

## **Pesquisas brasileiras da Ciência da Informação sobre Serviços de Redes Sociais *Online*, Privacidade de Dados Pessoais e Vigilância**

*Brazilian Information Science Research on Online Social Network Services, Personal Data Privacy, and Surveillance*

*Investigación brasileña en ciencias de la información sobre servicios de redes sociales en línea, privacidad y vigilancia de datos personales*

*Débora Matni Fonteles<sup>1</sup>  
Fernando de Assis Rodrigues<sup>2</sup>*

**Resumo:** O objetivo desta pesquisa foi realizar uma revisão sistemática de pesquisas científicas brasileiras da Ciência da Informação que tratam os temas de Serviços de Redes Sociais *Online*, Privacidade e Vigilância, a fim de estabelecer as principais preocupações sobre o uso destes serviços. Como método, utilizou-se a Revisão Sistemática de Literatura, utilizando como estratégia de busca termos relacionados a redes sociais e privacidade, nas bases de dados *Base de Dados em Ciência da Informação*, *Scientific Electronic Library Online* e *Academic Search Premier*, recuperando publicações científicas em língua portuguesa, publicadas em periódicos científicos no período de 2002 a 2020. Identificou-se um total de 331 publicações que, após uma filtragem qualitativa, analisou-se 20 publicações aderentes ao escopo de pesquisa. Os resultados revelaram fatores ligados a coleta de dados (tempo de permanência, fornecimento de dados e metadados, termos de serviço, motivação para interação e mecanismos de identificação), a privacidade (público e privado, compartilhamento de dados e quebra de confidencialidade, percepção da privacidade e criação de perfis) e vigilância (internet e dispositivos móveis, interações, funcionalidades e monitoramento e nível de confidencialidade). Todos os fatores foram analisados sob a ótica dos detentores de Serviços de Redes Sociais *Online* e dos sujeitos, verificando nas publicações os principais problemas referentes aos temas da pesquisa. Conclui-se que as publicações estabelecem uma relação com a literatura contemporânea, especialmente a

---

<sup>1</sup> Universidade Federal do Pará (UFPA), Belém, Pará, Brasil, dmatnif@gmail.com.

<sup>2</sup> Universidade Federal do Pará (UFPA), Belém, Pará, Brasil, deassis@ufpa.br.

vigilância líquida, ao verificar potenciais ações prejudiciais a privacidade dos sujeitos no momento em que utilizam os Serviços de Redes Sociais *Online*.

**Palavras-chave:** Serviços de Redes Sociais *Online*. Privacidade. Vigilância. Dados Pessoais. Dados.

**Abstract:** The objective of this research was to conduct a systematic review of Brazilian scientific studies in Information Science that address the topics of Online Social Network Services, Privacy, and Surveillance, to establish the main concerns regarding the use of these services. The method employed was a Systematic Literature Review, utilizing search strategies with terms related to social networks and privacy, in the databases *Base de Dados em Ciência da Informação*, *Scientific Electronic Library Online*, and *Academic Search Premier*. The review retrieved scientific publications in Portuguese, published in academic journals between 2002 and 2020. A total of 331 publications were identified, which, after qualitative filtering, resulted in the analysis of 20 publications aligned with the research scope. The results revealed factors related to data collection (time spent, provision of data and metadata, terms of service, motivation for interaction, and identification mechanisms), privacy (public and private, data sharing and breach of confidentiality, privacy perception, and profile creation), and surveillance (internet and mobile devices, interactions, functionalities, monitoring, and confidentiality levels). All factors were analyzed from the perspective of the holders of Online Social Network Services and the users, identifying the main issues related to the research themes in the publications. Concludes that the publications establish a connection with contemporary literature, especially liquid surveillance, by identifying potential harmful actions to users' privacy when engaging with Online Social Network Services.

**Keywords:** Online Social Network Services. Privacy. Surveillance. Personal Data. Data

**Resumen:** El objetivo de esta investigación fue realizar una revisión sistemática de investigaciones científicas brasileñas en el campo de la Ciencia de la Información que aborden los temas de Servicios de Redes Sociales en Línea, Privacidad y Vigilancia, con el fin de establecer las principales preocupaciones sobre el uso de estos servicios. El método utilizado fue la Revisión Sistemática de la Literatura, empleando como estrategia de búsqueda términos relacionados con redes sociales y privacidad, en las bases de datos *Base de Dados em Ciência da Informação*, *Scientific Electronic Library Online* y *Academic Search Premier*. Se recuperaron publicaciones científicas en portugués, publicadas en revistas científicas entre 2002 y 2020. Se identificaron un total de 331 publicaciones, que, tras un filtrado cualitativo, resultaron en el análisis de 20 publicaciones alineadas con el alcance de la investigación. Los resultados revelaron factores relacionados con la recopilación de datos (tiempo de permanencia, provisión de datos y metadatos, términos de servicio, motivación para la interacción y mecanismos de identificación), la privacidad (público y privado, compartiendo de datos y violación de la confidencialidad, percepción de la privacidad y creación de perfiles) y la vigilancia (internet y dispositivos móviles, interacciones, funcionalidades, monitoreo y niveles de confidencialidad). Todos los factores fueron analizados desde la perspectiva de los poseedores de los Servicios de Redes Sociales en Línea y los sujetos, verificando en las publicaciones los principales problemas relacionados con los temas de la investigación. Se concluye que las publicaciones establecen una relación con la literatura contemporánea, especialmente con la vigilancia líquida, al identificar potenciales acciones perjudiciales para la privacidad de los sujetos al interactuar con los Servicios de Redes Sociales en Línea.

**Palabras clave:** Servicios de redes sociales en línea. Privacidad. Vigilancia. Datos personales. Datos.

## 1 INTRODUÇÃO

Serviços de Redes Sociais *Online* (SRSOs), dados pessoais e privacidade possuem uma relação estreita na contemporaneidade. No contexto das mídias sociais, os dados pessoais são os principais insumos para os sistemas de informação que possibilitam a existência dos Serviços de Redes Sociais *Online*. Os sujeitos, na condição de usuários destes serviços, enviam informações pessoais aos seus perfis, realizam publicações de textos, de fotografias e de vídeos, interagem com demais sujeitos da rede, *ad infinitum*. Estas informações pessoais são organizadas pelos sistemas de informação dos detentores dos serviços. As informações pessoais são parte de um processo de coleta, inseridas em um massivo banco de dados, de forma sistematizada.

O uso de tecnologia para a formação de redes sociais não é algo novo. Trata-se de uma evolução. Com o passar do tempo, as tecnologias empregadas para permitir outras formas de transmissão de informação, para além dos gestos e da fala, se modificaram. Entre as tecnologias, surgiram a escrita, a imprensa e a internet, procurando criar sistemas e novas formas de comunicação, além ampliar as possibilidades sobre como as mensagens e as informações nelas contidas são transmitidas entre os sujeitos. No contexto contemporâneo, a infraestrutura propiciada pela internet é uma das mais significativas. Representa “[...] a possibilidade de expressão e sociabilização através das ferramentas de Comunicação Mediada pelo Computador (CMC)” (Recuero, 2014, p. 24), permitindo a quebra de barreiras temporais e espaciais (Freire, 1991), facilitando uma comunicação globalizada aos sujeitos participantes.

O uso da infraestrutura da internet, associado a uma disponibilidade de equipamentos como os dispositivos móveis, produz uma situação ímpar, aonde,

São perceptíveis as alterações do espaço e tempo na sociedade em rede promovidas pela mudança na esfera da comunicação, oriundas da revolução tecnológica, que resultou da transição dos meios de comunicação de massa tradicionais para um novo sistema de redes horizontais determinados pela internet e pela comunicação sem fio, culminaram em abolir distâncias e transformaram a sociedade em um sistema interativo de comunicação local – global em tempo real (Boff; Fortes; Freitas, 2018, p. 32).

Tais alterações, associadas ao processo comunicacional, estão relacionadas a um formato de interação entre os sujeitos (Boyd; Ellison, 2007; Recuero, 2014; Cruz; Araújo, 2020) contribuindo com a formação de ambientes informacionais – como as interações por meio das interfaces dos SRSOs (Rodrigues; Sant’Ana, 2018), tais como: *Facebook*, *Instagram*, *Kwai*, *TikTok* e *X*. Nos SRSOs, abrem-se possibilidades de participação direta, por

meio da produção de conteúdo e interações, e indireta, socializando e compartilhando conteúdo dentro e fora dos serviços, na ordem de promover discussões (França *et al.*, 2014).

Este processo é complementado pela forma com que os dados pessoais são produzidos, armazenados e acessados em SRSOs, por meio da multiplicidade de dispositivos móveis e de aplicativos disponíveis – sendo estes os recursos técnicos que oferecem condições para que os sujeitos sejam alvo de uma coleta de dados para monitoramento de sua rotina diária pelos SRSOs, possibilitando até acesso aos conteúdos audiovisuais produzidos; além de, caso seja de interesse do sujeito, ser canal para divulgá-las de forma deliberada para parceiros desses serviços, ou mesmo para um público externo (Boff; Fortes; Freitas, 2018; Rodrigues; Sant’Ana, 2018).

O que pode tornar tal processo preocupante é o que é passível de realização com os dados pessoais, especialmente sobre os aspectos inerentes a privacidade dos sujeitos. Os SRSOs possuem um Termo de Serviço: contrato social estabelecido entre sujeitos e detentores dos serviços. O problema reside na descrição destes processos nestes termos, pois são diluídos em linguagem jurídica e tecnicista (Rodrigues, Sant’Ana, 2018). Deixando de lado uma visão maniqueísta e superficial, um exemplo é a adição de metadados aos dados pessoais, permitindo agregar a geolocalização, as redes públicas e privadas de internet no raio de ação do dispositivo móvel, os sujeitos que estão próximos e, a partir disso, realizar a segmentação de interesses e gostos, por meio do reconhecimento de padrões (Boff; Fortes; Freitas, 2018).

Com relação aos reconhecimentos de padrões, os SRSOs possuem capacidade ímpar. A coleta de dados pessoais, agora fomentada e ampliada pelo uso de Tecnologias de Informação e Comunicação (TICs) (Príncipe, 2013), resultado das interações entre os sujeitos nos SRSOs, é massiva e contínua. A partir desta quantidade massiva de dados pessoais disponíveis (que é contextualizada como parte integrante do fenômeno *big data*), os serviços conseguem verificar o “[...] reconhecimento de padrões de suas conexões e a visualização de suas redes sociais” (Recuero, 2014, p. 24), padrões estes que podem estabelecer um regime de vigilância sobre os sujeitos participantes dos serviços.

Como os SRSOs já são uma realidade estabelecida na comunicação entre sujeitos – inclusive influenciando gostos, intenções de compra e até aspectos religiosos e políticos (Sanhotene; Silveira; Lavarda, 2017) – é natural que seja fenômeno observado por diferentes áreas do conhecimento, incluindo a Ciência da Informação – uma das áreas do conhecimento que possuem, *a priori*, uma forte relação com estudos do fluxo informacional. Neste sentido, desconhecer como publicações científicas desta área do conhecimento convergem os temas

SRSOs, Privacidade e Vigilância pode, conseqüentemente, ofuscar como as pesquisas abordam este assunto, as principais observações e inquietações, problema desta pesquisa.

Especialmente no Brasil este tema se torna excepcionalmente relevante, ao levar em consideração que, no ano de 2022, 92 milhões de brasileiros acessaram a internet apenas por meio de dispositivo móvel e 43% postaram conteúdo de sua autoria (Cetic.br, 2023), sendo o país que liderou o tempo diário gasto em uso deste tipo de serviço em 2024 (Statista, 2024).

Portanto, o objetivo desta pesquisa foi realizar uma revisão sistemática de pesquisas científicas brasileiras da Ciência da Informação que tratam os temas de Serviços de Redes Sociais *Online*, Privacidade e Vigilância, a fim de estabelecer as principais preocupações sobre o uso destes serviços.

## **2 SERVIÇOS DE REDES SOCIAIS ONLINE, COLETA DE DADOS E PRIVACIDADE: UMA SOCIEDADE VIGIADA?**

Uma das principais razões do sucesso dos serviços *online* está na praticidade. Os aplicativos para dispositivos móveis se tornaram essenciais à vida moderna, desde o acesso a conta em uma instituição financeira até nos comunicarmos com os entes próximos, como os SRSOs (França *et al.*, 2014). No caso dos SRSOs, a praticidade reside não só na possibilidade de comunicação, mas também um acesso a conteúdo multimídia que permitem a realização tanto de atividades de entretenimento, como profissionais (Rodrigues; Sant'Ana, 2018).

Por sua vez, a praticidade tem estreita ligação com o conceito de latência: a mensuração do tempo de solicitar dados e obter uma resposta em uma infraestrutura de rede. Uma baixa latência reflete em uma maior rapidez com que os sujeitos são atendidos em suas necessidades (Novo; Azevedo, 2014). Soma-se a isto a multiplicação de dispositivos com *multisensores* (*e.g. smartphones, smartwatches e tablets*), que permitem registrar fotografias, vídeos, áudios, batimentos cardíacos e pressão arterial, passos, rastreamento por geolocalização, posicionamento do giroscópio, entre outras funcionalidades que, combinadas, permitem registrar fatos do cotidiano (França *et al.*, 2014) e, conseqüentemente, aumentando de forma exponencial a transmissão de dados pela internet. Um exemplo é o sujeito que, ao executar uma atividade física de corrida, está ouvindo música, postando fotografias e vídeos do treino, monitorando sua condição física, permitindo o rastreamento do percurso e o *pace* (ritmo médio de um corredor, em minutos por quilômetro), que ao final postará também seu percurso em um SRSOs para seus seguidores.

As detentoras dos SRSOs são entendidas

[...] como instituições que elaboram um ou mais serviços. Os serviços são disponibilizados por meio de ferramentas na forma de *websites* e de aplicativos para dispositivos móveis, eletrodomésticos e *wearables*, com o intuito de subsidiar um espaço que permita a comunicação e o inter-relacionamento de Referenciados, que podem ser pessoas, grupos ou instituições. [...] Afinal, por que se aborda as Redes Sociais *Online* como um serviço e não uma ferramenta ou uma plataforma? A resposta é simples. O indivíduo é obrigado a assinar e concordar com um Termo de Serviço ao acessar pela primeira vez o sistema. Trata-se de um contrato social entre o indivíduo e a instituição detentora do serviço, tal qual é realizado com uma operadora de internet ou com a assinatura de um serviço de eletricidade. O que pode dar certa opacidade neste contrato é que os Serviços de Redes Sociais *Online* são gratuitos para utilização, na maioria dos casos. (Rodrigues, 2024a, p. 23-43)

Como supramencionado, o Brasil está entre o grupo de maior uso deste tipo de serviço. Em 2022, o Brasil possuía uma população de aproximadamente 203 milhões de habitantes (IBGE, 2022), com 132 milhões de sujeitos conectados à internet, mais da metade da população. Segundo relatório da Data.ai (2024), a média de uso mensal de SRSOs em 2024 por parte dos brasileiros está distribuída da seguinte forma. Os nove serviços mais utilizados são: *TikTok* (30 horas), *WhatsApp* (24 horas), *YouTube* (22 horas), *Instagram* (22 horas), *Facebook* (12 horas), *X* (três horas), *Pinterest* (duas horas), *Telegram* (uma hora) e *LinkedIn* (menos de uma hora).

Esse uso cotidiano é constante dos SRSOs, associado a uma quantidade expressiva de postagens e conteúdo que os sujeitos deliberadamente enviam para os serviços, deixa-se uma pegada digital (ou rastro digital).

Neste sentido,

Os Termos de Uso e as Políticas de Privacidade já são bastante explícitos sobre os poderes extremos da plataforma sobre seus usuários e os rastros que deixam, sem muito pudor de expor tal ascensão acerca da vida das pessoas. Investigações de autoridades regulatórias e sanções mostraram diversos casos de violação por parte do *Facebook*, inclusive recorrentes. Na análise dos componentes e dos recursos técnicos, a elaboração das ferramentas visando a coleta de dados ficou bastante visível, do *news feed* aos logins e *plugins* sociais para *apps* e sites (Valente, 2019a, p. 342).

Os dados coletados pelos detentores dos SRSOs são processados em “[...] um conjunto de sistemas que possibilitam a análise de textos em quantidades massivas [...]” (Novo; Azevedo, 2014, p. 65) sendo considerado também o *Santo Graal* do conhecimento comportamental, pela razão que dados e metadados revelam impressões ou sintomas do comportamento ou humor real das pessoas (Van Dijck, 2014).

Contudo, visualizar dados pessoais em SRSOs apenas como um ativo financeiro dos detentores dos serviços é limitar a visão apenas pelo lado econômico. Processar os dados

personais e seus metadados também pode ser objeto de uma forma de controle social, de modulação de comportamentos e, mais grave, permitir um grau maior de vigilância sobre os sujeitos (Valente, 2019b).

Em senso comum, vigiar remete a ideia de observar algo ou alguém. É necessário ter o objeto de vigilância sob a ótica da visão digital. Na literatura, podemos observar este fenômeno por conceitos e alegorias, como o conceito descrito por Bentham (2008, p. 89) como panóptico, “[...] dispositivo polivalente da vigilância, a máquina óptica universal das concentrações humanas”, a figura do Grande Irmão de Orwell (2009), o líder supremo totalitário que controla uma máquina estatal de vigilância, entre outras ficções.

A utilização de dispositivos (como os SRSOs) para controle social não é um fenômeno novo. As formas de controle social descritas por Foucault (2014) no século XIX não tinham apenas o objetivo da reclusão em escolas ou em instituições prisionais, mas também impor disciplina por meio de aplicação de limitações repetidas seja na execução de exercícios com horários determinados ou na movimentação do corpo de maneira obrigatória acreditando ser o treino a melhor maneira de controlar o comportamento humano.

Já na percepção de Bauman e Lyon (2013), o conceito contemporâneo é um pós-panóptico, aonde a vigilância e as formas de controle, antes relacionadas a um estado estável (sólido) que atingia habitualmente a classe marginalizada, se tornaram móveis e flexíveis, influenciando outras áreas da sociedade, se transformando em uma dimensão central da modernidade.

Ou seja, as formas de controle social descritas por Foucault (2014) e alegorizadas por Bentham (2008) e por Orwell (2009) foram se aperfeiçoando ao longo do tempo. A vigilância deixou de ter relação com prisões, disciplina e punição. Para Bauman e Lyon (2014), as paredes de concreto deram lugar às telas, as câmeras de vigilância e outros sensores que coletam dados por meio de atividades cotidianas, de forma rotineira, automática e espontânea, assim como nossas interações em SRSOs.

As formas de controle deram lugar à flexibilidade, ao controle do entretenimento e do consumismo (Bauman; Lyon, 2014), fazendo com que dados pessoais dos sujeitos, antes privados, agora se tornem públicos nos SRSOs. No imaginário popular, o ato de ter uma conta privada em SRSOs dá a sensação de tornar seus dados pessoais privados, quando na prática estão disponíveis irrestritamente aos detentores dos serviços – instituições privadas, de capital aberto ou fechado, que visam o lucro para manter a operação dos serviços ofertados (Rodrigues, 2024a), impactando em potenciais problemas de privacidade dos dados pessoais.

Solove (2009) contextualiza a ideia de privacidade, em uma releitura contemporânea das teorias propostas por Westin (1970), primeiramente, em compreender que o conceito de privacidade não só é mutável como culturalmente distinto. Privacidade é, portanto, “[...] um direito fundamental, essencial para a liberdade, democracia, bem-estar psicológico, individualidade e criatividade. Alguns alegam que a privacidade está próxima da extinção; outros argumentam que a ameaça à privacidade é ilusória” (Solove, 2009, tradução nossa). Em um contexto de SRSOs, o estado de ambiente privativo para dados pessoais parece praticamente ilusório, mas a academia cabe um aprofundamento minucioso das relações entre SRSOs e a privacidade dos dados pessoais dos sujeitos.

### 3 PROCEDIMENTOS METODOLÓGICOS

Trata-se de uma pesquisa de abordagem qualitativa, de natureza básica, de objetivo exploratório. Com relação aos procedimentos, adotou-se a Revisão Sistemática de Literatura (RSL). Descartou-se a possibilidade do uso da meta-análise por não empregar o uso de estatística da produção científica analisada. Neste sentido, dados estatísticos das pesquisas não foram considerados, utilizando-se apenas resultados e considerações qualitativas sobre a temática investigada.

Utilizou-se uma adaptação do modelo de Conforto, Amaral e Silva (2011) para aplicação da RSL, contendo três fases, divididas em etapas de número variável para cada fase: a) Entrada (Fase I), aonde foram definidas as atividades iniciais da RSL, a partir do planejamento e do objetivo da pesquisa, b) Processamento (Fase II), que consistiu na execução das atividades planejadas na fase de Entrada, a fim de se chegar a amostra sobre pesquisas sobre o tema e c) Saída (Fase III), com enfoque em formular os resultados apresentados. As etapas de cada fase são detalhadas no Quadro 1.

**Quadro 1** – Fases e Etapas da RSL e a aplicação na pesquisa

Fase	Etapa	Aplicação
Entrada (I)	Definir as bases de dados para a recuperação das publicações científicas.	Base de Dados em Ciência da Informação (BRAPCI).
		<i>Scientific Electronic Library Online</i> (SciELO).
		<i>Academic Search Premier</i> (EBSCO).
	Definir os critérios de inclusão.	Artigos publicados em periódicos científicos.
		Textos em língua portuguesa.
		Acesso aberto ( <i>Open Access</i> ) ao texto completo.
Definir os critérios de qualidade.	Conter na introdução, resumo ou nas palavras-chave as variações dos termos {redes sociais <i>online</i> , redes sociais <i>on-line</i> ou mídias sociais} <sup>1</sup> , além de associá-los com o termo privacidade (utilizando o operador <i>and</i> ).	
	Período de publicação entre 2002 e 2020.	
		Publicações em Periódicos que possuíam critério de avaliação igual ou superior ao estrato QUALIS B2 (CAPES), quadriênio 2013-2016.

Fase	Etapa	Aplicação
	Estabelecer os filtros aplicados durante a realização das buscas.	Dependente de cada interface de pesquisa.
Processamento (II)	Executar as buscas das comunicações científicas.	Executado entre os dias 10 de novembro de 2021 a 13 de dezembro de 2021.
	Realizar o registro dos metadados e da publicação.	Registro dos metadados: Autoria, Título da Publicação, Ano de Publicação, Título do periódico, DOI, ISSN, Volume, Número, <i>Hyperlink</i> de acesso, Palavras-chave e Resumo. Armazenamento dos textos completos, em formato <i>Portable Document Format</i> (PDF).
	Fazer a leitura e análise das comunicações científicas.	Realizada a leitura técnica de partes da publicação: título, resumo, palavras-chave, introdução, considerações finais para definição se a publicação possui aderência ao tema da pesquisa. No caso de dúvidas, foi aprofundada a análise com a leitura do texto completo.
Saída (III)	Registrar e arquivar os artigos em periódicos utilizados em análise.	Separou-se os metadados e os documentos em formato PDF de publicações consideradas aderentes ao escopo da pesquisa.
	Sintetização dos resultados.	Fichamento das pesquisas, com enfoque em detalhar os principais avanços e conclusões sobre a temática.
	Elaboração dos resultados.	Sistematização e elaboração dos resultados desta pesquisa, apresentada nos resultados e discussão.

<sup>1</sup> Optou-se pelo uso destes termos compostos, a partir dos estudos sobre conceitos sobre Rede Sociais utilizadas por pesquisadores brasileiros (Rodrigues, 2024b).

**Fonte:** Elaborado pelos Autores (2024), adaptador de Conforto, Amaral e Silva (2011).

No caso da Etapa *Estabelecer os filtros aplicados durante a realização das buscas*, da Fase de Entrada (I), o processo de filtragem é dependente de cada interface de busca, a saber:

- BRAPCI: aplicação do filtro de janela temporal (2002 a 2020), pesquisa exata (com uso de aspas duplas) dos termos no texto completo, ordenados por relevância;
- SciELO: pesquisa dos termos em todos os índices, ordenados por relevância. Após a execução foi possível realizar a filtragem de janela temporal (2002 a 2020);
- EBSCO: pesquisa dos termos em todos os índices, ordenados por relevância. Após a execução foi possível realizar a filtragem de janela temporal (2002 a 2020).

No caso da EBSCO e da SciELO, optou-se por não utilizar a filtragem por área do conhecimento, pois há periódicos de outras áreas do conhecimento que são classificados em estratos da Área de Avaliação *Comunicação e Informação* do QUALIS. Portanto, o descarte coube a filtragem manual, a partir da etapa *Definir os critérios de qualidade*, da Fase de Entrada (I).

**Tabela 1** – Quantidade de comunicações científicas recuperadas para os termos de busca, segmentadas por termo de busca e base de dados, em valores absolutos e percentuais

Termo(s)	Nº de Publicações			Total	% de Representatividade			Total
	BRAPCI	SciELO	EBSCO		BRAPCI	SciELO	EBSCO	
Mídias sociais	0	110	5	115	0,000%	95,650%	4,350%	100,00%
Mídias sociais AND privacidade	1	1	0	2	50,000%	50,000%	0,000%	100,00%
Redes sociais AND privacidade	7	11	69	87	8,050%	12,640%	79,310%	100,00%
Redes sociais on-line	11	4	18	33	33,330%	12,120%	54,550%	100,00%

Redes sociais <i>on-line</i> AND privacidade	3	0	3	6	50,000%	0,000%	50,000%	100,00%
Redes sociais <i>online</i>	26	8	42	76	34,210%	10,530%	55,260%	100,00%
Redes sociais <i>online</i> AND privacidade	8	0	4	12	66,670%	0,000%	33,330%	100,00%
<b>Total</b>	<b>56</b>	<b>134</b>	<b>141</b>	<b>331</b>	<b>16,920%</b>	<b>40,480%</b>	<b>42,600%</b>	<b>100,00%</b>

Fonte: Elaborado pelos Autores (2024).

A Tabela 1 apresenta a quantidade de publicações coletadas nas três bases de dados, totalizando 331 publicações. Foram descartadas 111 publicações, por não serem publicações em periódicos científicos (indicador *Definir os critérios de inclusão*, da Fase de Entrada (I)) ou por estarem publicadas em periódicos com estrato QUALIS menor que B2 (indicador *Definir os critérios de qualidade*, Fase de Entrada ((I))).

Após este processo, foi realizada a etapa *Fazer a leitura e análise das comunicações científicas* da Fase de Processamento (II), descartando 200 publicações.

**Tabela 2** – Total de ocorrências de estratos QUALIS, segmentados por estrato QUALIS e base de dados, em valores absolutos

Estrato QUALIS	Redes sociais <i>online</i>	Redes sociais <i>on-line</i>	Redes sociais AND privacidade	Redes sociais <i>online</i> AND privacidade	Redes sociais <i>on-line</i> AND privacidade	Mídias sociais AND privacidade	Mídias sociais	Total
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
<b>Total</b>	<b>4</b>	<b>2</b>	<b>12</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>2</b>	<b>20</b>

Fonte: Elaborado pelos Autores (2024).

A Tabela 2 apresenta as publicações analisadas, totalizando 20 publicações (listadas no Apêndice A), sendo três publicações no periódico *Sessões do Imaginário* e as demais publicadas nos periódicos (com uma publicação cada): *Comunicação e Sociedade*; *Contemporânea: Revista de Comunicação e Cultura*; *Em Questão*; *Estudos e Pesquisas em Psicologia*; *Fórum Lingüístico*; *Interface – Comunicação, Saúde, Educação*; *Literatura: Teoria, História, Crítica*; *Movimento*; *Observatorio*; *Pesquisa Brasileira em Ciência da Informação e Biblioteconomia*; *Prisma Jurídico*; *Psicologia: Teoria e Prática*; *Revista Brasileira de Educação Médica*; *Revista Brasileira de Estudos Pedagógicos*; *Revista de Administração da UFSM*; *Revista de Gestão dos Países de Língua Portuguesa*, e; *Sociologias*.

#### 4 RESULTADO E DISCUSSÃO

O Quadro 2 sintetiza fatores que contribuem diretamente ou indiretamente com a coleta de dados pessoais pelos SRSOs, apresentando ações por parte dos detentores dos serviços, situações relacionadas aos sujeitos que utilizam os serviços, bem como as publicações que se relacionam com o fator.

**Quadro 2** – Síntese dos fatores identificados que contribuem para ações de coleta de dados pessoais em SRSOs

Fatores	Detentor dos SRSOs	Sujeitos	Publicações relacionadas
Tempo de permanência	Estimula maior tempo de permanência dos sujeitos participantes.	Há maior possibilidade de fornecimento de dados por nativos digitais. Os nativos digitais têm maior participação no uso de SRSOs.	Borges, 2020
			Rosado; Tomé, 2015
Fornecimento de dados e metadados	Estabelecem a necessidade de coleta de dados e metadados para permitir a utilização do serviço.	Fornece de atributos identificáveis ( <i>e.g.</i> nome, cidade de nascimento ou de domicílio atual), além de postagens e conteúdo multimídia.	Assumpção; Santana; Santos, 2015
			Lima, 2018
			Rosado; Tomé, 2015
			Sá, 2018
Termos de Serviço	Só permite o uso do serviço com aceite total dos Termos de Serviço	Ao utilizar o serviço, dá direito de exploração comercial de parte dos conjuntos de dados e metadados, além do conteúdo multimídia, ao detentor do serviço. Por se tratar de um texto em linguagem técnica e jurídica, pode ter um impacto sobre a soberania de seus dados pessoais, não compreendendo de forma ampla o que se realizará com seus dados.	Assumpção; Santana; Santos, 2015
			Borges, 2020
			Fugazza; Saldanha, 2018
Motivação para Interação	Motivam os sujeitos a interagirem de formas variadas, coletando desde comentários até reações emocionais.	A interação gera a monetização dos dados pessoais, equiparando o dado pessoal como uma mercadoria valiosa para geração de lucro para detentores e parceiros comerciais.	Amaral Filho; Blanco, 2014
			Borges, 2020
			Comin <i>et al.</i> , 2014
Mecanismos de Identificação	Investem em mecanismos sofisticados de identificação de dados pessoais.	Ficam suscetíveis a sua identificação em outros contextos fora do serviço, por meio de algoritmos que utilizam seus dados pessoais coletados para identificar e segmentar públicos, compartilhando parte dos dados e análises com parceiros comerciais.	Assumpção; Santana; Santos, 2015
			Borges, 2020
			Martorell; Nascimento; Garrafa, 2015

**Fonte:** Elaborado pelos Autores (2024).

A coleta de dados pode estar associada ao tempo de permanência, ou seja a quantidade de horas que um sujeito permanece logado e, portanto, aumentando o grau de participação em SRSOs, especialmente pelos nativos digitais. Quanto maior é a permanência em SRSOs, maior será o tempo de exposição e conseqüentemente de coleta de dados. Isto acontece porque os SRSOs possuem interfaces elaboradas como meio de entretenimento, no qual conseguem identificar e selecionar sujeitos mais suscetíveis a ficarem conectados (*e.g.* segmentando conteúdos aderentes), além de oferecer outros serviços para cada necessidade de público, sendo formas de mantê-los conectados diariamente.

Além disso, há uma expectativa do detentor do serviço em coletar dados fornecidos pelos sujeitos, já que o objetivo é a interação entre os sujeitos participantes, bem como o preenchimento de seus perfis com informações pessoais e circulação de conteúdo multimídia. Com isso, os sujeitos deixam rastros digitais de suas atividades.

Outro fator relacionado à coleta de dados é o aceite aos Termos de Serviço. Só há a possibilidade de participação nos SRSOs com o aceite aos termos de forma plena, o que em

muitos casos representa o direito de exploração de dados tanto pelos detentores como por parceiros comerciais. Como elemento complicador existe uma dificuldade de compreensão dos Termos de Serviço pelos sujeitos. Isso dificulta compreender o *modus operandi* quanto a coleta de dados, que ocorre com opacidade ao sujeito sobre o que é realizado com os dados pessoais.

Associado ao aceite pleno aos Termos de Serviço, os SRSOs são ambientes que motivam os sujeitos a interação – tanto entre sujeitos, como com conteúdo circulante – o que confere aos detentores de SRSOs a possibilidade coletar dados, analisá-los, e monetizá-los, ou seja, transformam dados em produto negociável. Por este processo ser a principal forma de lucro dos SRSO, os detentores, por meio de algoritmos, tentam motivar novas formas de interação, com a finalidade de que mais dados sejam coletados.

A partir da coleta de dados, todo o processo é construído para que seja possível identificar o sujeito de várias formas, aonde os detentores dos SRSOs investem em mecanismos de identificação e de coleta de dados, estabelecendo para isso parcerias com empresas como os *data-brokers*: corretores de dados que têm como função reunir, organizar e classificar dados pessoais, a partir do que é coletado em serviços *online*, tendo como foco a comercialização de dados pessoais ou análises de dados pessoais com terceiros (Valente, 2019).

Portanto, os mecanismos de identificação dos dados pessoais previamente coletados são sofisticados, a ponto de identificar um sujeito a partir de fragmentos de um único registro. Uma das técnicas é o reconhecimento facial e corporal, consiste em identificar dados por meio de análise de imagem. Assim, mesmo que um sujeito apareça parcialmente em uma fotografia enviada por outro sujeito, por parte de seu corpo é possível reconhecer características suas que, combinadas a outras registradas anteriormente, permita identificá-lo.

Com relação aos potenciais riscos à privacidade de dados pessoais, o Quadro 3 sintetiza as principais discussões das publicações analisadas.

**Quadro 3** – Síntese dos fatores identificados que contribuem para potenciais risco a privacidade de dados pessoais em SRSOs

Fatores	Detentor dos SRSOs	Sujeitos	Publicações relacionadas
Público e Privado	Permite a exposição de dados pessoais internamente e a terceiros.	Tem dificuldade em compreender que o ambiente dos SRSOs é um ambiente público, mesmo quando sua conta de usuário tem o perfil privado.	Assumpção; Santana; Santos, 2015
			Barriga, 2020
			Fugazza; Saldanha, 2018
			Rebs, 2017
			Thibes, 2017

Fatores	Detentor dos SRSOs	Sujeitos	Publicações relacionadas
Compartilhamento de dados e quebra de confidencialidade	O serviço possui uma facilidade e velocidade ímpar no ato de compartilhamento de dados.	Podem perder o controle sobre dados pessoais veiculados, pois o compartilhamento tem característica viral.	Amaral Filho; Blanco, 2014
			Bittencourt; Gonzatti; Esmitz, 2016
			Santos; Porto; Alturas, 2010
Percepção da Privacidade	O serviço pode permitir um acesso a dados pessoais não autorizado ou consentido a terceiros.	Sujeitos podem ter diferentes percepções sobre a privacidade, considerando ou não uma violação a privacidade de seus dados. Implica a exposição de dados de forma não autorizada.	Barriga, 2020
			Hage; Kublikowski, 2019
			Lima, 2018
			Martorell; Nascimento; Garrafa, 2015
			Mendes-Campos; Féres-Carneiro; Magalhães, 2016
			Purim; Tizzot, 2019
			Santos; Porto; Alturas, 2010
Criação de perfis	Permitem a criação de perfis falsos ou de <i>multiperfis</i> .	Para o sujeito, este tipo de possibilidade gera uma série de problemas, tais como: propagação de discursos de ódio, <i>hackeamento</i> de dados, falsidade ideológica e vazamento de dados.	Comin <i>et al.</i> , 2014
			Fugazza; Saldanha, 2018
			Rebs, 2017
			Santos; Porto; Alturas, 2010

**Fonte:** Elaborado pelos Autores (2024).

Com a chegada de SRSOs, houve uma mudança de compreensão sobre os conceitos do que é público ou do que é privado, impactando nos processos de proteção da intimidade do sujeito. A exibição da vida privada no contexto de SRSOs 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.

Em relação aos SRSOs, ainda existe ainda outra implicação – que funcionam como ambientes híbridos – a sensação de que configurar o perfil do sujeito de forma pública ou privada altera o acesso de todos os atores envolvidos no serviço, quando, na realidade, o detentor do serviço sempre terá acesso completo a todos os dados pessoais armazenados, potencializando ações que podem ser prejudiciais à privacidade.

O compartilhamento de dados é outro aspecto que foi observado. Além da velocidade de compartilhar conteúdos ser ímpar (que no final todos são atrelados a dados pessoais), com características virais de propagação, o modo de funcionamento pode apresentar potenciais ações que prejudique a privacidade dos dados dos sujeitos. Mesmo que o sujeito possua um perfil privado e compartilhe conteúdos somente com amigos com perfis no serviço, estes podem copiar, fazer *print-screen* (*screenshot*) e compartilhar com outros perfis e em outros SRSOs, de forma viral, forçando uma alteração do estado inicial do público autorizado a visualizar o conteúdo do sujeito, de privado para público, sendo portanto um risco à privacidade, quebrando a confidencialidade entre as partes: o detentor do serviço e o sujeito.

Outro aspecto abordado pelos autores é sobre a percepção de privacidade que não é igual para todos os sujeitos, além de não se terem um entendimento sólido sobre o seu conceito ou sobre a sua importância. No contexto dos SRSOs, o conceito de privacidade está vinculado às tentativas de proteger os dados do sujeito. Todavia, as publicações relacionadas a este tema sinalizam que a privacidade no contexto *online* deixou de ter importância ou está caindo em desuso, ou mesmo que os sujeitos abrem mão da privacidade em troca de algum tipo de interação. Afirma-se também que a privacidade possui valores distintos para diferentes gerações, tornando-a cada vez mais vulnerável e, portanto, não sendo uma prioridade de discussão para os governos como foram, por exemplo, as questões de ampliação do acesso à internet ou do acesso livre à informação.

Isto está relacionado a diferentes percepções que a privacidade pode assumir para cada sujeito, e esta percepção reflete sobre as escolhas no momento em que se compartilham dados pessoais. Assim, quando um sujeito toma a decisão de compartilhar dados a um amigo e não a um parente, está determinando como deseja ter a sua privacidade preservada. Porém o maior problema consiste no resguardo a ter seus dados pessoais coletados por empresas (detentoras de SRSOs), que podem ou não compartilhar dados pessoais ou a análise destes com parceiros comerciais.

Mesmo no caso de sujeitos que não são participantes de SRSOs, os serviços produzem um fenômeno que reflete na privacidade dos sujeitos. Um exemplo são os profissionais de saúde e de educação, que utilizam os SRSOs como forma de divulgar rotinas das clínicas, hospitais ou escolas. Ao fazerem este tipo de ação, sem o devido cuidado a legislação vigente, podem revelar particularidades de pacientes ou de estudantes sem uma prévia autorização, uma exposição de dados não autorizada.

Por último, outro fator em relação à privacidade nas publicações analisadas é a possibilidade de criação de perfis falsos, ou de vários perfis por um mesmo sujeito (*multiperfil*), não sendo necessário uma verificação que confirme a veracidade dos dados, como ocorre, por exemplo, com o registro de abertura de conta em uma instituição financeira. Os perfis falsos podem ser utilizados para obter informações sobre outros sujeitos ou empresas por meio de técnicas de engenharia social.

As estruturas dos SRSOs permitem a criação deste tipo de perfil, permitindo um certo anonimato e dificultando a sua identificação. Sujeitos com esses perfis se aproveitam da invisibilidade ou do uso de *multiperfis* para acessar páginas pessoais com a intenção de

perseguir (*cyberstalking*) um sujeito, obter dados pessoais para promover golpes e *hackeamento* ou propagar discursos de ódio.

Assim como apresentado no marco teórico, os conceitos de coleta de dados e de privacidade das publicações se relacionam com a ideia de um ambiente de vigilância em SRSOs. O Quadro 4 apresenta a síntese dos fatores identificados que podem contribuir para ações de vigilância em SRSOs.

**Quadro 4** – Síntese dos fatores identificados que podem contribuir para ações de vigilância em SRSOs

Fatores	Detentor dos SRSOs	Sujeitos	Publicações relacionadas
Internet e Dispositivos Móveis	Utiliza diversos sensores dos dispositivos móveis para uma maior coleta de dados e metadados do sujeito.	Cotidianamente utiliza os dispositivos móveis e o acesso à internet para o compartilhamento de dados pessoais.	Assumpção; Santana; Santos, 2015
			Barriga, 2020
			Borges, 2020
			Comin <i>et al.</i> , 2014
			Hage; Kublikowski, 2019
			Purim; Tizzot, 2019
Interações	Mantém um ambiente que motiva a interação entre sujeitos ou grupos de sujeitos, por meio do estabelecimento de redes de relações, diretas e indiretas.	Não compreende a fragilidade quanto à segurança de dados pessoais em função da possibilidade de interações indiretas.	Streck; Pellanda, 2017
			Amaral Filho; Blanco, 2014
			Assumpção; Santana; Santos, 2015
			Barriga, 2020
			Bittencourt; Gonzatti; Esmitez, 2016
			Hage; Kublikowski, 2019
			Leitzke; Rigo, 2020
			Lima, 2018
Rebs, 2017			
Funcionalidades e Monitoramento	Aproveita-se da maior produção e circulação de dados, permitindo melhores condições de monitoramento dos sujeitos, interferindo no comportamento dos sujeitos.	As funcionalidades resultam um comportamento dos sujeitos em utilizar os serviços como meios de divulgação, armazenamento e compartilhamento de fatos do cotidiano.	Rosado; Tomé, 2015
			Assumpção; Santana; Santos, 2015
			Barriga, 2020
			Borges, 2020
			Fugazza; Saldanha, 2018
			Jurno; D'andréa, 2017
Nível de confidencialidade	Tem acesso total e controle sobre os dados.	O sujeito tem a falsa sensação que pode controlar o acesso aos seus dados pessoais, restringindo-os a outros sujeitos participantes.	Streck; Pellanda, 2017
			Santos; Porto; Alturas, 2010

**Fonte:** Elaborado pelos Autores (2024).

Diferente dos primeiros aparelhos de telefonia móvel, os dispositivos móveis possuem diversos recursos de sensoriamento e registro, desde com câmeras fotográficas até sensores de *Global Positioning System* (GPS). Estes recursos são utilizados automaticamente ou manualmente pelos aplicativos instalados – incluindo os SRSOs – permitindo a coleta de dados e metadados do sujeito. Por exemplo, o sujeito pode registrar uma fotografia e enviar a um Serviço de Rede Social *Online* (SRSO), no qual poderá incluir metadados do dispositivo móvel e de georreferenciamento, a latitude e a longitude (coletada pelo sensor de GPS).

Mesmo que os detentores dos SRSOs não compartilhem estes metadados com os demais sujeitos participantes, os serviços poderão armazená-los em um banco de dados interno a detentora. Além disso, o aumento de disponibilidade de acesso à internet por banda larga fixa ou dados móveis, permitem o uso de SRSOs em qualquer lugar, compartilhando conteúdos de forma rápida e, conseqüentemente, aumentando o nível de exposição de dados pessoais nestes serviços. Percebe-se que esses dois elementos têm se tornado poderosos aliados no processo de vigilância.

Há uma mão de via dupla neste processo. As TICs oferecem uma maior praticidade a vida dos sujeitos, via acesso à internet e uso dos dispositivos móveis, porém, ao mesmo tempo, permite que sejam realizadas ações de vigilância, principalmente monitorando a interação dos sujeitos, seus passos, na intenção de identificar, de maneira eficiente, informações precisas sobre os participantes dos SRSOs.

As interações nestes serviços são consideradas extensões de nossas relações sociais no ambiente físico, em que informações e dados são transportados, mas agora de forma viral. Nos SRSOs, as estruturas são constituídas por unidades básicas configuradas em nós representando cada sujeito – pessoa física ou jurídica – conectados uns aos outros, formando novos nós em uma rede de relações. Esses nós no contexto dos SRSOs são representados por perfis que identificam cada usuário, por meio de particularidades, gostos e interesses.

Todavia, nem sempre o sujeito tem a percepção sobre quão frágil a segurança de seus dados está em um processo deste tipo, excluindo-se questões de *hackeamento* ou a exploração de brechas de acesso aos dados nos serviços.

Não compreende a fragilidade quanto à segurança de dados pessoais em função da possibilidade de interações indiretas. Assim como no fator *Compartilhamento de dados e quebra de confidencialidade* do Quadro 3, nós indiretos da rede (aqueles que não se relacionam diretamente ao perfil do sujeito) pode acabar tendo acesso aos dados pessoais e conteúdo veiculado do sujeito.

Ou seja, os SRSOs não estão no domínio privado do sujeito: se um conteúdo é veiculado pelo sujeito em um SRSO, ele pode ser facilmente copiado e replicado a uma rede indireta de sujeitos, mesmo que por meio de um *print-screen*. Percebe-se que qualquer que seja a ação de um sujeito, o resultado poderá permitir interações não previstas e, conseqüentemente, se tornar parte de ações de vigilância.

As funcionalidades dos SRSOs também são capazes de transformar suas experiências nesses ambientes em algo dinâmico (*e.g.* segmentar fotografias relacionadas somente a um

evento ou local de visitação), mas também ser utilizada como ferramenta de monitoramento, criando bolhas e câmaras de eco, ou seja, segmentando sujeitos que compartilham as mesmas ideias e posicionamentos, interferindo no comportamento dos sujeitos. Isso é potencialmente prejudicial ao sujeito devido à quantidade de dados circulante nos SRSOs, que é expressiva.

Por outro lado, essa dinamicidade se traduz na divulgação, armazenamento e compartilhamento de fatos do cotidiano. Alguns SRSOs possuem funcionalidades específicas para segmentação de público, tais como: a marcação de locais, o registro de onde as imagens fora captado, a marcação de amigos que podem visualizá-las ou que participaram da atividade, a possibilidade de criação de histórias nas imagens ou em vídeos, a inserção de *emojis*, de textos, de reações, de *hashtags*, de comentários, entre outros. Isso é um processo novo de produção de conteúdo, que permite ao sujeito elaborar conteúdos específicos para um determinado público ou para um local.

Portanto, o impacto que as funcionalidades provocam aos detentores e aos sujeitos caminham em sentido contrário. Enquanto para os detentores resulta em expansão na coleta de dados e no monitoramento – captados por algoritmos – para o sujeito haverá reflexos na forma de se entreter, na interação com outros sujeitos e no compartilhamento e no acesso a assuntos que impliquem diretamente no bem-estar e na forma se comportam em relação a temas de interesse coletivo. Contudo, os sujeitos podem não perceber quaisquer ações vinculadas a vigilância por parte de quem realiza o monitoramento de dados gerados por meio dessas funcionalidades.

Por fim, a vigilância tem relação com o nível de confidencialidade. Alguns autores discutem que além dos detentores dos SRSOs – que são os principais responsáveis pelo monitoramento de dados e tem total acesso aos dados pessoais – existem instituições públicas vinculadas ao Estado como potenciais agentes com interesse na realização da vigilância e na coleta de dados. Novamente, o sujeito acaba por ter a falsa sensação que pode controlar o acesso aos seus dados pessoais, restringindo-os a outros sujeitos participantes, quando os detentores dos SRSOs poderão, por força de lei, compartilhar os dados pessoais com instituições públicas. Em países não democráticos, isto pode ser fator-chave para ações de vigilância de seus cidadãos.

## **5 CONSIDERAÇÕES FINAIS**

Para atender ao objetivo da pesquisa buscou-se indicar alguns fatores que trouxessem reflexões acerca da coleta de dados pessoais, privacidade e vigilância em SRSOs, abordados nas publicações da Ciência da Informação.

Sobre a coleta de dados pessoais, percebeu-se que os SRSOs são locais estimulados para maximizar o tempo de permanência do sujeito. Este tempo de permanência, associado com um público cada vez maior de usuários dos serviços, há um ambiente propício a coleta de dados pessoais e metadados agregados, que podem aumentar a carga semântica dos dados como, por exemplo, identificar sujeitos, locais, reações, dispositivos móveis e redes de acesso.

Ao sujeito, fica obrigatório o aceite aos Termos do Serviço, sem a possibilidade de aceite parcial, sendo que as ações de acesso e de compartilhamento que serão realizadas com seus dados pessoais ficam ofuscadas em documentos com linguagem técnica e jurídica.

Também se estimula os sujeitos a interagirem com os conteúdos. Por parte dos sujeitos, as interfaces dos SRSOs são sofisticadas, ao permitir comentar, reagir e compartilhar conteúdos circulantes. Todavia, os detentores dos SRSOs utilizam destes dados pessoais para gerar uma monetização, transformando estas interações em lucro para detentores e parceiros comerciais. Para isso, os SRSOs investem em mecanismos sofisticados de identificação de dados pessoais, aonde os sujeitos ficam suscetíveis a sua identificação em outros contextos fora do serviço, por meio de algoritmos que utilizam seus dados pessoais coletados para identificar e segmentar públicos, compartilhando parte dos dados e análises com parceiros comerciais.

Sobre os aspectos inerentes a privacidade dos dados pessoais coletados, os principais avanços identificados nas publicações foram quatro fatores. A diluição entre os ambientes públicos e privados, no qual os detentores de SRSOs permitem a exposição de dados pessoais internamente e a terceiros, mas os sujeitos têm dificuldade em compreender que o ambiente dos SRSOs é um ambiente público, mesmo quando sua conta de usuário tem o perfil privado.

Agrava-se este comportamento dos detentores, pois os SRSOs possuem uma facilidade e velocidade ímpar no ato de compartilhamento de dados, o que pode impactar o sujeito em perder o controle sobre dados pessoais veiculados, pois o compartilhamento neste contexto tem característica viral. Além disso, os SRSOs podem permitir um acesso a dados pessoais não autorizado ou consentido a terceiros, não de forma deliberada. Um exemplo é a possibilidade de realizar *print-screens* de conteúdos e compartilhar com sujeitos fora da rede. Soma-se a isso as diferentes percepções sobre a privacidade dos sujeitos participantes, que podem ou não considerar certas ações como uma violação a privacidade de seus dados.

Os SRSOs permitem a criação de perfis falsos ou de *multi-perfis*, sendo que este tipo de possibilidade gera uma série de problemas, tais como: propagação de discursos de ódio, *hackeamento* de dados, falsidade ideológica e vazamento de dados.

Por último, relaciona-se a coleta de dados e a privacidade a um processo de vigilância dos sujeitos, em quatro fatores. Como todo aplicativo de dispositivo móvel, os SRSOs podem utilizar diversos sensores para uma maior coleta de dados e metadados do sujeito. Ao mesmo tempo, os dispositivos móveis permitem uma interação célere entre os sujeitos, combinado ao acesso à internet, para o compartilhamento de dados pessoais. Trata-se de uma situação cotidiana.

Os SRSOs são elaborados para manter um ambiente motivador à interação entre sujeitos ou grupos de sujeitos, por meio do estabelecimento de redes de relações, diretas e indiretas. Porém, os sujeitos não compreendem a fragilidade quanto à segurança de dados pessoais em função da possibilidade de interações indiretas (como os *print-screens*).

Este processo gera uma quantidade significativa de dados pessoais, no qual os SRSOs se aproveitam da maior produção e circulação de dados, permitindo melhores condições de monitoramento dos sujeitos, interferindo no comportamento dos sujeitos. Ao mesmo tempo, estas funcionalidades resultam um comportamento dos sujeitos em utilizar os serviços como meios de divulgação, armazenamento e compartilhamento de fatos do cotidiano. Os SRSOs têm acesso total e controle sobre os dados, mas o sujeito tem a falsa sensação que pode controlar o acesso aos seus dados pessoais, restringindo-os a outros sujeitos participantes.

Em síntese, nas publicações analisadas é possível associar parcialmente os SRSOs ao Panóptico de Bentham (2008). Por exemplo, os SRSOs são serviços com grandes concentrações humanas em que sujeitos passam um longo período diário de tempo, não em prisões, mas nas telas de dispositivos móveis. São monitorados pelos detentores dos SRSOs que possuem um papel semelhante ao da ficção, mas em vez de um mecanismo único de vigilância, são dotados de diversos e sofisticados mecanismos capazes de monitorar bilhares de pessoas simultaneamente. É possível entender que os detentores de SRSOs estão numa tarefa muito mais confortável do que na ficção, pois são auxiliados pelos algoritmos e se utilizam de mecanismos capazes de acelerar e serem mais eficientes no processo de vigilância, de captura e de decifração de dados pessoais.

As formas de controle descritas por Foucault (2014) e por Orwell (2009), a partir da disciplina, e no Panóptico de Bentham (2008), a partir da vigilância, possuem um contexto diferente nos SRSOs. São formas de controle silenciosas e invisíveis, mas também visam controlar o comportamento humano de formas variadas. Os sujeitos podem não ter conhecimento do que ocorre com seus dados pessoais. Não sabem quando, como e quem possui acesso aos dados pessoais coletados.

Já em uma perspectiva contemporânea, considera-se que nas publicações analisadas os sujeitos não tem controle pleno dos processos de coleta de dados pessoais, o que pode acarretar problemas de privacidade e uma possível vigilância, sendo um tema que se aproxima das formas de controle verificadas por Bauman (2014), no qual o sujeito abre mão da privacidade e de domínio de seus dados pessoais em troca de entretenimento e do consumismo.

Considera-se que a pesquisa atingiu o objetivo proposto, resolvendo o problema de pesquisa, ao trazer a luz as principais observações e inquietações sobre a temática na Ciência da Informação. Porém, é importante aprofundar o tema, especialmente pelas limitações de idioma (somente em língua portuguesa) e da quantidade de produção científica da amostra. Uma forma de aprofundamento é dirigir um estudo comparativo entre publicações em diferentes idiomas, para a verificação de formas internacionais de entendimento sobre o tema, a partir de resultados de pesquisa de pesquisadores vinculados a instituições em outros países.

## REFERÊNCIAS

AMARAL FILHO, O.; BLANCO, D. D. R. 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, 30 out. 2014. DOI: 10.15448/1980-3710.2014.1.14910. Disponível em:

<http://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/14910>. Acesso em: 13 nov. 2024.

ASSUMPCÃO, F. S.; SANTANA, R. C. G.; SANTOS, P. L. V. A. D. C. 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, 17 set. 2015. DOI: 10.19132/1808-5245212.31-48. Disponível em: <https://www.seer.ufrgs.br/index.php/EmQuestao/article/view/54545>. Acesso em: 13 nov. 2024.

BARRIGA, A. D. C. A publicitação do privado na era da pós-verdade: uma exploração às redes sociais dos líderes políticos portugueses. **Observatorio (OBS\*)**, v. 14, n. 2, p. 56–71, 2 jun. 2020. DOI: 10.15847/obsOBS14220201609. Disponível em:

<https://obs.obercom.pt/index.php/obs/article/view/1609>. Acesso em: 13 nov. 2024.

BAUMAN, Z.; LYON, D. **Vigilância líquida**. 1. ed. Rio de Janeiro, Brazil: Zahar, 2014. 160 p. ISBN: 978-85-378-1156-6.

BENTHAM, J. **O panóptico**. Tradução: Tomaz Tadeu. 2. ed. São Paulo, Brasil: Autêntica, 2008. 180 p. ISBN:978-85-86583-75-9.

BITTENCOURT, M. C. A.; GONZATTI, C.; ESMITIZ, F. De Rainha dos Baixinhos à Rainha dos Memes: o humor como vetor de cibercontecimentos a partir da ida de Xuxa da Rede Globo para a Rede Record. **Sessões do Imaginário**, v. 20, n. 34, p. 81–90, 16 fev. 2016. DOI: 10.15448/1980-3710.2015.2.20546. Disponível em:

<http://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/20546>. Acesso em: 13 nov. 2024.

BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. DE A. **Proteção de Dados e Privacidade**. 1ª edição ed. Rio de Janeiro, Brasil: Lumen Juris, 2018. 258 p. ISBN: 978-85-519-0840-2.

BORGES, M. T. Mercado, vigilância e Facebook na era do espetacular integrado, ou inside us all there is a code. **Literatura: teoria, história, crítica**, v. 22, n. 1, p. 137–178, 1 jan. 2020.

DOI: 10.15446/lthc.v22n1.82295. Disponível em:

<https://revistas.unal.edu.co/index.php/lthc/article/view/82295>. Acesso em: 13 nov. 2024.

BOYD, D.; ELLISON, N. Social Network Sites: Definition, History, and Scholarship.

**Journal of Computer-Mediated Communication**, v. 13, n. 1, p. 210–230, out. 2007. DOI:

10.1111/j.1083-6101.2007.00393.x. Disponível em: [http://doi.wiley.com/10.1111/j.1083-](http://doi.wiley.com/10.1111/j.1083-6101.2007.00393.x)

[6101.2007.00393.x](http://doi.wiley.com/10.1111/j.1083-6101.2007.00393.x). Acesso em 10 nov. 2024.

CETIC.BR. **TIC Domicílios – 2023**. Brasil: Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, 2023. Disponível em:

<https://cetic.br/pt/pesquisa/domicilios/indicadores/>. Acesso em: 8 nov. 2024.

COMIN, E. R. *et al.* Investigando o fenômeno de compras coletivas on-line: fatores que influenciam a intensidade das compras. **Revista de Administração da UFSM**, v. 7, n. 2, p. 196–213, 8 jun. 2014. DOI: 10.5902/198346597084. Disponível em:

<https://periodicos.ufsm.br/reaufsm/article/view/7084>. Acesso em: 13 nov. 2024.

CONFORTO, E. C.; AMARAL, D. C.; SILVA, S. L. da. Roteiro para revisão bibliográfica sistemática: aplicação no desenvolvimento de produtos e gerenciamento de projetos. Anais do 8º Congresso Brasileiro de Gestão de Desenvolvimento de Produto. **Anais...** Em: 8º CONGRESSO BRASILEIRO DE GESTÃO DE DESENVOLVIMENTO DE PRODUTO. Porto Alegre, Brazil: Escola de Engenharia de São Carlos, Universidade de São Paulo, 2011. Disponível em: <https://repositorio.usp.br/item/002833837>. Acesso em: 9 nov. 2024.

CRUZ, R. do C.; ARAÚJO, C. A. Á. Sujeito informacional, conceito em emergência: uma revisão teórico-conceitual de periódicos Ibero-Americanos. **Informação & Sociedade**, v. 30, n. 1, p. 1–22, 10 mar. 2020. DOI: <https://doi.org/10.22478/ufpb.1809-4783.2020v30n1.43934>. Disponível em: <https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/43934>. Acesso em: 09 nov. 2024.

DATA.AI. **Social Media Time Spent**. San Francisco, Estados Unidos da América: Sensor Tower, 2024. Disponível em: <https://www.data.ai/>. Acesso em: 11 nov. 2024.

FOUCAULT, M. **Vigiar e punir: Nascimento da prisão**. Tradução: Raquel Ramallete. 42. ed. Petrópolis, Brasil: Editora Vozes, 2014. 296 p. ISBN: 978-85-326-0508-5.

FRANÇA, T. C. *et al.* **Big Social Data: Princípios sobre Coleta, Tratamento e Análise de Dados Sociais**. Em: LÓSCIO, B. F.; MARTINS, V.; HARA, C. S. (Eds.). **Tópicos em Gerenciamento de Dados e Informações 2014**. 1. ed. Curitiba: Sociedade Brasileira de Computação, 2014. p. 8–45. ISBN: 978-85-7669-290-4.

FREIRE, I. M. Barreiras na comunicação da informação tecnológica. **Ciência da Informação**, v. 20, n. 1, p. 51–54, 1991. DOI: 10.18225/ci.inf..v20i1.416. Disponível em: <http://revista.ibict.br/ciinf/article/view/416>. Acesso em: 14 nov. 2024.

FUGAZZA, G. Q.; SALDANHA, G. S. 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, 27 dez. 2018. DOI: 10.5433/1981-8920.2018v23n3p462. Disponível em:

<https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/28108>. Acesso em: 13 nov. 2024.

HAGE, Z. C. M.; KUBLIKOWSKI, I. Estilos de uso e significados dos autorretratos no Instagram: Identidades narrativas de adultos jovens brasileiros. **Estudos e Pesquisas em Psicologia**, v. 19, n. 2, p. 522–539, ago. 2019. Disponível em:

[http://pepsic.bvsalud.org/scielo.php?script=sci\\_abstract&pid=S1808-42812019000200011&lng=pt&nrm=iso&tlng=pt](http://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1808-42812019000200011&lng=pt&nrm=iso&tlng=pt). Acesso em: 13 nov. 2024.

IBGE. **Panorama do censo 2022**. Brasília, Brasil: Instituto Brasileiro de Geografia e Estatística, 2022. Disponível em: <https://censo2022.ibge.gov.br/panorama/>. Acesso em: 12 nov. 2024.

JURNO, A. C.; D'ANDRÉA, C. F. D. B. (In)Visibilidade Algorítmica no “Feed De Notícias” do Facebook. **Contemporânea Revista de Comunicação e Cultura**, v. 15, n. 2, p. 463–484, 10 nov. 2017. DOI: 10.9771/contemporanea.v15i2.17796. Disponível em:

<https://periodicos.ufba.br/index.php/contemporaneaposcom/article/view/17796>. Acesso em: 13 nov. 2024.

LEITZKE, A. T. D. S.; RIGO, L. C. Sociedade de controle e redes sociais na internet: #saúde e #corpo no instagram. **Movimento (ESEFID/UFRGS)**, v. 26, p. e26062, 20 ago. 2020. DOI: 10.22456/1982-8918.100688. Disponível em:

<https://seer.ufrgs.br/Movimento/article/view/100688>. Acesso em: 13 nov. 2024.

LIMA, L. D. A. Diretrizes para aperfeiçoamento e interpretação da lei do marco civil da internet com vistas à garantia do direito à privacidade nas redes sociais. **Prisma Jurídico**, v. 17, n. 1, p. 59–81, 3 jul. 2018. DOI: 10.5585/prismaj.v17n1.8084. Disponível em:

[http://periodicos.uninove.br/index.php?journal=prisma&page=article&op=view&path\[\]=8084](http://periodicos.uninove.br/index.php?journal=prisma&page=article&op=view&path[]=8084). Acesso em: 13 nov. 2024.

MARTORELL, L. B.; NASCIMENTO, W. F. D.; GARRAFA, V. 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, 3 nov. 2015. DOI: 10.1590/1807-57622014.0902. Disponível em:

[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1414-32832016000100013&lng=pt&tlng=pt](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1414-32832016000100013&lng=pt&tlng=pt). Acesso em: 13 nov. 2024.

MENDES-CAMPOS, C.; FÉRES-CARNEIRO, T.; MAGALHÃES, A. S. Intimidade e Extimidade Virtual na Conjugalidade Contemporânea. **Interação em Psicologia**, v. 19, n. 3, p. 407–416, 9 nov. 2016. DOI: 10.5380/psi.v19i3.34887. Disponível em:

<http://revistas.ufpr.br/psicologia/article/view/34887>. Acesso em: 13 nov. 2024.

NOVO, R.; AZEVEDO, M. M. de. A percepção de vulnerabilidade e aplicação ética das informações nas redes soaicis pelos sisemas de *big data*. **Tekhne e Logos**, v. 5, n. 2, p. 64–78, 11 dez. 2014. Disponível em: <http://revista.fatecbt.edu.br/index.php/tl/article/view/298>. Acesso em: 11 nov. 2024.

ORWELL, G. **1984**. Tradução: Alexandre Hubner. 1 ed. São Paulo, Brasil: Companhia das Letras, 2009.

PURIM, K. S. M.; TIZZOT, E. L. A. Protagonismo dos Estudantes de Medicina no Uso do Facebook na Graduação. **Revista Brasileira de Educação Médica**, v. 43, n. 1, p. 187–196, mar. 2019. DOI: 10.1590/1981-52712015v43n1rb20180139. Disponível em:

[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0100-55022019000100187&tlng=pt](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-55022019000100187&tlng=pt). Acesso em: 13 nov. 2024.

REBS, R. R. O excesso no discurso de ódio dos haters. **Fórum Linguístico**, v. 14, p. 2512–2523, 24 nov. 2017. DOI: 10.5007/1984-8412.2017v14nespp2512. Disponível em: <https://periodicos.ufsc.br/index.php/forum/article/view/1984-8412.2017v14nespp2512>. Acesso em: 13 nov. 2024.

RECUERO, R. **Redes sociais na internet**. 2. ed. Porto Alegre, Brazil: Editora Sulina, 2014.

RODRIGUES, F. A. **Estruturas de dados em serviços de redes sociais online: uma abordagem metodológica de análise**. Marília/São Paulo: Oficina Universitária e Cultura Acadêmica, 2024a. 312 p. ISBN: 978-6-559-54469-1.

RODRIGUES, F. A.; SANT'ANA, R. C. G. Contextualização de conceitos teóricos no processo de coleta de dados de Redes Sociais Online. **Informação & Tecnologia**, v. 5, n. 1, p. 18–36, 2018. DOI: 10.22478/ufpb.2358-3908.2018v5n1.38077. Disponível em: <https://periodicos.ufpb.br/index.php/itec/article/view/38077>. Acesso em: 14 nov. 2024.

RODRIGUES, L. B. **Mapeamento e Categorização de Comunicações Científicas para a Construção de Portfólio de Propostas para Conceitos sobre Rede Social**. Dissertação (Mestrado em Ciência da Informação) – Instituto de Ciências Sociais Aplicadas, Universidade Federal do Pará, Belém, 2024b. 236 f.

SANCHOTENE, C.; SILVEIRA, A. C. M. da; LAVARDA, S. D. L. Quando as notícias mais compartilhadas são falsas: a circulação de boatos durante a semana do impeachment no Facebook. **Comunicação & Informação**, v. 20, n. 3, p. 99–112, 31 dez. 2017. DOI: 10.5216/ci.v20i3.46950. Disponível em: <https://www.revistas.ufg.br/ci/article/view/46950>. Acesso em: 12 nov. 2024.

VALENTE, J. C. L. **Tecnologia, informação e poder: das plataformas online aos monopólios digitais**. 2019a. Tese (Doutorado em Sociologia) - Instituto de Ciências Sociais, Universidade de Brasília, Brasília, 2019a. 339 f.

ROSADO, L. A. D. S.; TOMÉ, V. M. N. As redes sociais na internet e suas apropriações por jovens brasileiros e portugueses em idade escolar. **Revista Brasileira de Estudos Pedagógicos**, v. 96, n. 242, p. 11–25, abr. 2015. DOI: 10.1590/S2176-6681/324612565. Disponível em: [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S2176-66812015000100011&lng=pt&tlng=pt](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2176-66812015000100011&lng=pt&tlng=pt). Acesso em: 13 nov. 2024.

SÁ, F. P. D. Pesquisando co-viewing em redes sociais e aplicativos de mensagem instantânea: ética e desafios. **Comunicação e Sociedade**, v. 33, p. 391–408, 29 jun. 2018. DOI: 10.17231/comsoc.33(2018).2923. Disponível em: <https://revistacomsoc.pt/article/view/1071>. Acesso em: 13 nov. 2024.

SANTOS, V. S. DOS; PORTO, E.; ALTURAS, B. A. B. Análise de mecanismos de controle de acesso nas redes sociais. **Revista Portuguesa e Brasileira de Gestão**, v. 9, n. 3, p. 50–60, 11 jul. 2010. Disponível em: <https://hml-bibliotecadigital.fgv.br/ojs/index.php/rbpg/article/view/78824>. Acesso em: 13 nov. 2024.

SOLOVE, D. J. **Understanding privacy**. First Harvard University Press paperback edition ed. Cambridge: Harvard University Press, 2009. 257 p. ISBN: 978-0-674-03507-2.

STATISTA. **Global daily social media usage Q1 2023, by territory**. Hamburgo: Statista, 9 out. 2024. Disponível em: <https://www.statista.com/statistics/270229/usage-duration-of-social-networks-by-country/>. Acesso em: 9 nov. 2024.

STRECK, M.; PELLANDA, E. C. Instagram como interface da comunicação móvel e ubíqua. **Sessões do Imaginário**, v. 22, n. 37, p. 10–19, 10 set. 2017. DOI: 10.15448/1980-3710.2017.1.28017. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/view/28017>. Acesso em: 13 nov. 2024.

THIBES, M. Z. 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, dez. 2017. DOI: 10.1590/15174522-019004613. Disponível em: [http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S1517-45222017000300316&tlng=pt](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-45222017000300316&tlng=pt). Acesso em 13 nov. 2024.

VALENTE, J. C. L. **Tecnologia, informação e poder: das plataformas online aos monopólios digitais**. 2019a. Tese (Doutorado em Sociologia) - Instituto de Ciências Sociais, Universidade de Brasília, Brasília, 2019a. 339 f.

VALENTE, J. C. L. Algoritmos e Sites de Redes Sociais: uma discussão crítica sobre o caso do Facebook. **Pós – Revista Brasileira de Pós-Graduação em Ciências Sociais**, v. 14, n. 2, p. 87–113, 4 ago. 2019b. Disponível em: <https://periodicos.unb.br/index.php/revistapos/article/view/26491>. Acesso em: 12 nov. 2024.

VAN DIJCK, J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, p. 197–208, 9 maio 2014. DOI: 10.24908/ss.v12i2.4776. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication>. Acesso em: 11 nov. 2024.

WESTIN, A. F. **Privacy and freedom**. 1. ed. Londres: The Bodley Head Ltd, 1970.

## APÊNDICE A – Publicações analisadas

Ano	Autor(es)	Título	Periódico	Núm.	Vol.
2010	Santos, Vinicius Souza dos; Porto, Ed; Alturas, Bráulio Alexandre Barreira	Análise de mecanismos de controle de acesso nas redes sociais	Revista Portuguesa e Brasileira de Gestão	3	9
2014	Amaral Filho, Otacílio; Blanco, Danielle Dos Reis	O Espetáculo Cultural na rede social: A abordagem midiática do Coletivo Dirigível de teatro na Rede Social Digital <i>Facebook</i>	Sessões do Imaginário	31	19
2014	Comin, Everton Roberto; Teixeira, Rafael; Durayski, Juliana; Silva, Natália Gomes Da; Vieira, Julio	Investigando o fenômeno de compras coletivas on-line: fatores que influenciam a intensidade das compras	Revista de Administração da UFSM	2	7
2015	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	21	2

Ano	Autor(es)	Título	Periódico	Núm.	Vol.
2015	Martorell, Leandro Brambilla; Nascimento, Wanderson Flor Do; Garrafa, Volnei	Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no <i>Facebook</i>	Interface - Comunicação, Saúde, Educação	56	20
2015	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	242	96
2016	Aquino Bittencourt, Maria Clara; Gonzatti, Christian; Esmitz, Francielle	De Rainha dos Baixinhos à Rainha dos Memes: o humor como vetor de cibercontecimentos a partir da ida de Xuxa da Rede Globo para a Rede <i>Record</i>	Sessões do Imaginário	34	20
2016	Mendes-Campos, Carolina; Féres-Carneiro, Terezinha; Magalhães, Andrea Seixas	Intimidade e Extimidade Virtual na Conjugalidade Contemporânea	Interação em Psicologia	3	19
2017	Jurno, Amanda Chevtchouk; D'Andréa, Carlos Frederico De Brito	(In)Visibilidade Algorítmica no “ <i>Feed</i> de Notícias” do Facebook	Contemporânea Revista de Comunicação e Cultura	2	15
2017	Rebs, Rebeca Recuero	O excesso no discurso de ódio dos <i>haters</i>	Fórum Linguístico	-	14
2017	Streck, Melissa; Pellanda, Eduardo Campos	Instagram como interface da comunicação móvel e ubíqua	Sessões do Imaginário	37	22
2017	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	46	19
2018	Fugazza, Grace Quaresma; Saldanha, Gustavo Silva	A questão do direito à privacidade no <i>Facebook</i> : um estudo à luz da ética da informação	Informação & Informação	3	23
2018	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	1	17
2018	Sá, Fernanda Pires De	Pesquisando <i>co-viewing</i> em redes sociais e aplicativos de mensagem instantânea: ética e desafios	Comunicação e Sociedade	-	33
2019	Hage, Zakiee Castro Mufarrej; Kublikowski, Ida	Estilos de uso e significados dos autorretratos no <i>Instagram</i> : Identidades narrativas de adultos jovens brasileiros	Estudos e Pesquisas em Psicologia	2	19
2019	Purim, Kátia Sheylla Malta; Tizzot, Edison Luiz Almeida	Protagonismo dos Estudantes de Medicina no Uso do <i>Facebook</i> na Graduação	Revista Brasileira de Educação Médica	1	43
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*)	2	14
2020	Borges, Mariana Toledo	Mercado, vigilância e <i>Facebook</i> na era do espetacular integrado, ou <i>inside us all there is a code</i>	Literatura: teoria, história, crítica	1	22
2020	Leitzke, Angélica Teixeira Da Silva; Rigo, Luiz Carlos	Sociedade de controle e redes sociais na internet: #saúde e #corpo no <i>Instagram</i>	Movimento (ESEFID/UFRGS)	-	26

Fonte: Elaborado pelos Autores (2024).