificação unilateral. O grande impasse sobre essa cláusula é que quando os usuários se registram no *Facebook* estes estão automaticamente concordando com a cláusula. Tal concordância faz com que o *Facebook* altere quando quiser qualquer coisa sem que os usuários fiquem cientes das alterações realizadas. O resultado de tudo isso é que o *Facebook* quebra qualquer acordo feito anteriormente. Deste modo a empresa pode esconder ou mesmo omitir informações de como ocorre a manipulação dos dados dos usuários. Um dos exemplos mencionados pelo autor é sobre o não compartilhamento de dados com empresas de publicidade. Compromisso que pode ser contestado diante do aumento no lucro da empresa obtido por meio de parcerias estabelecidas com empresa de marketing digital (BORGES, 2020).

Portanto, o Facebook torna preocupações reais com a privacidade como algo que pode ser resolvido de maneira simples, ou como Borges afirma de forma enganosa. A empresa faz o usuário acreditar que para blindar a privacidade de seus dados basta compartilhá-los apenas com amigos mais próximos, mas isso não impede que seus amigos compartilhem dados com outros (BORGES, 2020).

O terceiro aspecto é sobre o alto poder de vigilância que o Facebook possui sobre seus usuários. São capazes, por exemplo, de saber a localização de um usuário apenas pela conexão que ele realiza por meio de seu *smartphone*, ou que lugares frequenta (BORGES, 2020). O *Facebook* não só realiza vigilância sobre dados do usuário, mas de todos os outros que com que ele mantenha algum tipo de relacionamento ou de “associação de likes" (BORGES, 2020, p. 160) aumentando a sua capacidade de vigilância e de coleta de dados.

Outro aspecto mencionado por Borges é a formação do banco de dados do *Facebook*. Ele é formado por dados identificáveis nos perfis dos usuários tais como idade ou gênero e ainda o status de relacionamento (BORGES, 2020), tudo isso informado de forma espontânea pelos usuários. Somam-se a esses dados gostos ou interesses dos

usuários assim como a "[...] marca e o modelo de seus carros [...]. (BORGES, 2020, p. 160).

Além da formação de banco de dados, o *Facebook* possui um software linguístico que capta "[...] um inventário de palavras-chave e expressões tidas como positivas ou negativas [...]" (BORGES, 2020, p. 162). Por meio do inventário é possível analisar comentários dos usuários sobre notícias publicadas. Com isso, o *Facebook* pretende saber até que ponto os usuários podem ser contagiados emocionalmente. Este tipo de experiência realizada pelo *Facebook* é feita sem o conhecimento dos usuários (BORGES, 2020).

Os algoritmos tornam a linha do tempo dos usuários um lugar tranquilo, visibilizando apenas postagens de amigos e isso causa uma sensação de bem-estar e de pertencimento. Tal efeito de alguma forma indica o nível de "[...] contágio entre os pares, criando imensas 'bolhas' de convivência [...]" com algum ou nenhum diálogo (BORGES, 2020, p. 164).

Para Borges, o *Facebook* se tornou muito mais do que um simples ambiente *on-line* de socialização e se transformou numa potência de coleta de dados. Primeiro porque é fácil de ser manuseado por seus usuários. Segundo, porque a plataforma oferece muitos atrativos aos usuários fazendo com que eles produzam dados espontaneamente, contribuindo assim de forma decisiva para a transformação de dados em lucros (BORGES, 2020).

O *Facebook* tem investido cada vez mais em tecnologias auxiliares para otimizar a coleta de dados. Por outro lado, há pouca transparência sobre suas ações ou sobre o uso de tecnologias como os algoritmos, o que implica em ausência de resistência dos usuários em relação ao uso de dados de forma comercial. Além disso, a questão da privacidade fica comprometida em meio a tudo isso.

Sobre isso Borges (2020, p. 172) afirma que

> [...] a erosão dos princípios democráticos e sua substituição por um totalitarismo estatal-econômico que submete a gestão orgânica da vida pública ao funcionamento fantasmagórico dos modelos algorítmicos elaborados com fins de maximização dos lucros —quase uma "ditadura da propaganda" stricto sensu, sendo a alma de toda propaganda sua qualidade deformadora e caricata discussão pública e o convencimento dão lugar a um regime do monopólio da visibilidade, em que ganha não quem aparece mais ou melhor, mas quem tenta ser o único visível, eliminando a concorrência. Em segundo lugar, nota-se a subtração do direito de privacidade de um lado e, de outro, o segredo como uma das mais poderosas armas do marketing, político ou não.

4.14 O espetáculo cultural na rede social: a abordagem midiática do coletivo dirigível de teatro no Facebook, por Amaral Filho e Blanco

Investigou-se o *Facebook* enquanto meio de apropriação e de uso para a divulgação de espetáculos culturais. Para isso buscou-se entender como se dá a relação entre os espetáculos culturais e SRSO. A relação do público em ambientes *on-line* indica a existência de uma dicotomia entre o público e o privado, sendo considerado como uma "[...] quebra de paradigma" (AMARAL FILHO; BLANCO, 2014, p. 32).

Para entender esta relação é preciso saber mais sobre os SRSO. A primeira consideração a se fazer é que para que os acessos às plataformas sejam representativos é necessário um grande número de acessos. Ao mesmo tempo tem-se os mais diversos tipos de públicos formados, como por exemplo pela personalização de consumo. A ambientação específica e diversa é um outro fator dessa quebra de paradigma (AMARAL FILHO; BLANCO, 2014)

Pela perspectiva do acesso, os SRSO servem aos usuários como um segmento de colaboração, mas ao mesmo tempo podem interferir coletivamente ou individualmente em assuntos debatidos nessas plataformas (AMARAL FILHO; BLANCO, 2014).

Quanto um usuário está logado em um SRSO tem a falsa sensação de que se está no controle quando na verdade não está. O que ocorre é que quando um usuário publica dados, como por exemplo imagens, isso se torna algo viral, sem controle algum (AMARAL FILHO; BLANCO, 2014). Dados percorrem todas as conexões possíveis e existentes. Algo que se imagina estar somente visível a grupos restritos de amigos pode circular em todos os continentes do mundo (AMARAL FILHO; BLANCO, 2014).

O movimento presente em SRSO de querer ver e ser visto envolvem ações tais como participar de grupos ou de criar fanpages ou mesmo de se engajar em causas; criar e compartilhar imagens e vídeos, ou somente curtir postagens (AMARAL FILHO; BLANCO, 2014).

Sobre essa produção de conteúdo Amaral Filho e Blanco tem duas concepções: a primeira remete a uma natureza de mercado, em que a publicação da mercadoria (dados) se traduz de forma direta na cultura do consumo. A segunda remete à questão da privacidade. A publicação de dados em um SRSO dá a condição a um usuário de ficar visível de maneira permanentemente, mesmo que ele não deseje ser visto. Essa complexa condição é comparada a um "[...] fetiche do escondido, do proibido, do insurreto, mas que está sendo visto por todos" (AMARAL FILHO; BLANCO, 2014, p. 32).

O *Facebook* é uma plataforma de SRSO que proporciona aos seus usuários opções de interação social. Dentre as opções disponíveis estão a formação de grupos, o uso de serviços das próprias plataformas ou de outras linkadas a ela. Nos serviços os usuários podem acessar fotos ou vídeos, entrar em salas de bate-papo, enviar mensagens, curtir postagens de seu interesse ou conectar seguidores (AMARAL FILHO; BLANCO, 2014).

O *Facebook* é considerado por Amaral Filho e Blanco como uma grande vitrine. É uma plataforma acessada por milhões de usuários em todo o mundo. As conexões são estabelecidas de forma direta ou indireta. Um usuário que não foi conectado a outros de maneira direta pode ser conectado de forma indireta a muitos outros, o que torna essa vitrine ainda maior (AMARAL FILHO; BLANCO, 2014). No Quadro 15 há exemplos de como as conexões indiretas são estabelecidas.

Quadro 15 - Formação de conexões no Facebook.

#	**Como se formam as conexões**		
Usuários A, B e C.	Usuários “A” e "B" possuem uma relação de amizade.	Mas “B” e “C” também tem uma relação de amizade.	Os usuários “A” e “C” não se conhecem. E mesmo assim podem se conectar por meio da relação de amizade em comum que “B” tem com “A” e “C”.

Fonte: Adaptado pela Autora, a partir de Amaral Filho e Blanco (2014).

Portanto pode existir novas conexões a partir de interações indiretas. Segundo Amaral Filho e Blanco (2014) as interações em SRSO estão configuradas em níveis, como no exemplo do Quadro 16.

Quadro 16 - Configuração de interação em um SRSO baseado em níveis.

Níveis de interações		**Consequências**
Um usuário “A” comenta na postagem do mural do usuário “B”	O usuário “C” que não tem relação de amizade com “A”, mas tem com “B” pode comentar, curtir e mesmo compartilhar o comentário do usuário “A”	O fato do usuário “C” comentar ou compartilhar o comentário de “A”, vai aumentar o número de conexões do usuário “A”.

Fonte: Adaptado pela Autora, a partir de Amaral Filho e Blanco (2014).

Sobre o compartilhamento de dados em SRSO, os autores observam que funciona de maneira análoga ao compartilhamento em ambientes físicos. Um usuário compartilha dados com outro usuário, que por sua vez compartilha com outro e a tantos outros, como se fosse uma corrente de compartilhamentos, até que se possa ter uma quebra (AMARAL FILHO; BLANCO, 2014).

4.15 De rainha dos baixinhos à rainha dos memes: o humor como vetor de ciberacontecimentos a partir da ida de Xuxa da rede globo para a rede record, por Gonzatti, Bittencourt e Esmitiz

O artigo contextualiza o aspecto social da interação de Xuxa Meneghel nos SRSO, o que entendemos como um vetor determinante para a construção do ciberacontecimento.

Os dispositivos tecnológicos assim como o desenvolvimento da cibercultura atuam para facilitar a vivência dos indivíduos. O ciberespaço é comparado a um palco de interações em que se pretende atingir a um público. É assim que surgem "[...] novas práticas sociais e identitárias [...]" (GONZATTI; BITTENCOURT; ESMITIZ, 2015, p. 83).

Ciberespaços como os SRSO são fontes de entretenimento, mas que precisam ser validados. Assim como por meio do compartilhamento de dados e de momentos alegres dos usuários, perpetuados nas plataformas de SRSO. Celebridades também fazem parte do ciberespaço e são passíveis de problemas com a privacidade e com a autoexposição, seja no *Facebook* ou no *Instagram* (GONZATTI; BITTENCOURT; ESMITIZ, 2015).

As celebridades talvez sejam os tipos de usuários mais ativos dos SRSO e devido ao uso frequente podem estar mais suscetíveis à quebra de privacidade, uma vez que elas mantêm uma relação mais profunda com seus fãs, muito em função da característica ubíqua desta tecnologia da TIC (GONZATTI; BITTENCOURT; ESMITIZ, 2015).

A relação que as celebridades mantêm com seus fãs ou seguidores gera uma possível identificação ou não de dados colocando em risco a sua privacidade, mas essa relação que as celebridades mantêm com seus fãs não coloca apenas em risco a sua privacidade, mas as dos próprios seguidores que interagem com ela cotidianamente (GONZATTI; BITTENCOURT; ESMITIZ, 2015)

As celebridades não apenas fazem parte dessa rede de relacionamento e de interação como são agentes potencialmente mobilizadores dentro delas, fazendo com que conteúdos e publicações viralizem em questão de minutos, indicando uma característica que "[...] é o nível de diversão das conexões que emergem de um acontecimento" (GONZATTI; BITTENCOURT; ESMITIZ, 2015, p. 83).

4.16 Extimidade virtual e conjugalidade:possíveis repercussões por Mendes-Campos, Féres-Carneiro e Magalhães

O texto é baseado na perspectiva de entender como foi construída a extimidade virtual que significa na verdade observar o que acontece na intimidade da internet. Isso tem uma relação muito próxima com a privacidade do ponto de vista histórico. Mas o que a investigação propôs foi a de saber como esse fenômeno repercute na vida de casais que são

usuários ativos de SRSO (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

A industrialização e sua posterior modernização causaram um impacto direto na sociedade ocidental. Um desses impactos foi a mudança de compreensão sobre os conceitos de público e de privado. Essa mudança provocou ainda um impacto na relação mais íntima das famílias e dos casais (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Antes da fase industrial a intimidade estava protegida por paredes. Com a chegada dos SRSO no século XXI houve uma mudança em relação à proteção da intimidade e consequentemente da privacidade (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Um aspecto mencionado pelos autores é de que a privacidade e a intimidade se relacionam, principalmente quando se trata da publicação de dados, ou seja de tornar público dados antes considerados de interesse íntimo e privado (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

A quantidade de dados disponíveis em SRSO são bem elevados e com isso surgem as preocupações em torno deles. Os comentários feitos em uma publicação podem conduzir a uma má interpretação ou podem se configurar em comentários suspeitos. As fotos publicadas podem exibir algum flagrante inesperado. Tudo isso torna a tela de um smartphone e a plataforma de SRSO como perfeitos instrumentos para acesso a dados (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Os indivíduos trazem consigo uma necessidade de serem notados. Na contemporaneidade isso ganha ainda mais força com os dispositivos móveis que colocam a disposição dos usuários meios de tornar isso possível. A busca dos usuários por algum tipo de reconhecimento, seja por meio das opiniões que emitem ou em outros tipos de publicações faz com que o ego dos usuários fique fortalecido (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Um exemplo do reconhecimento mencionado são as curtidas realizadas em postagens no *Facebook*. Os tipos de postagens ou publicações tais como vídeos ou fotos geram expectativa de reconhecimento que pode ser representado em SRSO pelas curtidas de outros usuários (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Um outro aspecto interessante do estudo foi o de saber como os indivíduos tratam a questão da intimidade e o que fazem para preservar a sua privacidade. Um dos

investigados relatou, por exemplo, que simplesmente desligava o celular quando estava na companhia de seu marido (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Casais que participaram do estudo revelaram ter problemas com o *Facebook*. Um deles é sobre a existência de conteúdos suspeitos. O outro problema indicado pelos participantes foram as paqueras realizadas por meio dos chats, que acontecem preferencialmente de madrugada. Uma das participantes disse se proteger desse tipo de ataque e justificou, dizendo que textos podem ser retirados do contexto original (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Outros participantes relataram ter algum tipo de problema com outros usuários por meio de discussões no *Facebook*. Foram desentendimentos com alguém próximo, amigos ou parentes. Um dos episódios de desentendimento entre amigos causou a exclusão de um deles da rede de relacionamento mantida até então. Normalmente os desentendimentos são provocados pela divergência de opiniões. E antes quem eram amigos se tornam rivais e passam a trocar ofensas chegando até ao fim da relação de amizade, o que os autores chamam de retaliação (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

Os autores chegaram à conclusão a partir das falas dos participantes do estudo que a extimidade virtual ou seja a capacidade de expor a intimidade é uma tendência cada vez mais normal e forte na vida dos indivíduos (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020), colocando a privacidade em segundo plano de prioridade.

> Se a presença do virtual em nossas vidas parece se desenhar como um caminho sem volta, precisamos aprender a construir as fronteiras entre os espaços de intimidade e de extimidade que parecem se interpenetrar (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020, p. 278).

A concepção ou conceito de privacidade pode estar relacionado às experiências geracionais. Isso poderia explicar porque a privacidade tem significados e importância diferentes para certos grupos de usuários. Essa diferença de concepção pode estar relacionada às experiências vividas pelos usuários. Questiona-se por exemplo se grupos de usuários que vivenciaram uma experiência antes e depois da internet tem uma concepção de privacidade diferente daqueles que só possuem a experiência pós-internet e SRSO. Os autores deixam em aberto que futuros estudos devem ser realizados para se contrastar essas

observações a respeito da privacidade e do uso de SRSO, internet (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020).

4.17 Estilos de uso e significados dos autorretratos no *Instagram*: identidades narrativas de adultos jovens brasileiros, por Zakiee, Hage e Kublikowski

Indivíduos que nasceram pós-internet ou em momentos de importantes avanços tecnológicos acabam tendo uma experiência de vida e até profissional no meio virtual bem diferente dos demais que nasceram em uma época pré-internet. Os ambientes virtuais como os SRSO são acessíveis e fortemente lugar de exposição e por isso são confundidos como palcos onde o cotidiano dos usuários é o grande espetáculo da vida íntima (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

As experiências vivenciadas em plataformas de SRSO podem ter um cenário diferente para esses indivíduos em relação, por exemplo, ao que é público ou privado, ou sobre a percepção de tempo ou de espaço. Mas são de fato locais de exposição do cotidiano, em que o usuário precisa ter o cuidado de se moldar e de moldar seus dados idealizando um indivíduo perfeito. “O belo é mostrado e seguido simultaneamente, evidenciando ser o Instagram uma rede social que preza a beleza e por ser mais reservada, é onde o sujeito se sente mais à vontade para se expor, contanto que não fuja ao padrão estético apregoado (ZAKIEE; HAGE; KUBLIKOWSKI, 2019, p. 534)

As reconfigurações de imagens em um SRSO como o Instagram realizadas pelos usuários indica que é “[...] possível definir e confirmar identidades idealizadas, refletidas pelos olhos da mídia e dos outros [...]” (ZAKIEE; HAGE; KUBLIKOWSKI, 2019, p. 524).

Publicar aspectos apenas positivos do cotidiano pelos usuários em uma plataforma de SRSO é mais importante que publicar fatos negativos e por isso acabam sendo descartados. Este tipo de publicação estaria fora do contexto de interesses dos SRSO afinal o que importa é a vida ideal (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

O Instagram foi eleito pelos usuários como um SRSO diferente dos demais. Isso porque foi considerado pelos usuários participantes da investigação como uma plataforma em que os usuários se sentem mais seguros para publicar dados, como images e momentos do seu dia a dia. Acham que tem controle de quem o está seguindo e a quem os dados serão direcionados (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

Essa segurança é atribuída pelo fato dos indivíduos acreditarem que seus dados possam ser visualizados e utilizados apenas por outros usuários que tenham vínculo mais forte com ele, assim não precisam se preocupar com questões como o da privacidade.

Além disso, enfatizam que tem liberdade para se se expor, o que favorece a composição de um diário on-line (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

Há uma inversão em relação à privacidade. Antes os diários físicos, fonte de registro de toda a intimidade e segredos de um indivíduo eram mantidos sob total privacidade, longe de olhar de curiosos e até dos mais íntimos. Em outro cenário, um diário-online pode ser acessado sem a menor preocupação com a privacidade uma vez que se entende que apenas os usuários autorizados terão acesso a ele (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

De maneira sucinta os respondentes do estudo consideraram o *Instagram* como um SRSO seguro para a exposição de dados e para a privacidade dos usuários (ZAKIEE; HAGE; KUBLIKOWSKI, 2019), pois:

1. É uma plataforma cuja há a publicação majoritária de imagens e vídeos;
2. Somente usuários com vínculos mais próximo do usuário publicador (amigos, familiares e namorados (as) terão acesso a dados ou ao "diário-on-line" (conjunto de dados de um usuário armazenados em um SRSO);
3. Sensação de liberdade de expor dados;
4. E ainda se tem o controle de quem pode seguir quem; isso depende de um aceite do usuário para seguir e ser seguido;
5. O Instagram tem a opção de deixar um perfil do usuário como privado

Também foram feitas comparações entre o Facebook e o Instagram e chegou-se aos seguintes resultados sobre ambos os SRSO. No Facebook, há uma variedade maior de estabelecimento de relações sociais, algumas próximas com familiares e amigos de trabalho, ou outras mais distantes como amigo de amigos e outros que nem sequer se conhecem. No Instagram, essas relações sociais tendem a ser mais próximas e acontecem de forma mais controlada e restrita (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

Sobre a privacidade, o estudo identificou que em

> [...] relação aos significados atribuídos às postagens, encontramos a noção de privacidade, com a possibilidade de gerenciar com mais facilidade o conteúdo publicado e a quem ele se destinará, tornando o aplicativo mais intimista e reservado (ZAKIEE; HAGE; KUBLIKOWSKI, 2019, p. 535).

4.18 Investigando o fenômeno de compras coletivas on-line: fatores que influenciam a intensidade das compras, por Everton, *et al*

Os SRSO reúnem usuários que interagem e que compartilham dos mesmos objetivos. Por outro lado, eles causam insegurança aos usuários em relação à atividade de

consumo de produtos e de serviços disponibilizados em suas plataformas, muito em função da exposição de dados pessoais ou financeiros (EVERTON, *et al.,* 2014, p. 201).

Essa insegurança dos usuários se fundamenta na premissa de que eles tomam decisões sobre as compras on-line baseados em emoções. Para Everton et al, os usuários deveriam ter um tempo maior para reflexões de suas ações, como buscar por exemplo a maior quantidade possível de informações sobre os produtos e serviços de seu interesse. Isso resultaria numa tomada de decisão mais racional (EVERTON, *et al.,* 2014)

Nesse aspecto os usuários podem estar mais suscetíveis a divulgar dados sobre si de forma inconsciente. Portanto, o estudo trouxe a discussão sobre como os usuários se comportam em relação às compras coletivas.

Os SRSO influenciam nas decisões dos usuários quanto aos interesses e intensidade com que realizam compras. Ressalta que o ponto chave deste processo é a dinâmica de troca de informação, uma vez que os produtos e serviços podem ser vistos por vários usuários ao mesmo tempo (EVERTON *et al.,* 2014).

Por outro lado existe uma preocupação dos usuários com os riscos relacionados ao comércio que é realizado por meio dos SRSO. Um dos riscos apontados são os vírus utilizados para captar dados sigilosos dos usuários. Tal receio evidencia o fato de que dados podem ser coletados e utilizados de maneira indevida por outros usuários. “Desse modo, para os fins deste estudo, o construto segurança pode ser entendido pelo usuário como uma percepção acerca de confiança e risco” (EVERTON, *et al.,* 2014, p. 204)

Empresas de SRSO podem identificar e selecionar usuários que estejam mais suscetíveis a realizar compras. Para isso utilizam os dados disponibilizados pelo próprio usuário são usados para saber quais são seus interesses e gostos (EVERTON, *et al.,* 2014)

A confiança que um usuário tem sobre um SRSO o qual utiliza tem peso em relação a decisões no momento de uma transação de compra on-line. Se um SRSO não oferece aos seus usuários mecanismos de segurança automaticamente eles não se sentem estimulados a fazer qualquer tipo de negócio (EVERTON, *et al.,* 2014).

Diante de tudo isso, os usuários tendem a não realizar compras em SRSO caso percebam que isso pode trazer algum tipo de risco ou dano a seus dados. Segundo Everton *et al*. (2014, p. 209), isso demonstra que “[...] o valor percebido da oferta tende a ser menor que um determinado valor percebido da segurança [...]”.

4.19 Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais, por Assumpção, Santana e Santos

O objetivo do estudo foi verificar de que maneira é abordada a questão da coleta de dados, especificamente de imagens no Facebook e no Instagram (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

O fator acesso à internet impulsionado pelo uso de dispositivos móveis garante a utilização de SRSO de forma intensa pelos usuários. Eles são os responsáveis pela massa de conteúdo de dados criados nessas plataformas e ao mesmo tempo são os maiores utilizadores de dados publicados por outros usuários. Além disso, eles interagem nessas plataformas, quando curtem um post ou quando baixam uma imagem ou vídeo de seu interesse. (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

Antes havia uma predominância de conteúdo textual nos SRSO. Hoje eles oferecem recursos para o compartilhamento também de imagens e de vídeos de forma praticamente ilimitada aos seus usuários. Com isso, as redes sociais, como o Facebook, estão cada vez mais permeadas por imagens, facilmente capturadas por dispositivos de baixo custo (ASSUMPÇÃO; SANTANA; SANTOS, 2015, p. 32).

Entende-se assim que a produção de imagens em larga escala seja um reflexo do aumento do número de dispositivos móveis e que ficaram mais acessíveis aos usuários. Esses dispositivos estão cada vez mais sofisticados e são atualmente desenvolvidos com câmeras mais bem elaboradas (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

Sabendo da importância das imagens, os autores se propuseram a fazer as seguintes perguntas: “O que acontece com as imagens submetidas pelos usuários nas redes sociais?”, “São coletados dados dessas imagens? Quais dados?”, “Como as redes sociais lidam com as imagens em seus termos de privacidade?” (ASSUMPÇÃO; SANTANA; SANTOS, 2015, p. 32).

O resultado da interação entre os usuários de SRSO é a produção de dados correlacionados tais como imagens, textos ou vídeos. Nessa correlação há dados secundários gerados a partir de uma imagem como por exemplo a data ou o local onde foi tirada, ou ainda dados gerados a partir de endereços de IPs ou de dispositivos móveis que os usuários utilizam para acessar um SRSO (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

As plataformas são ambientes públicos e que, portanto, podem interferir na privacidade dos usuários (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

As empresas de TICs facilitam o acesso dos usuários aos SRSO. Um usuário pode baixar as plataformas em seu *smartphone* ou pode usar uma conexão sem fio. As empresas que gerenciam os SRSO incentivam os usuários a publicarem dados e fazem os mesmos se sentirem à vontade para fazerem isso, uma vez que disponibilizam em suas plataformas configurações de privacidade para que eles se sintam seguros e pensem ser os donos de seus dados (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

A preocupação com a privacidade de dados permeia todas as fases do uso de dados pelas empresas de SRSO, incluindo desde o acesso até a recuperação e a coleta, sendo esta última de forma mais acentuada. Os autores afirmam que os usuários estão mais sujeitos a riscos em relação à privacidade, pois a partir do momento em que seus dados são coletados não existem mecanismos que impeçam que eles não sejam utilizados. Portanto a coleta é considerada uma fase de alto risco para a privacidade, uma vez que consideram que os usuários perdem o domínio sobre seus dados. Diante disso, é primordial levantar discussões acerca da privacidade, incluindo o compartilhamento de imagens (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

Os autores entendem que a Política de Uso do *Facebook* não deixa claro quais dados são coletados ou como fazem esse processo. Afirma-se ainda que a forma como os usuários utilizam os SRSO não é o único fator a contribuir para questões relacionadas à privacidade e explicam que mesmo que um usuário mantenha seu perfil privado e compartilhe dados apenas com amigos próximos, estes podem compartilhar os dados privados com outros usuários, perdendo portanto a configuração inicial de privado para público. Assim percebe-se que o compartilhamento de dados mesmo que entre amigos próximos é um risco para a privacidade (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

A coleta de dados de imagens no *Facebook* é feita por exemplo "[...] através de um sistema de reconhecimento facial, que consiste na análise de uma imagem na tentativa de encontrar características que levem à identificação de uma pessoa". Essa é uma forma de tentar extrair dados a partir de uma imagem, sendo portanto considerada uma técnica de coleta de dados (ASSUMPÇÃO; SANTANA; SANTOS, 2015, p. 40).

As permissões de coleta de dados concedidas pelos usuários às empresas como o *Facebook* dão a elas condições de fazer associações a partir do uso de dispositivos móveis com os quais eles acessam um SRSO, o que gera muitas formas de coleta de dados, especialmente de imagens (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

A identificação de metadados ou de dados de origem técnica está relacionada a conteúdos de dados publicados pelos usuários no *Facebook*. A Política de Uso do *Facebook* indica que os metadados são dados que acompanham as "[...] imagens digitais, tais como os metadados do padrão" EXIF (ASSUMPÇÃO; SANTANA; SANTOS, 2015, p. 42). Outro trecho da Política de Uso descreve que os metadados podem também estar relacionados a conteúdos adicionados pelos usuários no *Facebook* como por exemplo as *hashtags* (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

A persistência de conteúdo de dados e de metadados que são acrescentados ao conteúdo que ficam armazenados no sistema interno dos SRSO é um meio utilizado pelas empresas para recuperar imagens dos usuários (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

Não existe configuração de privacidade disponível no *Facebook* para prevenir o gerenciamento de coleta referente ao reconhecimento facial. A única opção para o usuário é definir as imagens que podem ficar livres de marcações. Isto não garante que os dados a partir de reconhecimento facial sejam preventivamente protegidos em ações de coleta de dados por empresas (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

No *Instagram* e no *Facebook* o usuário tem a opção de informar ou não a localização de uma imagem que ele deseje publicar ou compartilhar com outros usuários. Entretanto, não existem opções de privacidade para os metadados que se encontram nos arquivos digitais, em ambos os SRSO. Apesar da dificuldade apresentada em relação às configurações de privacidade, existem opções, embora não suficientes para a segurança e proteção de dados dos usuários (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

> Um exemplo desse empoderamento é que, juntos, Facebook e Instagram, podem constituir um dos maiores bancos de dados de imagens do mundo, principalmente por terem dados como "quem", "quando", "onde" e "o que" agregados a essas imagens – dados esses coletados por meio de reconhecimento facial, dos metadados, dos dados de localização e das tags. Com isso, assegurar que os usuários tenham, ao menos, um mínimo controle sobre a coleta de seus dados pessoais faz-se uma tarefa de considerável importância (ASSUMPÇÃO; SANTANA; SANTOS, 2015, p. 44).

Neste estudo defende-se que questões sobre a privacidade devem ser discutidas na fase de coleta de dados. As empresas de SRSO disponibilizam aos usuários apenas opções para configurar dados para o modo privado. No entanto, não impede a coleta de dados e sua utilização. Assim, na visão dos autores, o usuário deveria ter mais liberdade de escolha

sobre a coleta de dados (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

A política de privacidade tanto do *Instagram,* de 2013 quanto do *Facebook*, de 2015 mostraram-se muito limitadas em relação à coleta de dados de imagens, especificamente. As empresas não deixam claro em suas respectivas políticas quais dados podem ser coletados. Quando se compara as políticas do *Facebook* ao do *Instagram* se percebe que o Facebook tem mais informações sobre a coleta de dados de imagens do que o próprio Instagram, que um SRSO utilizado mais para o compartilhamento de imagens (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

4.20 As formas de manifestação da privacidade nos três espíritos do capitalismo: da intimidade burguesa ao exibicionismo de si nas redes sociais, por Thibes

O que caracteriza e fundamenta o primeiro espírito do capitalismo, segundo Thibes, é a "[...] oposição entre trabalho e família [...]" (THIBES, 2017, p. 331). Estar em um lar com a família significava estar em um lugar adequado para o descanso, onde as forças do trabalhador podiam ser recuperadas e a intimidade estava garantida. Proporcionando assim, uma sensação de proteção. No segundo espírito do capitalismo percebeu-se de forma clara uma maior influência de "forças econômicas" na condição da vida privada. Mas enfatiza que embora o trabalhador tenha uma preferência e dê mais importância pela vida em família do que pelo trabalho, tal esfera passou a ter um peso maior sobre a sua intimidade muito pelo que representam as mercadorias que foram adquiridas para melhorar a sua vida e de seus familiares (THIBES, 2017).

Portanto, na primeira esfera do capitalismo havia uma preocupação em separar trabalho (esfera econômica) e de "forças externas" da intimidade da vida familiar (esfera privada). Enquanto que na segunda esfera há um certa perda sobre a tranquilidade da vida familiar em decorrência de uma presença mais gradual e atuante da esfera econômica sobre o lar e consequentemente na vida em família (THIBES, 2017).

Neste contexto, a esfera privada seria uma rica fonte para o desenvolvimento da "sociedade de consumo", já que a separação mantida na primeira esfera entre trabalho e vida privada não gerava benefícios ao capital (THIBES, 2017).

No entendimento de Thibes, o trabalho traria novos significados e não seria visto apenas como uma forma de sobrevivência para as famílias. Era necessário ser acrescido a ele "[...] o gosto pelo risco, pela aventura, a ambição e a devoção ao trabalho" (THIBES, 2017, p. 331).

Estudos sobre as relações humanas no contexto industrial foram iniciados a fim de descobrir formas de conseguir integrar a "[...] vida privada ao trabalho [...]" (THIBES, 2017, p. 332). Enquanto isso, as políticas de distribuição do Estado e a forças alcançadas pelos sindicatos exigiam das corporações empresariais respostas frente às resistências impostas pelo trabalho, o que seria quebrado somente com a "[...] retórica das emoções [...]" (THIBES, 2017, p. 332), utilizando-se de um vocabulário mais tranquilo que fizesse fluir a comunicação, aliado ao uso "[...] da empatia e da cooperação [...]" (THIBES, 2017, p. 332). Além de quebrar a resistência ao trabalho em detrimento da vida familiar, o uso de tais recursos seriam capazes também de colocar o trabalhador mergulhado aos processos relacionados ao trabalho (THIBES, 2017).

Este engajamento foi fundamental para que ocorresse uma proximidade entre a "[...] vida privada e a economia [...]" (THIBES, 2017, p. 333), o que pode ser explicado na terceira esfera do capitalismo.

Primeiro, que as residências passaram a ficar cada vez mais isoladas de acontecimentos que ocorriam nas ruas, mantendo os indivíduos mais protegidos e alheios a isso. O recuo que até hoje é utilizado nas residências fez com que houvesse uma separação do ambiente privado (as casas) do ambiente público (a rua). Essa medida de proteção garantia que indivíduos que passassem em frente a residência não tivessem conhecimento do que ocorria ali (THIBES, 2017).

Esta separação de certa forma trouxe mais liberdade e privacidade aos indivíduos, deixando-os longe da "[...] vigilância alheias [...]" (THIBES, 2017, p. 333). Se por um lado os indivíduos se sentiam mais protegidos de olhares alheios, por outro lado, esse distanciamento deixou os indivíduos cada vez mais longe dos centros de sociabilidade tais como praças, mercados, bares localizados no bairro. Tal mudança aconteceu de forma gradativa com residentes dos grandes centros urbanos (THIBES, 2017).

No ambiente de trabalho, o cenário era outro. A existência de prédios em uma cidade colocava os habitantes numa condição de isolamento, o que tornava mais difícil o estabelecimento de relacionamentos entre eles. Isso contribuiu para que as relações em ambientes de trabalho se tornassem mais pessoais. A dificuldade em estabelecer relações pessoais entre os habitantes de um bairro ou cidade, é amenizada quando se começa a se constituir dentro de ambientes organizacionais considerados rígidos (THIBES, 2017).

A partir deste ponto da discussão, passa-se a compreender como a privacidade que foi experimentada tanto na primeira como na segunda esfera do capitalismo fica cada vez mais distante e "[...] sem lugar no capitalismo conexionista" (THIBES, 2017, p. 334).

As habilidades individuais para se lançar em um "mundo conexionista" são constituídas pelo modo como os indivíduos se relacionam com outros indivíduos, ou pela autonomia, pela capacidade de empreender e de ter iniciativa, além da flexibilidade para desenvolver vários projetos, ser comunicativo, aguentar as pressões, ter condições psicológicas e principalmente "[...] sociabilidade (para fazer contatos) [...]" (THIBES, 2017, p. 335). Tais qualidades e ou habilidades além de serem utilizadas para medir valores servem também para produzir uma linguagem que ultrapassam os muros das corporações e que definitivamente se instalou em outras esferas (THIBES, 2017).

No pilar moral da terceira esfera do capitalismo encontra-se a propriedade que sofreu uma "[...] transformação significativa [...]" (THIBES, 2017, p. 336). Na segunda esfera do capitalismo, a propriedade não tinha nenhuma relação com o poder, condição perdida na terceira esfera graças à possibilidade de locação ou mesmo de disponibilidade, mesmo que condicionada por um um período (THIBES, 2017, p. 335).

Mesmo a informação, colocada como um recurso fundamental dentro deste contexto, pode ser locada, emprestada e até recombinada "[...] conforme as necessidades ad hoc que os projetos criam" (THIBES, 2017, p. 336).

Isso leva a entender como um indivíduo antes tido como dono de si, deixa de o ser. Isso significa que a sua vida particular ou privada passa a ser "[...] apropriada pelo mundo do trabalho e pelo mercado como um todo" (THIBES, 2017, p. 337). Este fator é apontado por Thibes como um ponto central para entender como a vida privada tornou-se algo que poderia ser negociado (THIBES, 2017).

"O empreendedor de si mesmo sabe que o sucesso e a posse das características valorizadas pelo mundo em rede não são um dado genético" (THIBES, 2017, p. 337).

Segundo Thibes é necessário moldar as características individuais (internas) e transformá-las em recursos que promovam uma melhor imagem de si. Uma boa imagem pode atrair boas redes e conexões gerando um maior reconhecimento. Mas na balança isso não tem um peso tão grande. É preciso ter muito claro que deve haver também uma relação entre as novas TIC e o "capitalismo conexionista" (THIBES, 2017).

Neste sentido, os SRSO são plataformas ideais para a exibição de características corretas ou de indicações de sucesso. São excelentes vitrines pois ampliam as conexões e também o reconhecimento individual por outros pares (THIBES, 2017).

Para que tudo esteja completo é necessário que o último passo seja dado, e isso não é possível sem a "[...] publicização dos feitos [...]" de um indivíduo (THIBES, 2017, p. 338). Por outro lado, ter condições para se tornar bem-sucedido irá depender apenas do exercício de exibir de [...] símbolos de sucesso da cidade por projetos e seria o caminho para aumentar a rede de contatos e amigos, um dos maiores sinais de aprovação que o indivíduo pode ter" (THIBES, 2017, p. 338).

O que se conclui de tudo isso afirma Thibes (2017) é que:

I. a exibição de si e da vida privada em SRSO se tornou um fenômeno "ubíquo", mesmo que isso vá de encontro ao "princípio de resguardo" que é a parte mais importante e essencial para a compreensão da privacidade;

II. ficar visível nas plataformas de SRSO e se autogerenciar nelas pode até certo ponto gerar benefícios. Mas ficar distante desses ambientes também pode trazer benefícios principalmente os sociais.

A exibição da vida privada em SRSO pode ser sintetizada em dois caminhos: o primeiro é do uso consciente e responsável pelos usuários. Quando um indivíduo segue os passos de revelar as qualidades que o "mundo conexionista" espera, isso pode trazer excelentes benefícios, tais como econômico e o social, como o ganho de mais amigos e do estabelecimento de conexões. O outro caminho é que o uso dos SRSO pelos usuários se traduz em dados utilizados por empresas de TIC como insumos para os seus negócios (THIBES, 2017, p. 340).

A privacidade na primeira esfera do capitalismo estava vinculada à ideia da propriedade ou moradia como local de proteção contra as possíveis intromissões que a esfera pública pudesse causar. Essa ideia foi associada à privacidade no sentindo de proteger e preservar tanto o indivíduo quanto a sua família. Mas esta ideia foi caindo em desuso. E atualmente passou a ser associada a tentativas de proteger as qualidades individuais ou o patrimônio de um indivíduo (THIBES, 2017).

Acontece que na contemporaneidade, esse patrimônio passou a ser explorado com mais intensidade, uma vez que a ele foi atribuído valor e portanto é utilizado para gerar capital. Assim já não tem sentido mantê-lo resguardado. Ter privacidade sobre este patrimônio significa para as empresas de TIC enfrentar um grande obstáculo já que

impacta diretamente em seu lucro financeiro. Para os indivíduos seria uma obstáculo social, pois perdem a capacidade de serem reconhecidos pelos seus pares (THIBES, 2017). Para Thibes

> Assim, conforme os valores e as justificações que animam o capitalismo conexionista se estabelecem, nota-se a progressiva transformação dos contornos da esfera privada. Se, para os burgueses, a intromissão do mundo público na esfera privada era ilegítima e condenável, no terceiro espírito do capitalismo a vida privada pode ser legitimamente apreendida pela esfera econômica em razão das transformações nas formas de justificação da cidade por projetos. Conforme o foco da atenção se desvia dos processos – na organização burocrática – para a produtividade individual, a própria personalidade do indivíduo, antes relacionada à vivência privada, torna-se, no capitalismo conexionista, um asset a ser capitalizado no mercado. Etapa fundamental dessa capitalização é constituída pela exibição de si nas redes sociais (2017, p. 342).

Os estudos apresentaram aspectos relevantes sobre os SRSO e os riscos que afetam a privacidade. O estudo de Leitzke e Rigo (2020), por exemplo, traz uma reflexão sobre a forma como a sociedade vem se moldando diante de um cenário em que a exposição em SRSO pode gerar benefícios (THIBES, 2017). Mas para isso os autores deixam claro que é preciso ser aceito por comunidades existentes como as que surgem a partir de padrões de beleza. Por isso, ele menciona a existência de uma sociedade de controle, que é vigiada e controlada por meio de discursos, e que são utilizados como formas de seleção.

A existência de possíveis dicotomias a partir da observação dos SRSO é outro aspecto abordado pelos autores. A dicotomia entre público e privado foi tratada por exemplo por Barriga (2020). O que o autor menciona assim como Rebs (2017) é que qualquer indivíduo pode ter acesso ao que um outro usuário publica. Outros autores enfatizam que esse caráter de público estaria interferindo em problemas de privacidade (ASSUMPÇÃO; SANTANA; SANTOS, 2017). Em contrapartida, as empresas de SRSO oferecem aos seus usuários mecanismos de proteção a dados e a privacidade (ASSUMPÇÃO; SANTANA; SANTOS, 2017). Embora, se afirme que os mecanismos de proteção de dados e de privacidade são de difícil entendimento (SANTOS; PORTO; ALTURAS, 2010) e que portanto devem ser aperfeiçoados para que se consiga de fato se ter o caráter também privado . É por isso, que se fala em dicotomia e até na existência de um ambiente híbrido (BARRIGA, 2020) que seria uma mescla entre o público e privado.

Outro aspecto mencionado nos estudos é que para os usuários a privacidade deixou de ter importância ou que está desaparecendo (BARRIGA, 2020) ou que possui valores diferentes para as gerações de usuários (ZAKIEE; HAGE; KUBLIKOWSKI, 2019,

MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020) ou ainda que a privacidade está vulnerável (LIMA, 2018) ou mesmo que as Condições de Uso ou a Política de Privacidade das empresas não é algo tão claro aos usuários (FUGAZZA; SALDANHA, 2018, SÁ, 2018).

O fato é que os indivíduos sabendo ou não dos riscos que possam sofrer em decorrência do uso de SRSO parecem estar dispostos a se exibir cada vez mais, pois têm uma necessidade de serem notados, de serem vistos como afirma Amaral Filho e Blanco (2014) e Lima (2018). Assim, os SRSO se tornam o melhor instrumento de visibilidade. Há quem diga que a visibilidade em SRSO seja algo compulsório, permanente (AMARAL FILHO; BLANCO, 2014), em que o indivíduo não tem opção de escolha de quando ou não ficar visível.

Quanto ao acesso a publicações, Santos, Porto e Alturas (2010) afirmam existir uma ambiguidade sobre a privacidade (SANTOS; PORTO; ALTURAS, 2010). O que os autores enfatizam é que às vezes um usuário pode permitir o acesso a uma publicação quando por exemplo compartilha algo apenas com os amigos. Em outra perspectiva um usuário pode negar o acesso à mesma publicação para certos grupos tais como os familiares, o que os autores entendem como uma situação de relativização de privacidade (SANTOS; PORTO; ALTURAS, 2010).

Retornando à questão da visibilidade e da exposição (MARTORELL; NASCIMENTO; GARRAFA, 2016) é possível perceber nos estudos que existe uma certa seletividade daquilo que se publica (ZAKIEE; HAGE; KUBLIKOWSKI, 2019), ou seja os usuários teriam uma preferência em publicar apenas fatos positivos de suas vidas. Os autores afirmam que o *Instagram* é um tipo de SRSO que incentiva este tipo de seletividade de publicação.

Cabe ressaltar que a exposição e a visibilidade permitem que dados sejam acessados (JURNO; D'ANDRÉA; 2017, STRECK; PELLANDA, 2017) em função de uma produção de dados feita pelos usuários nunca antes vista e que hoje é considerada pelas empresas como uma valiosa mercadoria (BORGES, 2020).

Há também uma falsa sensação de segurança em relação aos dados e à privacidade (ZAKIEE; HAGE; KUBLIKOWSKI, 2019). Neste caso pelo fato de publicarem imagens e vídeos com os quais apenas familiares e amigos teriam acesso. Em contrapartida, certos usuários estariam com receio de publicar em SRSO, pois acreditam que seus dados financeiros possam ser de alguma forma acessados e utilizados (EVERTON, *et al.,* 2014).

Contrariamente a visibilidade que muitos buscam em SRSO, existem aqueles usuários que preferem manter a invisibilidade e o anonimato, como no caso dos haters (REBS, 2017).

Existem outros aspectos marcantes em SRSO tais como um elevado número de acessos (AMARAL FILHO; BLANCO, 2014). Isso pode estar associado à quantidade de perfis que um mesmo usuário pode criar, uma vez que não há restrição em relação a isso em SRSO. Outro aspecto importante é que os SRSO oferecem uma diversidade de opções para a interação entre os usuários (AMARAL FILHO; BLANCO, 2014). Tais recursos seriam uma forma de captação de dados pelas empresas (AMARAL FILHO; BLANCO, 2014, BARRIGA, 2020). Além disso, outras características dos SRSO e aspectos relacionados à privacidade de dados foram detalhadas na Seção 5.

5 DISCUSSÃO

A discussão foi desenhada da seguinte forma, cada subseção trata sobre as perspectivas da privacidade a partir da Taxonomia da Privacidade, proposta por Rodrigues e Sant'Ana. Nesse sentido, a primeira subseção descreve questões do Grupo I Coleta de Informações, sendo composto pelos subgrupos Vigilância e Interrogatório. A segunda subseção envolve problemas relacionados ao Processamento de Informações, formando o Grupo II. O Grupo é composto pelos subgrupos Agregação, Identificação, Insegurança, Uso secundário e Exclusão. A terceira subseção é a de Disseminação de Informações e compõe o Grupo III. O grupo é composto pelos subgrupos Quebra de confidencialidade, Divulgação, Exposição, Ampliação de Acesso, Chantagem, Apropriação e Distorção. O quarto e último grupo é a Invasão, que tem como subgrupos a Intrusão e a Interferência decisional. Cada seção apresenta informações aderentes das comunicações científicas analisadas na seção 4.

Ao final desta seção, se desenvolveu uma síntese com os potenciais riscos relacionados à privacidade de dados identificados na literatura - um dos objetivos específicos desta investigação.

5.1 Coleta de Informações

A coleta de dados em SRSO assim como ocorre em ambientes *off-line* são realizados para fins específicos ou pré-determinados. O Censo Demográfico é um exemplo de coleta de dados em ambientes *off-line.* Este tipo de coleta é realizado anualmente pelo Instituto Brasileiro de Geografia e Estatística - IBGE, que tem por objetivo mapear a situação atual da sociedade brasileira em diversos âmbitos (O IBGE…, 2022).

Nos ambientes *on-line* a coleta de dados segue padrões parecidos com os da coleta de informações em ambientes *off-line*. São entendidos como processos que podem ser contínuos ou não a depender dos objetivos. Cada processo é configurado por meio do planejamento e da execução de etapas. Em ambientes *on-line* a coleta de dados é bem estruturada. É necessário definir os objetivos, as estratégias, bem como as metodologias a serem aplicadas e as fontes de coleta (RODRIGUES, SANT'ANA, 2016).

A coleta de dados é a fase que mais preocupa em relação à privacidade (ASSUMPÇÃO; SANTANA; SANTOS, 2015), uma vez que os mecanismos de controle com os dados são limitados ou inexistentes em SRSO (FUGAZZA; SALDANHA, 2018). Isto significa dizer que uma vez que os dados são publicados não existem mais formas de impedir que eles sejam utilizados por empresas ou por terceiros o que impacta diretamente no descontrole sobre os dados e sobre a privacidade pelos usuários (AMARAL FILHO; BLANCO, 2014; ASSUMPÇÃO; SANTANA; SANTOS, 2015).

As empresas de SRSO coletam dados e metadados (ASSUMPÇÃO; SANTANA; SANTOS, 2017; SÁ, 2018) sobre o cotidiano dos usuários relacionados em uma lista bastante extensa. São fotos, marcação do local de onde as fotos foram tiradas, comentários, imagens e vídeos (ROSADO; TOMÉ, 2015; STRECK; PELLANDA, 2017) e tudo isso é uma rotina para as empresas (FUGAZZA; SALDANHA, 2018).

A produção de dados é algo inerente aos SRSO. Entretanto as formas como são produzidos sofrem variações e podem ser categorizados por tipos de ações em que são gerados pelos usuários.

A coleta de dados pode ocorrer de forma transparente ou de forma não transparente, indicando tipos de coleta existentes tais como a vigilância e o interrogatório (RODRIGUES, SANT'ANA, 2016). A coleta de dados indica também a existência de possíveis riscos relacionados à privacidade dos usuários. E as consequências do que ocorre com a privacidade irá depender do nível e da quantidade de informações fornecidas ou identificadas (GROSS; ACQUISTI, 2005; RODRIGUES; SANT'ANA, 2016).

Para as empresas o que é mais interessante não é proporcionar privacidade aos dados dos usuários e sim a sua transparência (FUGAZZA; SALDANHA, 2018). Somado a isso, tem-se uma certa ausência de compreensão por parte dos usuários sobre como os dados são coletados, para que são coletados e que tipo de riscos sofrem ao ter os dados utilizados por empresas. Cabe ainda mencionar que os usuários concedem a permissão de

coleta de dados às empresas (ASSUMPÇÃO; SANTANA; SANTOS, 2015). Tudo isso fomenta a coleta e o mercado relacionado a dados.

5.1.1 Vigilância

Uma das características da sociedade da informação ou em rede (CASTELLS, 1999; SIMON, c1998) ainda pouco discutidas é o papel que as TIC têm gerado tanto no controle como na vigilância dos indivíduos (SIMON, c1998).

Levy afirma que não existe nada que se possa identificar na informática que não seja imutável e exemplifica citando os computadores. As mudanças podem ocorrer com as próprias máquinas que se tornam mais modernas e atuais, perpassando pelo uso dos meios de comunicação. Levy menciona ainda que os computadores são redes de interfaces disponíveis para novas conexões mas que são ao mesmo tempo imprevisíveis e que como ele afirma são capazes de modificar de maneira radical tanto seu significado quanto seu uso (LÉVY, 1993).

De fato, as TIC modificaram o cotidiano dos indivíduos, principalmente a forma como eles se comunicam, se divertem ou aprendem. Mas por outro lado, o acesso e o uso de dispositivos móveis com os quais os usuários acessam os SRSO tornaram sua privacidade mais frágil, permitindo que qualquer outro indivíduo, instituições públicas ou privadas tenham acesso a dados, por meio por exemplo da vigilância.

A vigilância é o ato de observar alguém em suas atividades e fazer deste ato uma forma de controle. Para Rodrigues e Sant'Ana vigiar significa monitorar um indivíduo ou instituições, seja em suas atividades públicas ou privadas. A vigilância também ocorre em SRSO (RODRIGUES; SANT'ANA, 2016) sendo identificada na RSL.

Os SRSO são um novo modelo de vigilância mas são também extensões das relações sociais (ROSADO; TOMÉ, 2015; ZAKIEE; HAGE; KUBLIKOWSKI, 2019) presenciais vividas no espaço físico (ROSADO; TOMÉ, 2015). Nesse modelo há uma consolidação de uma sociedade de controle baseada nas relações de poder, em opiniões, nos discursos e nas ações de vigilância, assim como por meio da manipulação e da apropriação de dados. Esse modelo é análoga à sociedade de vigilância de Michel Foucault em que os indivíduos eram controlados por paranópticos (FUGAZZA; SALDANHA, 2018; BARRIGA, 2020; LEITZKE; RIGO, 2020), sendo na contemporaneidade vigiados por empresas e por indivíduos.

Somado a isso existem questões de TIC interferindo na relação dos indivíduos de controlado e de controlador. Julga-se que as experiências de indivíduos nascidos pós

internet têm um peso diferente em relação ao uso de tecnologias virtuais (SRSO) do que aqueles que não tiveram contato imediato com as plataformas (ZAKIEE; HAGE; KUBLIKOWSKI, 2019; MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020). O que os autores querem dizer é que os usuários que tiveram contato mais rápido com a internet e com os SRSO têm percepções diferentes sobre fornecimento de dados e sobre a privacidade indicando que isso seja portanto um problema geracional.

Além destes aspectos existem outros que podem ser relacionados a vigilância. O acesso a internet e aos dispositivos móveis contribuem para o uso intenso e frequente de SRSO pelos usuários (ASSUMPÇÃO; SANTANA; SANTOS, 2015; LIMA, 2018; BARRIGA, 2020). Tudo isso faz com que os SRSO tais como o *Facebook* possam ser baixados em qualquer *smartphone* ficando acessíveis a qualquer momento (ROSADO; TOMÉ, 2015; BARRIGA, 2020). Além disso, os dispositivos móveis mais modernos já vem com câmeras acopladas para facilitar a captura de imagens (STRECK; PELLANDA, 2017) facilitando também o processo de divulgação.

Os SRSO são movidos graças à produção de conteúdos de dados (JURNO; D'ANDRÉA; 2017). Desde que os dispositivos móveis passaram a integrar a vida dos indivíduos a produção e a divulgação de dados (BARRIGA, 2020) se tornaram quase que instantâneas (STRECK; PELLANDA, 2017). Assim, os usuários se tornaram os maiores produtores e os maiores consumidores de dados. E a maior parte dos dados produzidos por eles são o resultado do processo de interação (ASSUMPÇÃO; SANTANA; SANTOS, 2017).

A interação (AMARAL FILHO; BLANCO, 2014; ASSUMPÇÃO; SANTANA; REBS, 2017; SANTOS, 2017; LIMA, 2018; BARRIGA, 2020) e a diversidade de recursos utilizados pelos usuários em meio on-line são fatores que facilitam a vigilância.

Para que a vigilância se concretize é necessário que as empresas de SRSO adotem estratégias e uma das formas encontradas é fazer com que os usuários interajam cada vez mais. Para isso oferecem recursos de entretenimento e de interação tais como salas de bate-papo, murais, notícias sobre eventos, *story*, mensagens instantâneas e vídeos curtos, os quais são desenvolvidos pelas empresas como forma de melhorar a dinâmica nesses ambientes (PURIM; TIZZOT, 2019; BARRIGA, 2020).

De acordo com Boff, Fortes e Freitas (2018), a justificativa do controle é dar poder para que a burguesia exerça controle sobre as massas de forma delimitada e também efetiva. Essa forma de vigilância adotada pelas empresas de fato tem se mostrado bem

efetiva uma vez que realizam ações de vigilância sem que os usuários percebam. Oferecem recursos, criam novos produtos de TIC, trazem novas versões de dispositivos móveis. Assim, ao mesmo tempo em que oferecem novas formas de entretenimento, realizam paralelamente a coleta de dados e a vigilância.

Fugazza e Saldanha afirmam que a vigilância não ocorre apenas em uma direção, de empresa para usuário, mas estaria acontecendo também de usuário para usuário (FUGAZZA; SALDANHA, 2018). Além disso, tanto o Estado quanto as empresas são responsáveis pelo controle de dados e de metadados (ASSUMPÇÃO; SANTANA; SANTOS, 2015; FUGAZZA; SÁ, 2018; SALDANHA, 2018; BARRIGA, 2020).

Outro aspecto observado é que os usuários parecem dar mais prioridade à exposição do que fazem em seu dia a dia do que a privacidade. Barriga diz que os usuários não estão tão preocupados com a privacidade e por isso publicam dados de forma deliberada (BARRIGA, 2020).

A vigilância pode não somente atingir usuários com perfis formalmente registrados mas outros indivíduos ou grupos que nem sequer tenham conta e registro em SRSO, como é o caso de crianças, que têm suas imagens publicadas por usuários ativos com algum grau ou não de parentesco.

Pacientes e clientes de profissionais relacionados à área de estética e da saúde podem ser também potenciais alvos da vigilância. Os profissionais da área da saúde buscam visibilizar os procedimentos feitos em consultórios publicando imagens de seus pacientes. A discussão de casos clínicos (PURIM; TIZZOT, 2019) pelos profissionais por meio de SRSO pode indicar a existência de compartilhamento de dados considerados sensíveis uma vez que são dados de pacientes cuja revelação deve estar pautada no aspecto ético.

As mulheres compõem uma considerável parcela de clientes de profissionais da estética. Este grupo pode ser monitorado tanto por empresas, pois podem ser potenciais consumidores de produtos de beleza ou por clínicas que ofertam procedimentos estéticos por meio de anúncios bem como podem se tornar vítimas de stalkers.

5.1.2 Interrogatório

O segundo tipo de coleta de dados se dá pelo processo de Interrogatório. O processo acontece quando se pretende obter dados por meio de perguntas como ocorre por exemplo em formulários ou em entrevistas, caracterizando-se como uma forma direta e transparente de coleta de dados. Em SRSO os dados são solicitados e fornecidos no

momento do preenchimento de formulários disponibilizados aos usuários nas plataformas dos SRSO (BOYD; ELLISON, 2007; RODRIGUES; SANT'ANA, 2016).

Os dados solicitados aos usuários incluem nome e sobrenome, idade, gênero ou data de aniversário, Cadastro de Pessoa Física (CPF), número de telefone (SÁ, 2018). Sem a prévia informação dos dados (LIMA, 2018; SÁ, 2018) o usuário não terá como ter acesso aos SRSO sendo esta uma condição obrigatória (SÁ, 2018).

Diante de tudo isso, percebe-se que a coleta de informações é um potencial risco para a privacidade. Este assunto ainda é muito delicado e parece ser uma mão de via dupla, pois ao mesmo tempo que o usuário necessita utilizar um SRSO para buscar entretenimento ou se relacionar com outros usuários, se vê também incentivado a publicar dados. Portanto entende-se que é bem complexo para o usuário ter controle sobre a sua privacidade.

5.2 Processamento da Informação

Os dados coletados sobre os usuários decorrentes do processo de Vigilância e de Interrogatório são armazenados "[...] em uma camada física [...], com o auxílio de softwares utilizados para a manipulação de dados (RODRIGUES; SANT'ANA, 2018, p. 25). Posteriormente eles são reunidos e processados. É por meio do processamento que se identifica por exemplo os interesses e gostos dos usuários (EVERTON, *et al.,* 2014).

Processar significa extrair dados de uma fonte e a partir dela construir um conjunto de informações. Para entender como ocorre o processamento de dados em SRSO é preciso saber como e onde eles são armazenados e de que forma são utilizados.

No contexto de SRSO as fontes de coleta de dados são os dados publicados pelos usuários e são atualmente considerados como mercadoria (AMARAL FILHO; BLANCO, 2014; FUGAZZA; SALDANHA, 2018; BORGES, 2020). Os dados ficam armazenados de forma permanente em bancos de dados (JURNO; D'ANDRÉA, 2017; PELLANDA; STRECK, 2017). Os dados armazenados são processados por sistemas computacionais de e são transformados em informações sobre os usuários (BOFF; FORTES; FREITAS, 2018).

Para Thibes (2017) a vida privada antes era algo que podia ser protegido e podia estar seguro, longe de curiosos, fosse por meio dos muros da residência ou pela própria concepção do que deveria estar sob sigilo. Mas atualmente, a vida privada deixou de ter relevância e passou a ser algo que pode ser negociado (THIBES, 2017).

Os dados são a mercadoria mais valiosa (AMARAL FILHO; BLANCO, 2014; BORGES, 20202) e por isso são negociados com terceiros como as empresas de marketing ou representantes de produtos ou de serviços. E dessa negociação resultam lucros exorbitantes (BORGES, 2020).

Assim, transformar grandes quantidades de dados, sejam eles textuais ou não, estruturados ou não estruturados contribui para o fornecimento de informações úteis (BOFF; FORTES; FREITAS, 2018).

Assim, para que os dados possam ser úteis às empresas eles precisam passar pela fase de Processamento que incluem seis etapas sendo elas: a Agregação, a Identificação, a Insegurança, o Uso Secundário e a Exclusão (RODRIGUES; SANT'ANA, 2016).

5.2.1 Agregação

No Processamento da Informação agregar significa somar ou combinar algo a um dado armazenado. Quanto mais dados se coletam a partir de múltiplas fontes melhor será para o processo de Agregação. O resultado do processo de Agregação é a obtenção e revelação de informações sobre os usuários (RODRIGUES; SANT'ANA, 2016).

Os SRSO são espécies de *websites ou gêneros de websites* constituído por redes coletivas de participantes que produzem conteúdos variados de dados e de forma diária. Fatos do cotidiano ou as curtidas, os compartilhamentos, o uso de *hashtags,* o uso de códigos ou um conjunto de dados provenientes de várias fontes como as que convergem pelo Feed de Notícias (FN) (JURNO; D'ANDRÉA, 2017; STRECK; PELLANDA, 2017), são exemplos de dados que podem ser combinados a outros já existentes em banco de dados.

Para que as informações sobre um usuário sejam mais consistentes é preciso extrair o maior número de dados disponibilizados pelo usuário ou por amigos, familiares, ou por qualquer usuário de sua rede de relacionamento (ROSADO; TOMÉ, 2015; JURNO; D'ANDRÉA, 2017).

Quando um usuário concede o direito às empresas de coletarem dados estão também dando condições a elas de fazerem associações a partir do uso de dispositivos móveis com os quais eles acessam um SRSO, o que gera muitas formas de coleta de dados, especialmente de imagens (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

Quando se publica uma fotografia no *Instagram* é possível agregar outros dados a imagem que foi armazenada, tais como a marcação do local de onde a foto foi registrada bem como as curtidas, compartilhamentos ou *emojis* (STRECK; PELLANDA, 2017).

5.2.2 Identificação

Os dados coletados e agregados resultam na identificação de informações sobre os usuários (RODRIGUES; SANT'ANA, 2016). De uma forma geral, dados identificáveis, tais como imagem pessoal, nome e sobrenome estão disponíveis a qualquer pessoa que esteja registrada em qualquer rede de usuários membros do *Facebook,* por exemplo (GROSS; ACQUISTI, 2005), porque são ambientes públicos (ASSUMPÇÃO; SANTANA; SANTOS, 2015), embora Barriga (2020) considere que podem ser ambientes híbridos, ou seja dependendo de cada contexto ou situação podem ser tanto público como privado.

Um usuário que tenta manter sua privacidade em um SRSO pode ser identificado por meio de publicações de imagens feitas em perfis de amigos, familiares ou de profissionais de saúde quando estes realizam por exemplo procedimentos estéticos. (MARTORELL; NASCIMENTO; GARRAFA, 2016).

Existem técnicas utilizadas pelas empresas para realizar a identificação de um usuário a partir de fragmentos de publicações. O reconhecimento facial é uma forma de identificação de dados realizada por meio de análise de imagem. Mesmo que um indivíduo tenha publicado apenas parte de seu rosto em uma imagem é possível identificar características suas que combinadas a outras publicadas permita identificá-lo (MARTORELL; NASCIMENTO; GARRAFA, 2016; ASSUMPÇÃO; SANTANA; SANTOS, 2017).

5.2.3 Insegurança

Qualquer atividade executada por empresas ou por outros usuários que venha a colocar em risco os dados e a privacidade dos usuários pode ser configurado como uma atividade pouco confiável e portanto insegura para acesso e uso de SRSO. O vazamento de dados é um caso típico de vulnerabilidade e de insegurança (RODRIGUES; SANT'ANA, 2016; LIMA, 2018).

Não está muito claro a questão da vulnerabilidade no uso e no compartilhamento de dados em SRSO para os usuários. Primeiro porque eles desconhecem as consequências do compartilhamento de dados. Em segundo lugar, eles não apenas confiam na privacidade de seus dados a aqueles que compõem a sua rede de relacionamento como também a terceiros, que muitas vezes se aproveitam da situação de visibilidade para obterem vantagens (BOFF; FORTES; FREITAS, 2018).

Fatores como os que foram identificados na RSL causam preocupação e insegurança em relação aos dados e à privacidade. O fato de serem ambientes públicos

(ASSUMPÇÃO; SANTANA; SANTOS, 2015; REBS, 2017) dificulta e interfere na manutenção da privacidade dos usuários (ASSUMPÇÃO; SANTANA; SANTOS, 2017), uma vez que os dados percorrem muitas conexões e portanto ficam acessíveis a qualquer um. Isso facilita também o uso de dados de forma não autorizada (ASSUMPÇÃO; SANTANA; SANTOS, 2017; FUGAZZA; SALDANHA, 2018; REBS, 2017).

A própria política de privacidade de SRSO como o do *Facebook* gera vulnerabilidade (BORGES, 2020; FUGAZZA; SALDANHA, 2018). Embora existam mecanismos para controle de acesso a dados e sejam até simples de serem utilizados não são suficientemente flexíveis a ponto de garantir segurança aos usuários (SANTOS; PORTO; ALTURAS, 2010), mesmo porque os SRSO são mais bem elaborados do que os ambientes *off-line* (FUGAZZA; SALDANHA, 2018).

Uma outra situação de vulnerabilidade identificada na RSL que causa insegurança é a criação de multiperfis ou de perfis falsos (FUGAZZA; SALDANHA, 2018; LIMA, 2018; SANTOS; PORTO; ALTURAS, 2010; ROSADO; TOMÉ, 2015). Indivíduos estranhos às redes dos usuários se aproveitam da invisibilidade, de perfis falsos ou do uso de multiperfis para ter acesso a páginas pessoais dos usuários. Alguns com a intenção de cometerem crimes tais como o da perseguição, da falsidade ideológica ou mesmo para obterem informações sigilosas tais como os dados bancários (EVERTON, *et al.,* 2014; FUGAZZA; SALDANHA, 2018; SANTOS; PORTO; ALTURAS, 2010; REBS, 2017).

Manter os dados seguros, longe da vigilância de estranhos pode tornar o uso de SRSO menos inofensivo. Uma das formas de controlar os riscos é executar os recursos de configurações disponíveis nas plataformas. Evitar fornecer alguns dados, tais como status de relacionamento, ou publicar fotos sem marcação de localização. Manter suas redes de relacionamento o mais restrito possível.

5.2.4 Uso secundário

O Uso Secundário corresponde ao ato de usar dados para uma finalidade mas que ao mesmo tempo pode ser usado para outros fins (RODRIGUES; SANT'ANA, 2016).

A priori, as empresas de SRSO são moldadas para a interação dos indivíduos (ASSUMPÇÃO; SANTANA; SANTOS, 2015; BARRIGA, 2020; GONZATTI; BITTENCOURT; ESMITIZ, 2015; LIMA, 2018). Embora isso aconteça, as empresas têm outras pretensões para os dados produzidos ou que resultam das interações.

O Marketing direcionado é um exemplo de Uso Secundário de Dados. Para isso, as empresas realizam a personalização de perfis recorrendo aos algoritmos (BORGES, 2020;

JURNO, D'ANDRÉA, 2017; FUGAZZA; SALDANHA, 2018). Os perfis são moldados para ter o jeito do usuário. E baseado nos dados fornecidos pelos usuários é possível que as empresas consigam decifrar que tipos de produtos ou de serviços os usuários podem adquirir.

Uma das técnicas de processamento é a caracterização de perfil, ou de perfilamento (Profiling) (BOFF; FORTES; FREITAS, 2018). A técnica é aplicada nos dados dos usuários. Os autores ainda mencionam que a finalidade do emprego da técnica é saber o que é importante para certos grupos de indivíduos, a partir de uma amostra (BOFF; FORTES; FREITAS, 2018).

O Marketing via SRSO não é algo democrático pois não é dado ao usuário o direito de escolher se aceita ou não que propagandas sejam exibidas em seu FN. Este tipo de ação parece estar de encontro a liberdade de escolha do usuário.

Por outro lado, alguns usuários consideram o *Instagram* como um SRSO seguro para publicar dados. Eles acreditam que suas publicações serão visualizadas apenas por amigos mais próximos, portanto não precisam se preocupar tanto com a privacidade. Essa confiança leva os usuários a ficarem permanentemente logados em suas contas fazendo com que seja possível compor um diário completo sobre o usuário (ZAKIEE; HAGE; KUBLIKOWSKI, 2019).

O diário completo de dados pode ser utilizado por terceiros (BORGES, 2020; SÁ, 2020) e isso descredibiliza o *Instagram* como um SRSO que pode ser considerado seguro. Anúncios de publicidade como os de agências de viagens podem surgir nas páginas dos usuários. Portanto, isso significa que as empresas têm interesse em obter lucro e não em proteger a privacidade de dados dos usuários (FUGAZZA; SALDANHA, 2018).

5.2.5 Exclusão

A atividade de exclusão se configura como uma ausência na capacidade de decisão dos usuários sobre o que é realizado com seus dados, principalmente na fase de coleta, armazenamento, uso e compartilhamento de dados (RODRIGUES; SANT'ANA, 2016).

Uso de dados de pacientes por profissionais de saúde (MARTORELL; NASCIMENTO; GARRAFA, 2016) para fins de compartilhamento com outros profissionais e até com outros usuários é caracterizado como uma atividade de exclusão. Os dados são utilizados e compartilhados por meio de conexões sem que seja dada a chance aos pacientes de decidir se gostariam ou não que seus dados fossem utilizados.

Casos de recompartilhamento de publicações ou de compartilhamento em cadeia (AMARAL FILHO; BLANCO, 2014; BORGES, 2020; GONZATTI; BITTENCOURT; ESMITIZ, 2015; SANTOS; PORTO; ALTURAS, 2010) podem ser caracterizadas também como exclusão.

O usuário que decidiu compartilhar suas publicações apenas com usuários mais confidenciais como os amigos corre o risco de ter sua publicação recompartilhada por algum deles. É preciso ter ciência de que até o presente momento não é possível evitar o compartilhamento ou recompartilhamento de publicações, mesmo porque os SRSO são muito dinâmicos e difíceis de serem controlados.

Outro fator que contribui para a exclusão é a ausência de garantias de que os dados armazenados pelas empresas sejam removidos definitivamente. Um usuário pode apagar uma postagem de uma imagem publicada em sua página mas não de forma permanente, mesmo porque elas ficam armazenadas em banco de dados (ASSUMPÇÃO; SANTANA; SANTOS, 2015; JURNO; D'ANDRÉA; 2017; STRECK; PELLANDA, 2017) e podem ser recuperadas quando necessário (ASSUMPÇÃO; SANTANA; SANTOS, 2015). Portanto isso pode causar uma falsa sensação de segurança e ao mesmo tempo demonstra que os usuários podem não ter gerência sobre seus dados. E se existe uma ausência de gerência sobre os dados isto implica em riscos à privacidade.

Assim, a atividade de exclusão está relacionada ao uso indevido de dados associada à ausência de autorização formal pelo usuário para uso e compartilhamento de dados por profissionais de qualquer atividade profissional ou por qualquer outro usuário.

5.3 Disseminação da Informação

A disseminação da informação é o ato de promover a visibilidade de algo independente da forma ou do meio de divulgação. Na Taxonomia da Privacidade está dividida em seis tipos de atividades que podem ser identificadas por meio da Quebra de Confidencialidade, Divulgação, Exposição, Ampliação de Acesso, Chantagem e a Apropriação (RODRIGUES; SANT'ANA, 2016).

Existe uma rapidez na disseminação de dados (SANTOS; PORTO; ALTURAS, 2010). Este fator impacta na perda de controle sobre os dados uma vez que são publicados e se espalham rapidamente de forma viral (AMARAL FILHO; BLANCO, 2014; GONZATTI; BITTENCOURT; ESMITIZ, 2015). As celebridades por exemplo são tipos de usuários que têm suas publicações percorrendo as conexões três vezes mais rápidas que os demais usuários (GONZATTI; BITTENCOURT; ESMITIZ, 2015).

Além disso, o *Facebook* é comparado a uma vitrine onde os dados são disseminados e tem um alcance global uma vez que são utilizados por milhões de usuários (AMARAL FILHO; BLANCO, 2014).

Todos esses fatores levam a inferir que existe uma dinamicidade na disseminação de dados e que as publicações realizadas por celebridades são disseminadas de forma mais rápida. A velocidade com que as publicações e os dados são compartilhados é outro fator que chama a atenção e pode ser um aspecto que pode ter muitas variações e elementos intrínsecos e extrínsecos, sendo portanto um interessante tema a ser investigado.

5.3.1 Quebra de confidencialidade

É possível entender que a violação ou quebra de confidencialidade (RODRIGUES; SANT'ANA, 2016) acontece quando há uma ruptura de confiança de uma das partes envolvidas na manutenção da privacidade.

A ruptura de confiança pode estar associada ao entendimento de que os dados devem estar visíveis a todos e em qualquer momento, o que Fugazza e Saldanha denominam de cultura de transparência de dados. Essa cultura segundo os autores é justificada como sendo um ato de cidadania. Mencionam ainda que o fato dos usuários terem absorvido essa cultura tão bem deixa a parte discussões mais relevantes sobre a privacidade (FUGAZZA; SALDANHA, 2018).

Um exemplo dessa ruptura são as publicações realizadas pelos profissionais de saúde que utilizam cada vez mais os SRSO como meio de promoção de suas atividades (MARTORELL; NASCIMENTO; GARRAFA, 2016). Considera-se que seja um uso inadequado uma vez que estão publicando imagens de pacientes de forma indevida e não autorizada. Como foi verificado nos estudos isso pode desencadear uma série de riscos aos pacientes, entre eles está a ridicularização ou julgamentos.

A confidencialidade é um aspecto que garante que os dados dos usuários fiquem visíveis apenas a quem tenha autorização de acesso (ASSUMPÇÃO; SANTANA; SANTOS, 2015; SANTOS; PORTO; ALTURAS, 2010).

Porém a autorização de acesso não garante segurança e nem tampouco que as publicações compartilhadas apenas com os amigos sejam mantidas privadas. Um usuário pode definir por meio de configurações disponíveis nas plataformas de SRSO quem serão os usuários a terem acesso a sua página e as suas publicações. Mas em algum momento um dos amigos pode romper com a confidencialidade e compartilhar as publicações com

outros usuários estranhos a sua rede de relacionamento (ASSUMPÇÃO; SANTANA; SANTOS, 2015).

5.3.2 Divulgação

A divulgação consiste em usar meios ou atividades com a intenção de publicar conteúdos de dados sobre os indivíduos. O problema é que em SRSO aquilo que é publicado ou divulgado pode ser alterado ou retirado do contexto original (RODRIGUES; SANT'ANA, 2016) podendo ser recebido e interpretado de maneira equivocada por outros usuários resultando em julgamentos equivocados ou que podem ser alvo de crimes.

A divulgação de publicações realizadas por mulheres levam a possíveis crimes tais como do stalking. O stalkeador seleciona publicações preferencialmente de mulheres, descobre número de telefone e envia mensagens de forma persistente.

Neste contexto, as mulheres são um tipo de público que pode ter problemas com a privacidade do que é divulgado. Ao acessar o *Facebook* podem ser alvos de incomodações como as paqueras. Esse tipo de contato é realizado normalmente durante a madrugada por meio de *chats* (MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020). Essa tentativa de conexão e do que é conversado pode ser retirado do contexto original ou ser divulgado de forma parcial levando a problemas com familiares, amigos e companheiros.

Portanto, a divulgação implica em situações difíceis de serem tratadas, pois mexem com a privacidade, o direito de ser deixado só, e a liberdade individual (SOLOVE, 2008). Recentemente no Brasil foi aprovada a Lei 14.132, de 31 de março de 2021 (BRASIL, 2021) que trata de crimes relacionados à perseguição em quaisquer meios e que levem ao constrangimento ou restrição de liberdade de um indivíduo ou qualquer outra questão relacionada à privacidade. A Lei ainda prevê que a penalidade seja acrescida quando cometida contra idoso, criança, adolescente ou mulheres, podendo a penalidade chegar a dois anos de reclusão (BRASIL, 2021).

5.3.3 Exposição

A exposição está relacionada ao uso de imagens ou de dados obtidos em situações delicadas, comprometedoras ou que deveriam ser mantidas em sigilo máximo. Ainda que a publicação possa ser deletada não impede que transtornos possam ser causados aos usuários (RODRIGUES; SANT'ANA, 2016).

Os SRSO são plataformas que facilitam a exposição e por isso são confundidos como palcos onde o cotidiano dos usuários é o grande espetáculo da vida íntima (ZAKIEE; HAGE; KUBLIKOWSKI, 2019). Por isso, a publicação de certos dados pelos usuários

deveria ser ainda mais criteriosa, ainda mais quando se trata de dados que podem causar danos graves, como por exemplo no caso de exposição de partes do corpo ou da nudez (RODRIGUES; SANT'ANA, 2016).

A manutenção da privacidade de pacientes por profissionais de saúde é uma prioridade de acordo com os conselhos de ética. Entretanto, o que se nota na análise dos estudos realizados na RSL é que alguns profissionais utilizam os SRSO para publicarem suas atividades ou para discutir casos clínicos, expondo dados que deveriam ser mantidos sob sigilo, ferindo assim os direitos à privacidade de pacientes (MARTORELL; NASCIMENTO; GARRAFA, 2016; PURIM ; TIZZOT, 2019).

Dados financeiros são dados sigilosos que são solicitados em transações comerciais *on-line* (BOFF; FORTES; FREITAS, 2018; EVERTON, *et al.,* 2014) e que tem preocupado alguns usuários (EVERTON, *et al.,* 2014). Tal preocupação se justifica uma vez que estes podem ser rastreados (BOFF; FORTES; FREITAS, 2018) e utilizados como fonte para aplicação de golpes trazendo prejuízos financeiros aos usuários.

A exposição de características físicas de um usuário deveria ser motivo de respeito. Entretanto certos grupos de usuários ao exporem suas imagens são atacados por *haters*, por indivíduos que propagam o discurso do ódio. Um exemplo típico desses ataques é o sofrido por usuários que adotam o cabelo do tipo *black power*. Esses usuários recebem de forma massiva palavras ofensivas, denegrindo o indivíduo e o que ela representa (REBS, 2017).

Portanto há três questões observadas nessa discussão: a exposição de dados considerados sigilosos como os dados financeiros, o de pacientes, e a exposição de características físicas dos usuários. Ainda que os dois primeiros aspectos devam ser prioridade para a manutenção da privacidade, existe a questão da perseguição a indivíduos com padrões de beleza diferentes e que são motivos de ataques e de questionamentos.

A priori, os SRSO são utilizados como ambientes de exibição de padrões de beleza e como lugar de venda de um mundo perfeito. Além disso, servem como ambientes para manutenção de relações sociais, de poder e de divulgação de verdades coletivas, como por exemplo, de um corpo ideal ou de beleza ideal, que muitas vezes não condiz com a realidade. Esses questionamentos são temas que põem em evidência a questão da exposição exacerbada em SRSO e que podem ser abordados em futuras investigações.

5.3.4 Ampliação de acesso

A ampliação se refere à possibilidade de estender o nível de acesso a dados obtidos pelas empresas de SRSO a terceiros mesmo que isso tenha sido acordado nos Termos de

Uso. Assim, quando as empresas detentoras dos dados realizam o compartilhamento com outras empresas está ampliando o acesso a esses dados (RODRIGUES; SANT'ANA, 2016).

A ausência de preocupação dos usuários com o que está descrito nos Termos de Uso pode afetar a privacidade (SÁ, 2018). Além disso, o que está descrito nestes documentos está disponível de forma limitada aos usuários (FUGAZZA; SALDANHA, 2018).

Mas algo que está claro é que todo e qualquer tipo de conteúdo publicado pelos usuários deixam de pertencer a eles e passam a ser propriedade das empresas (FUGAZZA; SALDANHA, 2018).

Os Termos de Uso, a permissão de acesso a dados, o direito à propriedade cedido e a ausência de percepção dos usuários sobre como as empresas utilizam os dados e com quem compartilham torna o mercado de dados ainda mais promissor, pois os dados podem ser negociados sem nenhum tipo de burocracia ou de fiscalização.

Assim, a ampliação de acesso e uso de dados por terceiros (BORGES, 2020), empresas, governos, organizações políticas e até grupos terroristas são potenciais riscos à segurança e à privacidade dos usuários (BARRIGA, 2020).

5.3.5 Chantagem

É qualquer ação direcionada a chantagear, extorquir ou ameaçar usuários (RODRIGUES; SANT'ANA, 2016). Indivíduos mal intencionados podem usar os SRSO para selecionar e acessar páginas pessoais e publicações com a intenção de ameaçar ou de perseguir usuários (GROSS; ACQUISTI, 2005; RODRIGUES; SANT'ANA, 2016).

Um dos problemas discutidos nos estudos da RSL é que esses indivíduos estariam se utilizando do anonimato para cometer alguns crimes. O anonimato dificulta que estes usuários sofram algum tipo de punição. Rebs menciona que a interação entre os usuários e a própria estrutura dos SRSO permitem esses tipos de ações e ainda deixam protegidos aqueles que cometem crimes, uma vez que podem usar do anônimos (REBS, 2018).

Ações como o discurso de ódio (REBS, 2018) contra afrodescendentes, mulheres e integrantes do LGBTQIAi+[17] deixa claro que a privacidade é relevante pois pode ser a parede invisível que separa os usuários de possíveis indivíduos com discurso de ameaça ou de uma ameaça real.

[17] LGBTQIAi+ significa Lésbica, Gay, Bissexuais, Travestis, Queer, Intersexuais, Assexual e demais siglas e identidades relacionadas a este movimento.

O anonimato se dá em função da ausência de controle pelas empresas de SRSO em relação a criação de perfis falsos, sendo um risco eminente para os usuários. Existem tentativas de conexões de indivíduos com perfis falsos com outros usuários. Nesta tentativa os que adotam perfis falsos tentam estabelecer uma relação de confiança (SANTOS; PORTO; ALTURAS, 2010) e com isso praticar crimes como os de extorsão.

Os SRSO são espaços com muita liberdade para se fazer qualquer coisa. Alguns usuários postam conteúdos positivos, de incentivo a ética e a moral, de convivência social saudável. Outros enveredam para o lado do humor, pois imaginam que os indivíduos precisam se divertir. Outros postam conteúdos que refletem seu momento de vida como uma realização profissional ou de um relacionamento afetivo.

O problema é que essa mesma liberdade é dada a indivíduos que disseminam o discurso de ódio, a pedófilos ou estelionatários, em que ao contrário de outros tipos de conteúdos verbalizam, agem e utilizam os SRSO para cometerem crimes direcionados a grupos específicos, que violam e extrapolam qualquer tipo de liberdade.

5.3.6 Apropriação

É o ato de se apropriar de dados para gerar benefícios. Os benefícios podem ser obtidos normalmente quando são vinculados a propagandas com a intenção de obter ganhos financeiros ou para validar algum serviço realizado por profissionais. As empresas podem se apropriar de dados publicados por um usuário como as imagens e associá-lo a uma propaganda publicitária, por exemplo. O problema é que este tipo de atividade muitas vezes não acontece de forma autorizada (RODRIGUES; SANT'ANA, 2016).

O uso de imagens de pacientes para autopromoção por profissionais de saúde é considerada uma apropriação (PURIM; TIZZOT; 2019). Os odontólogos que atuam na área de estética se apropriam de imagens de pacientes como forma de promover o serviço que realizam.

Os dados apropriados nestes casos são divulgados muitas vezes sem a ciência e aprovação dos usuários. É muito incomum que exista algum tipo de contrato em que o usuário possa autorizar a associação de sua imagem a um serviço ou a um produto como forma de garantia para obtenção de algum tipo de vantagem.

É preciso ter ciência de que a apropriação de dados é uma realidade e é uma das dicotomias mencionadas por Barriga (2020). Ao mesmo tempo que os usuários divulgam dados as empresas e a outros usuários com interesses comerciais também se apropriam

deles (BARRIGA, 2020) e por mais que os SRSO sejam “gratuitos” eles não geram nenhum tipo de benefício ou lucro aos usuários (FUGAZZA; SALDANHA, 2018).

Os usuários têm interesse em utilizar um SRSO, desejam interagir e estabelecer conexões com outros usuários, ampliar suas redes de relacionamento, mas há de se questionar se o preço que pagam por isso não seja alto demais uma vez que perdem o controle sobre seus dados. Neste sentido, percebe-se que as empresas têm uma grande vantagem em relação a isso pois os usuários acreditam que a troca possa ser justa.

5.3.7 Distorção

A distorção é o ato de disseminar publicações que podem ser alteradas ou retiradas do contexto original. A distorção pode ainda acontecer por meio da disseminação de informações falsas (RODRIGUES; SANT’ANA, 2016).

Uma imagem ou até mesmo um cenário de uma imagem podem ser alterados por meio de aplicação de filtros na intenção de tornar a imagem mais apresentável e isso é muito comum no *Instagram*. Entretanto este tipo de recurso pode tirar do contexto original, fazendo com que os demais usuários tenham acesso apenas a uma parte dos dados, ou que fatos ou indivíduos sejam omitidos da imagem original (STRECK; PELLANDA, 2017).

5.4 Invasão

São ações relacionadas à invasão de privacidade (RODRIGUES; SANT’ANA, 2016). Invadir significa ir além do permitido ou realizar atividades que não foram permitidas.

Cabe discutir que problemas relacionados à invasão de privacidade são ainda mais frequentes porque ainda não se chegou a uma atribuição de valor e de significado segura sobre a privacidade (LIMA, 2018; SÁ, 2018). Os usuários renunciam a sua privacidade (LIMA, 2018), abrem mão dela em troca da interação e da utilização dos recursos. Isso tudo estaria levando a desvalorização da privacidade e até mesmo do seu desaparecimento (BARRIGA, 2020).

Uma boa reflexão que se pode fazer sobre a privacidade é saber de que forma isso deixou de ter relevância para os indivíduos, ou quais as necessidades que os levaram a expor suas intimidades e seus dados em espaços considerados públicos como os SRSO, sabendo-se que o uso de tais serviços implica em potenciais riscos para o indivíduo e para a sua privacidade.

Neste sentido, os usuários de SRSO tem um papel crucial nos problemas relacionados à privacidade. Primeiro porque os usuários dão condições de serem vigiados.

A realização de um registro, por si só, já produz dados, uma vez que são solicitados para a realização do acesso. O ato de expor publicações produz outros conjuntos de dados, e outras ações realizadas somam-se às iniciais como se fosse um círculo vicioso. E quanto mais publicam e se expõe mais vulneráveis deixam a sua privacidade.

Por outro lado, os mecanismos de defesas contra possíveis invasões disponíveis aos usuários nas Política de Privacidade são bem complexos e dificultam seu uso (SANTOS; PORTO; ALTURAS, 2010).

As jurisprudências existentes para proteger a privacidade de usuários em plataformas de SRSO como o Marco Civil da Internet tem atendido alguns casos, porém de forma isolada (LIMA, 2018). Tudo isso pode afetar a privacidade, deixando os usuários e os dados expostos de forma que possam sofrer dois tipos de ações que são a Intrusão e a Interferência Decisória.

5.4.1 Intrusão

Considera-se que a oferta de recursos disponibilizados aos usuários pelas empresas tais como *story*, *chats*, salas de bate-papo (BARRIGA, 2020; PURIM; TIZZOT, 2019; STRECK; PELLANDA, 2017) sejam mecanismos criados pelas empresas para acessar dados dos usuários. As empresas justificam a oferta de tais recursos como um meio de tornar os SRSO mais dinâmicos (BARRIGA, 2020).

A personalização do FN dos usuários pelos algoritmos é também uma forma de intrusão. O agenciamento[18] de dados no *Facebook* pelos algoritmos torna os dados visíveis mesmo sem os usuários terem ciência disso (JURNO; D'ANDRÉA; 2017).

O próprio registro obrigatório dos usuários em uma plataforma de SRSO (SÁ, 2018) é uma intrusão uma vez que permite que empresas possam ter acesso a dados a partir do preenchimento de formulários.

Os recursos desenvolvidos pelas empresas e disponibilizados aos usuários para uso, entretenimento, para a interação e que tenham como objetivo o acesso a dados pelas empresas podem ser considerados como meios de intrusão.

5.4.2 Interferência decisória

São todas as ações ou atividades executadas pelo Estado e que interferem em assuntos privados dos usuários. Para Boff, Fortes e Freitas o Estado tem necessidade de obter dados dos indivíduos e isso seria uma forma do Estado estar presente na vida deles.

[18] Ver seção 4.10.

Além disso, o Estado pode utilizar o poder estrutural de que dispõe para exercer interferência na vida dos indivíduos (BOFF; FORTES; FREITAS, 2018).

Barriga menciona que os SRSO além de atenderem os interesses de empresas, servem também a instituições governamentais e ao Estado (BARRIGA, 2020). Portanto, saber que de alguma forma o Estado pode interferir em eleições para cargos públicos como as que aconteceram nos Estados Unidos e no Brasil é bem preocupante. Por isso, instituições que têm poder de fiscalizar as ações do Estado estão discutindo e tomando decisões para minimizar este tipo de interferência (FORNASIER; BECK, 2020).

5.5 Síntese da Discussão

Nesta subseção foi elaborado um Quadro Síntese (Quadro 17) contendo os principais achados na RSL sobre os potenciais riscos relacionados à privacidade. O Quadro Síntese está baseado nos Grupos e Subgrupos da Taxonomia da Privacidade de Rodrigues e Sant'Ana (2016). A primeira coluna representa os Grupos. A segunda coluna representa os Subgrupos e a terceira coluna os potenciais riscos identificados na RSL. Por fim, a quarta coluna representa os autores que discutem sobre os potenciais riscos relacionados à privacidade de dados.

Quadro 17 - Potenciais riscos à privacidade de dados em SRSO categorizados pela Taxonomia da Privacidade, ordenados pelo ano de publicação da literatura vinculada aos potenciais riscos, de forma crescente.

Taxonomia da Privacidade		**Potenciais Riscos segundo a literatura analisada**	**Literatura vinculada aos Potenciais Riscos**
Grupo	**Subgrupo**		
Coleta de Dados	Vigilância	Novo modelo de vigilância.	(ROSADO; TOMÉ, 2015)
		O acesso à internet e aos dispositivos móveis facilitam o acesso aos SRSO.	(ROSADO; TOMÉ, 2015)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
			(STRECK; PELLANDA, 2017)
			(LIMA, 2018)
			(BARRIGA, 2020)
		Os SRSO são comparados a panóptico. Uma vez que controlam e permitem controlar por meio de discursos, opiniões e dados.	(FUGAZZA; SALDANHA, 2018)
			(BARRIGA, 2020)
			(LEITZKE; RIGO, 2020)
		As TIC têm um papel relevante na coleta de dados e na vigilância, principalmente aos usuários que tiveram contato rápido com os SRSO. Essa percepção leva ao entendimento de que o uso de TIC por usuários mais jovens e portanto sem aparente preocupação com a vigilância sobre os dados é um problema geracional.	(ZAKIEE; HAGE; KUBLIKOWSKI, 2019)
			(MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020)
		Existência de produção de dados de forma instantânea.	(STRECK; PELLANDA, 2017)
		A vigilância não ocorre somente de empresa para usuário. Ela ocorre também de usuário para usuário. Além disso, o Estado detém também o controle sobre	(FUGAZZA; SALDANHA, 2018)
			(BARRIGA, 2020)

Taxonomia da Privacidade		Potenciais Riscos segundo a literatura analisada	Literatura vinculada aos Potenciais Riscos
Grupo	**Subgrupo**		
		os dados dos indivíduos.	
		Publicação de dados de forma deliberada.	(BARRIGA, 2020)
	Interrogatório	Condição obrigatória de informar dados por meio de preenchimento de formulários.	(LIMA, 2018)
			(SÁ, 2018)
Processamento da Informação	Agregação	A produção variada e diária de dados são armazenados em um banco de dados. Os dados armazenados podem sofrer o processo de agregação. O principal objetivo deste processo é obter informações sobre os usuários.	(JURNO; D'ANDRÉA, 2017)
			(STRECK; PELLANDA, 2017)
		Existem fontes geradoras de dados que podem ser utilizadas no processo de Agregação. São exemplos as curtidas, o uso de hashtags, o uso de códigos ou mesmo o FN.	(ROSADO; TOMÉ, 2015)
			(JURNO; D'ANDRÉA, 2017)
			(STRECK; PELLANDA, 2017)
		A agregação de dados pode ser realizada por meio de dispositivos móveis com os quais os usuários acessam os SRSO, identificando por exemplo quando e onde uma imagem foi publicada.	(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
		Dados tais como marcação de local são dados que agregados a uma imagem servem de estratégia para as empresas para extrair informações sobre o usuário.	(STRECK; PELLANDA, 2017)
	Identificação	Dados podem ser identificáveis por meio de imagens publicadas em um SRSO pelo próprio usuário. Outros dados como nome de paciente e idade expostos por profissionais de saúde são passíveis de identificação, como por exemplo em um exame de Raio X.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
		As empresas estão investindo em técnicas para identificação de dados como por exemplo o de reconhecimento facial.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
	Insegurança	Os SRSO são ambientes públicos. Isso implica na visibilidade de dados e em sua acessibilidade por qualquer indivíduo com registro em um SRSO.	(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
			(REBS, 2017)
		Há utilização de dados por terceiros de forma não autorizada.	(ASSUMPÇÃO; SANTANA; SANTOS, 2015)
			(REBS, 2017)

Taxonomia da Privacidade		Potenciais Riscos segundo a literatura analisada	Literatura vinculada aos Potenciais Riscos
Grupo	**Subgrupo**		
			(FUGAZZA; SALDANHA, 2018)
		As Políticas de Privacidade geram vulnerabilidade e causam insegurança.	(FUGAZZA; SALDANHA, 2018)
			(BORGES, 2020)
		A possibilidade de criar multiperfis ou utilizar perfis falsos é um fator que causa insegurança.	(SANTOS; PORTO; ALTURAS, 2010)
			(ROSADO; TOMÉ, 2015)
			(FUGAZZA; SALDANHA, 2018)
			(LIMA, 2018)
		Possibilidade de ocorrência de crimes: perseguição, obtenção de dados bancários ou sigilosos.	(SANTOS; PORTO; ALTURAS, 2010)
			(EVERTON, et al., 2014)
			(REBS, 2017)
			(FUGAZZA; SALDANHA, 2018)
	Uso Secundário	A formação de diários completos sobre um indivíduo como os que são produzidos no Instagram podem ser utilizados para fins diferentes da proposta inicial do SRSO, e isso gera uma falsa segurança aos usuários.	(ZAKIEE; HAGE; KUBLIKOWSKI, 2019).
		A personalização de perfis é uma estratégia de Marketing adotada pelas empresas. A ideia não é somente personalizar a página do usuário, mas identificar nela seus gostos e interesses.	(FUGAZZA; SALDANHA, 2018)
			(BORGES, 2020)
	Exclusão	Uso e compartilhamento de dados por terceiros sem a autorização formal. Este tipo de ação requer uma decisão sobre o que pode ou não ser feito com os dados. Mas quase sempre aqueles que deveriam tomar decisões participam do processo.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
		O recompartilhamento de publicações ou o compartilhamento em cadeia são ações que excluem o usuário de decisões sobre suas publicações e sobre seus dados.	(SANTOS; PORTO; ALTURAS, 2010)
			(AMARAL FILHO; BLANCO, 2014)
			(GONZATTI; BITTENCOURT; ESMITIZ, 2015)
			(BORGES, 2020)
		O armazenamento de dados de forma permanente pelas empresas não dá direito de escolha aos usuários de excluir definitivamente seus dados.	(STRECK; PELLANDA, 2017)
			(JURNO; D'ANDRÉA; 2017)
			(ASSUMPÇÃO; SANTANA; SANTOS,

Taxonomia da Privacidade		Potenciais Riscos segundo a literatura analisada	Literatura vinculada aos Potenciais Riscos
Grupo	**Subgrupo**		
			2015)
Disseminação da Informação	Quebra de confidencialidade	Cultura da transparência de dados.	(FUGAZZA; SALDANHA, 2018)
		Divulgação das performances de profissionais de saúde e de estética relacionada a uso e divulgação não autorizada de dados, por vezes até ferindo a ética profissional.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
		A autorização de acesso garante que os dados estejam visíveis apenas a um grupo restrito. Tudo o que fuja a isso é considerado Quebra de confidencialidade.	(SANTOS; PORTO; ALTURAS, 2010)
			(ASSUMPÇÃO; SANTANA; SANTOS, 2017)
	Divulgação	A divulgação de publicações especialmente feita por mulheres pode levar a ação dos stalkings, provocando constrangimento, restrição de liberdade, possibilidade de distorção de publicação por meio de montagens de imagens e alteração de textos.	(MENDES-CAMPOS; FÉRES-CARNEIRO; MAGALHÃES, 2020)
	Exposição	Há uma facilidade para a exposição de dados em SRSO.	(ZAKIEE; HAGE; KUBLIKOWSKI, 2019)
		Dados sigilosos, protegidos por código de ética na área da saúde são utilizados para promoção das atividades profissionais, levando a uma exposição de dados dos pacientes. O agravante é que alguns profissionais não solicitam autorização formal dos pacientes.	(MARTORELL; NASCIMENTO; GARRAFA, 2016)
			(PURIM ; TIZZOT, 2019)
		A exposição de dados financeiros e outros dados sigilosos divulgados em SRSO trazem preocupações aos usuários. Os dados quando não protegidos adequadamente podem ser rastreados e utilizados por indivíduos mal intencionados.	(EVERTON, et al., 2014)
		A exposição de características físicas de usuários são alvos de perseguição e do discurso do ódio.	(REBS, 2017).
	Ampliação de acesso	Ausência de preocupação dos usuários com o que é feito com os dados.	(SÁ, 2018)
		O que está descrito nos Termos de Uso para os usuários sobre como os dados são utilizados ainda é muito limitado.	(FUGAZZA; SALDANHA, 2018)
		Dados dos usuários são propriedade de empresas. Isto é algo descrito nos Termos de Uso e dá o direito às empresas inclusive para compartilhar dados com terceiros.	(FUGAZZA; SALDANHA, 2018)
			(BORGES, 2020)

Taxonomia da Privacidade		Potenciais Riscos segundo a literatura analisada	Literatura vinculada aos Potenciais Riscos
Grupo	**Subgrupo**		
		A ampliação de acesso a dados pode ser estendida ao Estado e a grupos terroristas.	(BARRIGA, 2020)
	Chantagem	O anonimato de usuários é um recurso permitido pelos SRSO que pode contribuir com a chantagem.	(REBS, 2018)
		Existem ameaças direcionadas a grupos de usuários tais como afrodescentes.	(REBS, 2018)
		A possibilidade de criação de perfis falsos dá condições ao anonimato.	(SANTOS; PORTO; ALTURAS, 2010)
		Estabelecimento de relação de confiança com a intenção de tirar vantagem ou extorquir os usuários.	(SANTOS; PORTO; ALTURAS, 2010)
	Apropriação	O uso de imagens de pacientes por profissionais de saúde que atuam na área da estética é um exemplo de apropriação uma vez que eles tem a pretensão de se autopromover e assim alcançar mais clientes.	(PURIM; TIZZOT; 2019)
		Existência de uma dicotomia. A divulgação de dados é algo recorrente em SRSO mas ao mesmo tempo aquilo que é divulgado por ser utilizado por empresas para marketing ou por outros usuários, com a intenção de gerar benefícios. A apropriação de dados é ainda pouco conhecida pelos usuários.	(BARRIGA, 2020)
		Obtenção de lucro pelas empresas a partir da apropriação de dados dos usuários. Isso seria uma forma de opressão. Os dados dos usuários estariam gerando lucro apenas as empresas e não a eles, em tese proprietários dos dados.	(FUGAZZA; SALDANHA, 2018)
	Distorção	Alguns dos recursos oferecidos aos usuários pelos SRSO tais como filtros podem alterar uma imagem, omitindo certos dados e fazendo com que os usuários que acessam a publicação vejam apenas uma parte de todo o contexto. Isso pode levar a distorção que é o ato de modificar, de alterar algo, de maneira que possa confundir os usuários.	(STRECK; PELLANDA, 2017)
Invasão	Intrusão	Os recursos ofertados pelas empresas aos usuários tais como os story, chats, salas de bate-papo seriam utilizados como meio para captar dados. O uso de tais recursos é justificado pelas empresas para melhorar os SRSO para os usuários.	(STRECK; PELLANDA, 2017) (PURIM; TIZZOT, 2019) (BARRIGA, 2020)
		Uma outra forma de intrusão conhecida nos SRSO é a personalização do FN. Este recurso é também um meio de acesso a dados dos usuários pelas empresas.	(JURNO; D'ANDRÉA; 2017)

Taxonomia da Privacidade		Potenciais Riscos segundo a literatura analisada	Literatura vinculada aos Potenciais Riscos
Grupo	**Subgrupo**		
		O preenchimento de formulário pelos usuários para terem acesso aos SRSO é uma forma de intrusão, e ainda mais por ser uma condição obrigatória.	(SÁ, 2018)
	Interferência Decisional	Os SRSO atendem aos interesses de empresas, mas servem também aos interesses do Estado, sendo portanto uma fonte utilizada pelo Estado com a intenção de interferir no poder de decisão dos usuários sobre qualquer assunto, principalmente os relacionados à área política.	(BARRIGA, 2020)

Fonte: Autora (2022).

A percepção sobre o Quadro 17 foi que os autores que mais discutem aspectos relacionados aos potenciais riscos para a privacidade de dados em SRSO foram: Santos, Porto e Alturas (2010), Rosado e Tomé (2015), Martorell, Nascimento e Garrafa (2016), Assumpção, Santana e Santos (2015), Streck e Pellanda (2017), Fugazza e Saldanha, (2018), Barriga (2020), Borges (2020).

No grupo I, de Coleta de Dados os principais autores foram Barriga (2020) identificado em (4) aspectos relacionados aos potenciais riscos, Streck e Pellanda (2017) com destaque em (2) aspectos, Fugazza e Saldanha (2018) identificado também em (2) aspectos, assim como Rosado e Tomé (2015) identificado também em (2) aspectos. A maioria dos autores foram mencionados no subgrupo da “Vigilância”. Apenas Lima (2018) e Sá (2018) foram mencionados no subgrupo de “Interrogatório", cada um identificado em (1) aspecto cada.

No grupo II, de Processamento da Informação os principais autores foram: Assumpção, Santana e Santos (2015) e Fugazza e Saldanha (2018), identificados em (5) aspectos relacionados aos potenciais riscos dentre os seis subgrupos existentes. Já Streck e Pellanda (2017) foi identificado em (4) aspectos, seguido de Martorell, Nascimento e Garrafa (2016) com (3) aspectos, Jurno e D’Andréa (2017) com (3) e Borges (2020) também com (3) aspectos.

Dentre estes os que mais se destacaram em relação aos aspectos sobre os potenciais riscos para a privacidade de dados relacionados ao subgrupo “Agregação” foram Streck e Pellanda (2017) e Jurno e D’Andréa (2017). Ao subgrupo “Identificação” o autor com de maior destaque foi Martorell, Nascimento e Garrafa (2016), e no subgrupo “Insegurança” foram Fugazza e Saldanha (2018), Assumpção, Santana e Santos (2015) e Santos, Porto e Alturas (2010). Nos subgrupos de “Uso Secundário” e de “Exclusão” houve variação de autores discutindo o tema, não havendo portanto qualquer destaque.

No grupo III, de Disseminação da Informação os autores com maior destaque quanto aos aspectos relacionados aos potenciais riscos identificados foram Fugazza e Saldanha (2018) com (4) aspectos, seguido por Santos, Porto e Alturas (2010) e Rebs (2018) com (3) aspectos cada, Streck e Pellanda (2017) e Barriga (2020) com (2) aspectos cada.

Houve uma diversidade de autores discutindo aspectos relacionados aos potenciais riscos sobre a privacidade de dados nos subgrupos “Quebra de Confidencialidade”, “Divulgação”, "Exposição" e "Distorção", não sendo portanto possível destacar qualquer

um. Destacou-se no subgrupo “Chantagem” Santos, Porto e Alturas (2010) e Rebs (2018). No subgrupo “Ampliação de Acesso” o autor em destaque foi Fugazza e Saldanha (2018).

No grupo IV, Invasão o autor em destaque foi Barriga (2020), não sendo possível destacar demais autores em assuntos relacionados aos subgrupos “Intrusão” e “Interferência Decisional”.

6 CONCLUSÃO

Diante de tudo que foi abordado e da estrutura metodológica desenvolvida foi possível atender aos objetivos desta investigação. Primeiro que a partir da RSL foram identificados nas comunicações científicas a temática de privacidade de dados associada ao acesso e uso de SRSO no Brasil.

Quanto aos aspectos teóricos tratados nas vinte comunicações científicas revisadas, verificou-se que os autores abordaram questões sobre a Privacidade e ao Uso de SRSO relacionadas à Ética, à Saúde, ao Direito trazendo o Marco Civil da Internet, as TIC, a Proteção de dados, a Vigilância, a Exposição, a Política de Privacidade e os Termos de Uso e das condições disponíveis aos usuários para proteção dos dados, a Confidencialidade de Dados, as funções dos algoritmos, dentre tantos outros aspectos que contribuíram para o entendimento de uma tema tão complexo.

Posteriormente, os potenciais riscos sobre a privacidade em SRSO foram elencados e relacionados com a Taxonomia da Privacidade (RODRIGUES; SANT'ANA, 2016). Dentre os subgrupos com maior destaque em relação ao tema proposto destacam-se, em ordem, a "Vigilância", a "Agregação", a "Insegurança", a "Exclusão", a "Exposição", a "Ampliação de Acesso", a "Chantagem", a "Apropriação" e a "Intrusão". Os subgrupos com menor atenção foram o "Interrogatório", a "Identificação", o "Uso Secundário", a "Divulgação", a "Distorção" e a "Interferência Decisional".

Ao investigar o tema de Privacidade e de SRSO foi possível compreender que as TIC tem um papel fundamental em relação à promoção da visibilidade de dados. Os dispositivos móveis foram apontados por alguns autores como uma das formas que interfere na questão de acesso rápido e prolongado em SRSO, o que impacta no aumento da quantidade de publicações e por conseguinte de dados diariamente divulgados.

Para as empresas, talvez isso seja bem mais interessante do que desenvolver melhorias na Política de Privacidade ou na transparência do que é feito com os dados dos usuários. Afinal, as empresas de SRSO sobrevivem de dados, da exposição e de tudo aquilo que os usuários publicam, seja por meio de imagens, textos, vídeos ou qualquer outro tipo de fonte de geração de dados.

Se por um lado, existem usuários que publicam dados de forma espontânea, existem outros que são incentivados por meio da oferta de recursos disponíveis até mesmo para aqueles que relutam em utilizar um SRSO. Embora exista também outros grupos de usuários que mesmo não sendo registrados em um SRSO podem ter sua imagem ou dados

divulgados por terceiros, como é o caso de crianças e adolescentes ou e atrelados ao serviço de marketing, como é o caso de pacientes de profissionais de estética. De maneira geral, percebe-se que sendo de forma espontânea ou não o acesso e a exposição de dados em um SRSO sem cuidados mínimos com a privacidade tais como a restrição de acesso de publicações apenas aos mais íntimos pode afetar a privacidade de dados de todos de maneira igual.

Observou-se ainda dentre os aspectos discutidos pelos autores que os SRSO são uma tendência na formação de uma sociedade passível de controle. Durante a RSL percebeu-se alguns indícios de que os usuários são controlados por empresas e até mesmo por outros usuários. Não são apenas os dados que estão sendo vigiados e controlados, mas existe também a percepção de que há movimentos de grupos que desejam que os SRSO sejam povoados por indivíduos com as mesmas ideologias ou com as mesmas perspectivas políticas e religiosas, ou ainda por padrões de beleza que eles julgam ser a ideal. Este tipo de controle exercido pelos indivíduos em SRSO tem amparo na utilização de multiperfis ou de perfis falsos.

Além disso, alguns autores evidenciaram que os SRSO são ambientes públicos ou que podem ser também híbridos e isso de certa forma facilita a vigilância. Este é também um fator que leva os usuários e as empresas a terem acesso a dados e a exercer algum tipo de controle sobre o que os usuários desejam ver, como os anúncios ou até mesmo aquilo que pode não ser de seu interesse.

Dentro de tudo que foi abordado na RSL percebeu-se que na literatura brasileira existem características em comum de autores sobre os SRSO e a privacidade de dados. A primeira aponta para a contribuição de acesso à internet e aos dispositivos móveis como os mais relevantes fatores relacionados à rapidez de acesso e o tempo de permanência dos usuários em um SRSO. Isso eleva os riscos da vigilância, da coleta de dados e do uso para fins estranhos ao conhecimento do usuário.

A segunda característica se refere ao compartilhamento ou recompartilhamento de publicações. Isso é uma ação comum em SRSO mas que na visão dos autores exclui os usuários de decisões sobre seus dados. Esse poder de decisão e de controle sobre as publicações e dados passa a ser do usuário que compartilha e não mais do usuário origem, ou seja de onde a publicação foi publicada originalmente. Cabe destacar que isso seja um dos maiores potenciais riscos para a privacidade, uma vez que causa o compartilhamento em cadeia, como um dos autores mencionaram e de forma descontrolada.

A terceira característica está atrelada à ideia de que os SRSO podem ser equiparados a um panóptico, ou seja, um mecanismo capaz de controlar os usuários enquanto eles publicam e interagem. Diferentemente de outras formas de controle, os SRSO representam aos mais despreocupados usuários uma ameaça silenciosa e invisível, repleta de atrativos.

A quarta característica observada em SRSO está relacionada ao armazenamento de dados dos usuários de forma permanente. Isso tira o poder do usuário de decidir pela exclusão definitiva dos dados.

Por fim, alguns autores indicam que os recursos disponibilizados aos usuários tais como story, mensagens instantâneas e vídeos curtos, seriam maneiras de captar dados. As empresas precisam manter os usuários logados assim investem cada vez mais em recursos de entretenimento e para a interação com a intenção de atrair os usuários.

O tema investigado tem muito ainda a ser explorado, especialmente na área da CI, visto que ainda são poucas as comunicações científicas na área relacionada aos SRSO e a privacidade. Sendo assim existem alguns aspectos que podem ser explorados em futuras investigações tais como:

1. Investigar as principais fontes produtoras de dados no contexto de SRSO. Isso talvez leve a entender melhor como as empresas realizam a coleta de dados e a partir de quais fontes realizam esta atividade. Na pesquisa percebeu-se que o FN é um exemplo de fontes de dados, mas possivelmente existem outras fontes a serem identificadas, analisadas e categorizadas.
2. Destaca-se ainda a existência de uma possível sociedade de controle que estaria sendo formada por meio do processo de vigilância. Seria de fato os SRSO um novo paranóptico, que tipo de controle as empresas exercem sobre os usuários, além da utilização dos dados? E que tipo de controle também estaria acontecendo de usuário para usuário? Qual o papel dos algoritmos?
3. Outro aspecto que pode ser investigado é a valoração da privacidade para os usuários. Será que é possível medir o valor da privacidade aos indivíduos. Será que a privacidade tem menos valor para os usuários que praticamente tiveram contato mais rápido com a internet e com os SRSO, do que aqueles que não tem registro em um SRSO ou que pouco acessam?

4. Investigar os tipos de perfis (Profiling) de usuários e as técnicas aplicadas em SRSO na identificação dos gostos e interesses dos usuários a partir dos dados publicados seja um tema interessante a ser investigado.
5. Por fim, cabe ainda verificar nas comunicações científicas estrangeiras a visão dos autores sobre os SRSO e os potenciais riscos para a privacidade dos dados e para a proteção dos usuários, na intenção de saber as divergências ou convergências em relação ao tema e ao que foi identificado nas comunicações científicas brasileira.

Observa-se na pequena amostra da literatura brasileira que os autores convergem em alguns pontos em relação à privacidade como foi mencionado anteriormente. Primeiro que os usuários precisam utilizar os SRSO de forma cuidadosa, uma vez que seu uso descontrolado e sem os cuidados básicos com a privacidade pode oferecer riscos como acesso a dados sigilosos, julgamentos, constrangimento, perseguição, descontextualização das publicações, além de exposição de grupos protegidos pela legislação brasileira como no caso de crianças. Além disso, verifica-se que os profissionais de saúde têm utilizado bem mais os SRSO na intenção de se autopromover, o que afeta de forma direta os pacientes e viola o que rege o código de ética da profissão sobre a exposição indevida e sem autorização prévia.

A privacidade está longe ainda de ser dimensionada, mas foi possível entender a partir da investigação sobre o tema que muito do que acontece com os dados está relacionado a um uso inconsciente, irreflexivo dos usuários, sendo portanto parte responsável pelos potenciais riscos ocorridos.

Por fim, o tema investigado tem algumas limitações, dentre elas cita-se a amostra delimitada apenas as comunicações científicas em língua portuguesa, o que pode ser ampliado em outras investigações. Além disso, apesar do quantitativo de comunicações científicas recuperadas nas três bases ser elevado, muitas não eram aderentes ao tema, o que limitou ainda mais a exploração do tema. Assim, recomenda-se em futuras investigações verificar bases de conhecimento mais específicas, tais como as voltadas para as TIC.

REFERÊNCIAS

AFFONSO, Elaine Parra ; SANT'ANA, Ricardo César Gonçalves. **Privacy awareness issues in user data collection by digital libraries.** 2018. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/0340035218777275?casa_token=b10zRYu0rlEAAAAA%3ADu9qAt-ahsgTjlwNCA67sjDsIVaXs8ARocm9GLUKhtAnkzafqHLmCwioOrwZJ8V4cq71ScblzZGIoSA&journalCode=iflb. Acesso em: 4 jun. 2022.

AMARAL FILHO, Otacílio Amaral; BLANCO, Danielle Dos Reis. O Espetáculo Cultural na rede social: A abordagem midiática do Coletivo Dirigível de teatro na Rede Social Digital Facebook. **Sessões do Imaginário**, v. 19, n. 31, p. 29–38, 2014. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/14910. Acesso em: 2 fev. 2022.

ASSUMPÇÃO, Fabrício Silva; SANTANA, Ricardo Cesar Gonçalves; SANTOS, Plácida Leopoldina V. A. da Costa. Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais. **Em Questão**, v. 21, n. 2, p. 31–48, 2015. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/54545. Acesso em: 2 fev. 2022.

AUXIER *et al*. **Americans and Privacy:** Concerned, Confused and Feeling Lack of Control Over Their Personal Information. 2019. Disponível em: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Acesso em: 7 mar. 2022.

BARNES, S. B. A privacy paradox: Social networking in the United States. **First Monday**, v.11, n. 9, September, 2006. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312. Acesso em: 19 maio 2020.

BARRIGA, Antónia do Carmo. A publicitação do privado na era da pós-verdade: uma exploração às redes sociais dos líderes políticos portugueses. **Observatorio (OBS*)**, v. 14, n. 2, 2020. Disponível em: http://obs.obercom.pt/index.php/obs/article/view/1609. Acesso em: 2 fev. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges; Freitas, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro, Lumen Juris, 2018.

BORGES, Mariana Toledo. Mercado, vigilância e Facebook na era do espetacular integrado, ou inside us all there is a code. **Literatura: Teoría, Historia, Crítica**, v. 22, n. 1, p. 137-178, 2020. Disponível em: https://www.redalyc.org/journal/5037/503763261005/html/. Acesso em: 2 fev. 2022.

BOYD, D. M; ELLISON, N. B. Social Network Sites: Definition, History, and Scholarship. **Journal of Computer-Mediated Communication**, v. 13, n. 1, p. 210-230, 2007. Disponível em: https://academic.oup.com/jcmc/article/13/1/210/4583062. Acesso em: 1 jun. 2020.

BRANCO, Paulo; BARBAS, Maria. **Interação Humano-Computador e Redes Sociais Online**: potencialidades e tendências. [S.l : S.n], 2012. Disponível em:

https://www.academia.edu/22682668/Intera%C3%A7%C3%A3o_Humano-Computador_e_Redes_Sociais_Online. Acesso em: 3 set. 2021. 1 PDF.

BRAPCI - Base de Dados em Ciência da Informação. Disponível em: https://www.brapci.inf.br/. Acesso em: 14 out. 2021.

BRASIL, Ministério da Defesa. **Lei Geral de Proteção de Dados Pessoais (LGPD).** 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 14 jul. 2021.

BRASIL, Presidência da República. **Lei nº 14.132, de 31 de março de 2021.** 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14132.htm. Acesso em: 29 de abr. de 2022.

BUSCA básica: EBSCOhost. Disponível em: https://web-b-ebscohost.ez3.periodicos.capes.gov.br/ehost/search/basic?vid=0&sid=dfc41470-add5-4bb1-8e21-a3c8d30d6f41%40sessionmgr102. Acesso em: 14 out. 2021.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 1999. Disponível em:https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 28 set. 2021.

CASTELLS, M. **A Sociedade em rede**. 19. ed. Rio de Janeiro: Paz & Terra, 2018.

CONFORTO, Edivandro Carlos ; AMARAL, Daniel Capaldo; SILVA, Sérgio Luis da. **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.

CONHEÇA a Meta. Disponível em: https://about.facebook.com/br/meta/. Acesso em: 25 fev. 2022.

CHEN, Deyan; ZHAO, Hong. Data Security and Privacy Protection Issues in Cloud Computing. *In*: **2012 International Conference on Computer Science and Electronics Engineering**. [s.l.: s.n.], 2012, v. 1, p. 647–651. Disponível em: https://ieeexplore.ieee.org/document/8465318. Acesso em: 28 set. 2021.

DONEDA, Danilo. Reflexões sobre proteção de dados pessoais em redes sociais. **Revista Internacional de Protección de Datos Personales**, 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.

EBSCOhost. Disponível em: https://web-b-ebscohost.ez3.periodicos.capes.gov.br/ehost/search/basic?vid=0&sid=dfc41470-add5-4bb1-8e21-a3c8d30d6f41%40sessionmgr102. Acesso em: 14 out. 2021.

EVERTON, Roberto; COMIN; TEIXEIRA, Rafael; *et al*. Investigando o fenômeno de compras coletivas on-line: fatores que influenciam a intensidade das compras. **Rev. Adm.** v. 7, p. 196-213, 2014. Disponível em: https://www.researchgate.net/publication/268509490_Investigando_o_fenomeno_de_compras_coletivas_on-line_fatores_que_influenciam_a_intensidade_das_compras. Acesso em: 2 fev. 2022.

FELT, Adrienne; EVANS, David. Privacy protection for social networking platforms. *In*: Oakland, CA: [s.n.], 2008. Disponível em: https://www.researchgate.net/publication/228629208_Privacy_protection_for_social_networking_platforms. Acesso em: 2 mar. 2022.

FONTELES, Débora Matni; RODRIGUES, Fernando de Assis. A privacidade em ambientes de Redes Sociais On-line: *In:* **Fórum de Estudos em Informação, Sociedade e Ciência**, v. 3, p. 68–70, 2020. Disponível em: //https:https://www.ufrgs.br/feisc/index.php/feisc/article/view/41/41. Acesso em: 06 jan. 2022.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge analytica: escândalo, legado e possíveis futuros para a Democracia. **Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí**. 2020, jan. / jun, v. 29, n. 53,p. 182–95. Disponível em: : https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033/6360. Acesso em: 23 maio 2020.

FUGAZZA, Grace Quaresma; SALDANHA, Gustavo Silva. A questão do direito à privacidade no Facebook: um estudo à luz da ética da informação. **Informação & Informação**, 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.

FUNG, B. C. M.; WANG, K.; FU, A. W.; *et al*. **Introduction to Privacy-Preserving Data Publishing:** concepts and Techniques. [s.l.]: CRC Press, 2010. Disponível em: https://books.google.com.br/books?id=fUopcSpQuNMC&lpg=PP1&dq=Introduction%20to%20Privacy-Preserving%20Data%20Publishing%3A%20Concepts%20and%20Techniques&lr&hl=pt-BR&pg=PP1#v=onepage&q&f=false. Acesso em: 6 jul. 2020. EBOOK.

Google Workspace: Apps empresariais e ferramentas de colaboração. Disponível em: https://workspace.google.com/intl/pt-BR/. Acesso em: 7 jun. 2022.

GONZATTI, Christian; BITTENCOURT, Maria Clara Aquino; ESMITIZ, Francielle. 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 Ano 20 n. 34. 2015**, 2015. Disponível em: https://www.academia.edu/22611068/De_Rainha_dos_Baixinhos_a_Rainha_dos_Memes_o_humor_como_vetor_de_ciberacontecimentos_a_partir_da_ida_de_Xuxa_da_Rede_Glob

o_para_a_Rede_Record_From_Queen_of_the_Shorties_to_Queen_of_Memes_humor_as_cyberevents_vector_when_Xuxa_goes_from_Rede_Globo_to_Rede_Record. Acesso em: 2 fev. 2022.

GROSS, R.; ACQUISTI, A. Information revelation and privacy in online social networks. *In*: **Proceedings of the 2005 ACM workshop on Privacy in the electronic society**. Alexandria, VA, USA: Association for Computing Machinery, 2005, p. 71-80. (WPES '05). Disponível em: //https://dl.acm.org/doi/10.1145/1102199.1102214. Acesso em: 18 jul. 2020.

HAGE, Zakiee Castro Mufarrej; KUBLIKOWSKI, Ida. Estilos de uso e significados dos autorretratos no Instagram: Identidades narrativas de adultos jovens brasileiros. **Estudos e Pesquisas em Psicologia**, v. 19, n. 2, p. 522–539, 2019. Disponível em: https://www.e-publicacoes.uerj.br/index.php/revispsi/article/view/44285. Acesso em: 2/2/2022.

JURNO, Amanda Chevtchouk; D'ANDRÉA, Carlos Frederico de Brito. (In)visibilidade algorítmica no "feed de notícias" do Facebook. **Contemporanea | Revista de Comunicação e Cultura**, v. 15, n. 2, p. 463-484, 2017. Disponível em: https://periodicos.ufba.br/index.php/contemporaneaposcom/article/view/17796. Acesso em: 13 fev.. 2022.

KAUFMAN, Dora; SANTAELLA, Lucia. O papel dos algoritmos de inteligência artificial nas redes sociais. **Revista FAMECOS**, v. 27, p. 1-10, 2020. Disponível em: https://revistaseletronicas.pucrs.br/index.php/revistafamecos/article/view/34074. Acesso em: 14 out. 2021.

KEMP, Simon. **Relatório digital 2020**. Disponível em: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media. Acesso em: 15 jul. 2021.

KOKOLAKIS, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. **Computers & Security**, v. 64, p. 122-134, 2017. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404815001017. Acesso em: 12 maio 2020.

LEITZKE, Angélica Teixeira da Silva ; RIGO, Luiz Carlos. 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.

LÉVY, Pierre. **As tecnologias da inteligência:** o futuro do pensamento na Era da Informática. Tradução de Carlos Irineu da Costa. Rio de Janeiro: Editora 34, 1993. Disponível em: https://lucianabicalho.files.wordpress.com/2014/02/as-tecnologias-da-inteligencia.pdf. Acesso em: 13 out. de 2021.

LEVY, Yair; ELLIS, J. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. **Informing Science Journal,** v. 9, 2006.

Disponível em: http://www.inform.nu/Articles/Vol9/V9p181-212Levy99.pdf. Acesso em: 10 de ago. 2021.

LIMA, Luciano de Almeida. 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,** v. 17, n. 1, p. 59–81, 2018. Disponível em: https://periodicos.uninove.br/prisma/article/view/8084. Acesso em: 2/2/2022.

MARTORELL, Leandro Brambilla; NASCIMENTO, Wanderson Flor do; GARRAFA, Volnei. Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no facebook. **Interface - Comunicação, Saúde, Educação**, 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, Carolina; FÉRES-CARNEIRO, Terezinha; MAGALHÃES, Andrea S. Extimidade virtual e conjugalidade: possíveis repercussões. **Psicologia: teoria e prática**, v. 22, n. 1, p. 285–299, 2020. Disponível em: http://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1516-36872020000100010&lng=pt&nrm=iso&tlng=pt. Acesso em: 17 de fev. 2021.

MISLOVE, A. *et al*. Measurement and Analysis of Online Social Networks. *In:* **IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, 7**. San Diego, California: Association for Computing Machinery. New York ,NY, United States, 2007, p. 29-42. Disponível em: https://dl.acm.org/doi/pdf/10.1145/1298306.1298311. Acesso em: 13 maio 2020. DOI 10.1145/1298306.1298311.

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

O QUE é o Open Access? Disponível em: https://openaccess.sdum.uminho.pt/?page_id=276https://openaccess.sdum.uminho.pt/?page_id=276. Acesso em: 23 ago. 2021.

O QUE é Cloud Computing? Entenda a sua definição e importância. Blog da Salesforce. Disponível em: https://www.salesforce.com/br/blog/2016/02/o-que-e-cloud-computing.html. Acesso em: 6 set. 2021.

O USO da internet por adolescentes. Brasília: UNICEF, 2013. Disponível em: http://www.crianca.mppr.mp.br/arquivos/File/publi/unicef/br_uso_internet_adolescentes.pdf. Acesso em: 3 de jul. 2020.

PARISIER, Eli. **O filtro invisível: o que a internet está escondendo de você.** São Paulo: Zahar, 2012. E-book.

PLATAFORMA Sucupira. Disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsf. Acesso em: 15 out. 2021.

PINHEIRO, Lena Vania Ribeiro; FERREZ, Helena Dodd. Tesauro Brasileiro de Ciência da Informação. 2014. Disponível em: http://sitehistorico.ibict.br/publicacoes-e-institucionais/tesauro-brasileiro-de-ciencia-da-informacao-1/copy_of_TESAUROCOMPLETOFINALCOMCAPA24102014.pdf. Acesso em: 3 de jul. 2020.

PRÍNCIPE, E. *In:* Comunicação científica e redes sociais. **Fronteiras da Ciência da Informação**. [S.l.]: IBICT, 2013. p. 196-216. Disponível em: https://ridi.ibict.br/bitstream/123456789/492/1/Fronteiras%20da%20Ci%c3%aancia%20da%20Informa%c3%a7%c3%a3o.pdf Acesso em: 13 maio 2021.

PURIM, Kátia Sheylla Malta; TIZZOT, Edison Luiz Almeida. Protagonismo dos Estudantes de Medicina no Uso do Facebook na Graduação. **Revista Brasileira de Educação Médica**, 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.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Sulina, 2020.

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

RODRIGUES, Fernando de Assis; SANT'ANA, Ricardo César Gonçalves. Use of taxonomy of privacy to identify activities found in social networks' terms of use. **Knowledge Organization**, v. 43, n. 4, p. 285–295, 2016. Disponível em: https://www.nomos-elibrary.de/10.5771/0943-7444-2016-4-285/use-of-taxonomy-of-privacy-to-identify-activities-found-in-social-networks-terms-of-use-jahrgang-43-2016-heft-4. Acesso em: 10 de ago. 2021.

RODRIGUES, F. A. **Coleta de dados em redes sociais:** privacidade de dados pessoais no acesso via Application Programming Interface. 2017. TESE (Doutorado em Ciência da Informação) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista (UNESP). Disponível em: https://repositorio.unesp.br/handle/11449/149768. Acesso em: 7 jun. 2020.

ROSADO, Luiz Alexandre da Silva; TOMÉ, Vitor Manuel Nabais. As redes sociais na internet e suas apropriações por jovens brasileiros e portugueses em idade escolar. **Revista Brasileira de Estudos Pedagógicos**, v. 96, p. 11–25, 2015. Disponível em: http://www.scielo.br/j/rbeped/a/Sptq7rTsYB9QyqYXyzTjVts/abstract/?lang=pt. Acesso em: 11 jan. 2021.

ROZA, R. H. Ciência da informação, tecnologia e sociedade. **BIBLOS**, v. 32, n. 2, p. 177-190, 2018. Disponível em: https://periodicos.furg.br/biblos/article/view/7546/5861. Acesso em: 6 jul. 2021.

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

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

SARACEVIC, Tefko. A natureza interdisciplinar da ciência da informação. **Ciência da Informação**, v. 24, n. 1, p. 36-41, 1995. Disponível em: https://www.brapci.inf.br/_repositorio/2017/07/pdf_7810a51cca_0000015436.pdf. Acesso em 10 de ago. 2021.

SciELO.org. Disponível em: <https://www.scielo.org/>. Acesso em: 14 out. 2021.

SIMON, Paul. Do Pós-industrialismo à pós-modernidade. *In:* LYON, David. **Pós-modernidade.** São Paulo: Paulus: c1998, p. 59-83.

SOLOVE, Daniel J. Introduction: Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, v. 126, p. 1880, 2012. Disponível em https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2093&context=faculty_publications.. Acesso em 11 de out. 2021.

SOLOVE, Daniel J. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press, 2008. E-book.

STRECK, Melissa; PELLANDA, Eduardo Campos. Instagram como interface da comunicação móvel e ubíqua. **Sessões do Imaginário**, v. 22, n. 37, p. 10–19, 2017. Disponível em https://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/28017 . Acesso em: 10 fev. 2022.

TESAURO de la UNESCO. Disponível em: http://vocabularies.unesco.org/browser/thesaurus/en/?clang=es. Acesso em: 20 out. 2021.

THESA: tesauro Semântico Ciência da Informação - #Mídias sociais. Disponível em: https://www.ufrgs.br/tesauros/index.php/thesa/c/19126/64. Acesso em: 20 out. 2021.

THIBES, Mariana Zanata. As formas de manifestação da privacidade nos três espíritos do capitalismo: da intimidade burguesa ao exibicionismo de si nas redes sociais. **Sociologias**, v. 19, n. 46, p. 316–343, 2017. Disponível em https://www.scielo.br/j/soc/a/xsDnXCNzvBzXTzP3KL7xYQg/?format=pdf&lang=pt. Acesso em: 11 jan. 2021.

VALENTE, Jonas. Brasil tem 134 milhões de usuários de internet.... 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa. Acesso em: 10 ago. 2021.

ZOTERO: your personal research assistant. Disponível em: https://www.zotero.org/. Acesso em: 15 out. 2021.

APÊNDICE A - TOTAL DE OCORRÊNCIAS DE COMUNICAÇÕES CIENTÍFICAS, SEGMENTADAS POR BASE DE CONHECIMENTO, INCLUINDO COMUNICAÇÕES CIENTÍFICAS DESCARTADAS NA ANÁLISE, EM VALORES ABSOLUTOS

Tabela 3 - Total de ocorrências de comunicações científicas, segmentadas por base de conhecimento, incluindo comunicações científicas descartadas na análise, em valores absolutos (n >= 2).

#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências	#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
1	Instagram como interface da comunicação móvel e ubíqua	0	0	5	**5**	27	Deliberação no youtube? debates em torno da questão lgbt	0	0	2	**2**
2	Análise de sentimento de participantes de redes sociais online: o twitter e o ufc 202 (ultimate fighting championship)	0	0	4	**4**	28	Escrita, memória e cuidado - testemunhos de trabalhadores de saúde na pandemia	0	1	1	**2**
3	Coleta de dados a partir de imagens: considerações sobre a privacidade dos usuários em redes sociais	4	0	0	**4**	29	Facebook como espaço de preservação da memória local: uma análise por meio da social media analytics	1	0	1	**2**
4	Análise de redes sociais pode aproximar governo e cidadão?	0	0	3	**3**	30	Here we go again: the reemergence of anti-vaccine activism on the internet	0	2	0	**2**
5	Apresentação[1]	0	0	3	**3**	31	Indicadores altmétricos em periódicos brasileiros da ciência da informação	2	0	0	**2**
6	Como gestores planejam seu comportamento nas redes sociais online	0	0	3	**3**	32	Informação sobre diabetes nos blogs: aplicabilidade do modelo de análise do discurso noticioso em saúde	0	2	0	**2**
7	Contribuição para o desenho e proposta de laboratório de pesquisa e ensino a partir da análise de ischools de referência	0	0	3	**3**	33	Inovações na atenção primária em saúde: o uso de ferramentas de tecnologia de comunicação e informação para apoio à gestão local	0	2	0	**2**
8	Nativos digitais: a influência das novas tecnologias no desenvolvimento moral infanto-juvenil	0	0	3	**3**	34	Internação mediada: as novas configurações da internação hospitalar na era das mídias sociais	0	2	0	**2**

#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências	#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
9	Popularidade e visibilidade em redes sociais online: negociação de capitais sociais em meio digital para ampliação de audiência	0	0	3	**3**	35	Mensuração da competitividade em instituições de ensino superior privadas com base nas redes sociais digitais	2	0	0	**2**
10	Protagonismo dos estudantes de medicina no uso do facebook na graduação	0	3	0	**3**	36	O (en)canto e o silêncio das sereias: sobre o (não)lugar da criança na (ciber)cultura	0	0	2	**2**
11	“Mas não tive coragem de contar”: a revelação da condição sorológica na experiência amorosa de pessoas que vivem com hiv	0	2	0	**2**	37	O papel dos sites de redes sociais nas estratégias comunicativas de organizações da sociedade civil de salvador-bahia-brasil	0	1	1	**2**
12	A memória social registrada no facebook	2	0	0	**2**	38	O twitter como estratégia mediática para a chegada de novos partidos à assembleia da república portuguesa	0	0	2	**2**
13	A publicitação do privado na era da pós-verdade: uma exploração às redes sociais dos líderes políticos portugueses	0	1	1	**2**	39	O uso do aplicativo whatsapp nas práticas de gestão do conhecimento: o caso de uma comunidade virtual informal de profissionais na área de tecnologia	2	0	0	**2**
14	A rede social acadêmica researchgate como mecanismo de visibilidade e internacionalização da produção científica brasileira e portuguesa na área de biblioteconomia e ciência da informação	1	1	0	**2**	40	O uso do twitter como minerador de eventos adversos de medicamentos de combate à malária: o caso da doxiciclina	0	2	0	**2**
15	Altmetrics: métricas alternativas de impacto científico com base em redes sociais	1	1	0	**2**	41	Pesquisa social em ambientes digitais em tempos de covid-19: notas teórico-metodológicas	0	2	0	**2**

#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências	#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
16	Aplicativos de literatura-serviço: experiência e comportamento do usuário infantil	2	0	0	**2**	42	Proposta teórico-metodológica para o estudo de sujeitos informacionais usuários de sites de redes sociais virtuais	2	0	0	**2**
17	As mídias e as plataformas digitais no campo da educação permanente em saúde: debates e propostas	0	2	0	**2**	43	Propriedades do compartilhamento da informação em grupos de apoio social no facebook: uma revisão sistemática	2	0	0	**2**
18	Assessoria de imprensa no twitter: o que levou o "partido do twitter" a sentar-se na assembleia da república	0	0	2	**2**	44	Redes de tratamento e as associações de pacientes com doenças raras	0	2	0	**2**
19	Big data e mídias sociais: monitoramento das redes como ferramenta de gestão	0	2	0	**2**	45	Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no facebook	0	2	0	**2**
20	Blogueiros fitness no instagram: o corpo e o merchandising editorial de suplementos alimentares	2	0	0	**2**	46	Saúde coletiva e uma escolha de sofia: defender a privacidade no ciberespaço	0	2	0	**2**
21	Bullying na adolescência: visão panorâmica no brasil	0	2	0	**2**	47	Tecnologia de informação e comunicação no ensino de enfermagem	0	2	0	**2**
22	Ciclos de atenção a dietas da moda e tendências de busca na internet pelo google trends	0	2	0	**2**	48	Tecnologias de informação e comunicação, ativismo e movimentos sociais: uma revisão crítica da literatura brasileira (2010-2017) na perspectiva do campo de estudos de movimentos sociais	0	0	2	**2**
23	Comunicação, informação e imaginário no processo eleitoral brasileiro: o “messias” bolsonaro e o mito do rei pela graça de deus	1	0	1	**2**	49	Trabalho sexual em período de pandemia por covid-19 no contexto íbero-americano: análise de anúncios em websites	0	2	0	**2**

#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências	#	Título da Comunicação Científica	BRAPCI	SciELO	EBSCOhost	Total de Ocorrências
24	Contextualização de conceitos teóricos no processo de coleta de dados de redes sociais online	2	0	0	**2**	50	Uso da rede social facebook como ferramenta de comunicação na área de educação em saúde: estudo exploratório produção científica da área – 2005 a 2011	2	0	0	**2**
25	Covid-19, as *fake news* e o sono da razão comunicativa gerando monstros: a narrativa dos riscos e os riscos das narrativas	0	2	0	**2**	51	Ver com os olhos dos outros: (des) encontros e afetos em incursões etnográficas	0	0	2	**2**
26	Curta e compartilhe: conteúdos sobre alimentação saudável e dietas em páginas do facebook	0	2	0	**2**	52	**Total**	**15**	**20**	**31**	**66**

Fonte: Autora.

APÊNDICE B - TOTAL DE OCORRÊNCIAS DE TIPOS DE COMUNICAÇÕES CIENTÍFICAS, SEGMENTADAS POR STRING, INCLUINDO COMUNICAÇÕES CIENTÍFICAS TOTAIS (SEM RECORTE) E DESCARTADAS NA ANÁLISE (COM RECORTE), EM VALORES ABSOLUTOS E EM PERCENTUAIS

Tabela 5 - Total de ocorrências de tipos de comunicações científicas, segmentadas por string, incluindo comunicações científicas totais (sem recorte) e descartadas na análise (com recorte), em valores absolutos e em percentuais.

Tipo de Comunicação Científica	**Mídias sociais**	**Mídias sociais AND privacidade**	**Redes sociais AND privacidade**	**Redes sociais on-line**	**Redes sociais on-line AND privacidade**	**Redes sociais online**	**Redes sociais online AND privacidade**	**Total**		**Mídias sociais**	**Mídias sociais AND privacidade**	**Redes sociais AND privacidade**	**Redes sociais on-line**	**Redes sociais on-line AND privacidade**	**Redes sociais online**	**Redes sociais online AND privacidade**	**Total (em %)**
Sem recorte																	
Artigo de revisão	0	0	1	1	0	0	0	**2**		0,00%	0,00%	50,00%	50,00%	0,00%	0,00%	0,00%	**100,00%**
Artigo em Anais	0	0	1	0	0	2	0	**3**		0,00%	0,00%	33,33%	0,00%	0,00%	66,67%	0,00%	**100,00%**
Artigo em Periódico	112	2	83	29	5	67	8	**306**		36,60%	0,65%	27,12%	9,48%	1,63%	21,90%	2,61%	**100,00%**
Comunicação oral	0	0	0	1	0	1	1	**3**		0,00%	0,00%	0,00%	33,33%	0,00%	33,33%	33,33%	**100,00%**
Ensaios	0	0	1	0	0	0	0	**1**		0,00%	0,00%	100,00%	0,00%	0,00%	0,00%	0,00%	**100,00%**
Pecha Kucha	0	0	0	0	0	1	0	**1**		0,00%	0,00%	0,00%	0,00%	0,00%	100,00%	0,00%	**100,00%**
Periódico	0	0	1	0	0	0	1	**2**		0,00%	0,00%	50,00%	0,00%	0,00%	0,00%	50,00%	**100,00%**
Pesquisa em	0	0	0	1	0	1	0	**2**		0,00%	0,00%	0,00%	50,00%	0,00%	50,00%	0,00%	**100,00%**

Tipo de Comunicação Científica	Mídias sociais	Mídias sociais AND privacidade	Redes sociais AND privacidade	Redes sociais on-line	Redes sociais on-line AND privacidade	Redes sociais online	Redes sociais online AND privacidade	Total		Mídias sociais	Mídias sociais AND privacidade	Redes sociais AND privacidade	Redes sociais on-line	Redes sociais on-line AND privacidade	Redes sociais online	Redes sociais online AND privacidade	Total (em %)
andamento																	
Preprints	3	0	0	0	0	0	0	**3**		100,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**100,00%**
Relato de experiência	0	0	0	0	0	2	0	**2**		0,00%	0,00%	0,00%	0,00%	0,00%	100,00%	0,00%	**100,00%**
Relato de Pesquisa	0	0	0	1	1	2	2	**6**		0,00%	0,00%	0,00%	16,67%	16,67%	33,33%	33,33%	**100,00%**
Total	115	2	87	33	6	76	12	**331**		34,74%	0,60%	26,28%	9,97%	1,81%	22,96%	3,63%	**100,00%**
Com recorte																	
Artigo de revisão	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Artigo em Anais	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Artigo em Periódico	2	0	12	2	0	4	0	**20**		10,00%	0,00%	60,00%	10,00%	0,00%	20,00%	0,00%	**100,00%**
Comunicação oral	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Ensaios	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Pecha	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**

Tipo de Comunicação Científica	Mídias sociais	Mídias sociais AND privacidade	Redes sociais AND privacidade	Redes sociais on-line	Redes sociais on-line AND privacidade	Redes sociais online	Redes sociais online AND privacidade	Total		Mídias sociais	Mídias sociais AND privacidade	Redes sociais AND privacidade	Redes sociais on-line	Redes sociais on-line AND privacidade	Redes sociais online	Redes sociais online AND privacidade	Total (em %)
Kucha																	
Periódico	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Pesquisa em andamento	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Preprints	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Relato de experiência	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Relato de Pesquisa	0	0	0	0	0	0	0	**0**		0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	**0,00%**
Total	**2**	**0**	**13**	**2**	**0**	**5**	**0**	**22**		**10,00%**	**0,00%**	**60,00%**	**10,00%**	**0,00%**	**20,00%**	**0,00%**	**100,00%**

Fonte: Autora (2022).

Emitido em 23/05/2022

DISSERTAÇÃO Nº 13/2022 - FAARQ (11.36.15)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 30/06/2022 08:01)
FERNANDO DE ASSIS RODRIGUES
PROFESSOR DO MAGISTERIO SUPERIOR
ICSA (11.36)
Matrícula: ###853#1

Para verificar a autenticidade deste documento entre em https://sipac.ufpa.br/documentos/ informando seu número: **13**, ano: **2022**, tipo: **DISSERTAÇÃO**, data de emissão: **30/06/2022** e o código de verificação: **dea26e6d52**