

ARIADNE CHLOE MARY FURNIVAL

**A COMPETÊNCIA DIGITAL NO CONTEXTO DO USO SEGURO E PRIVADO DA INTERNET:  
UMA REVISÃO DE LITERATURA**

Relatório de Pós-doutorado realizado na  
Universidade Estadual Paulista (UNESP),  
Faculdade de Filosofia e Ciências, Marília.

Supervisora: Profa. Dra. Helen de Castro  
Silva Casarin

Marília

2025

RELATÓRIO Pós-Doutorado

## **A competência digital no contexto do uso seguro e privado da Internet: uma revisão da literatura**

**Ariadne Chloe Mary Furnival**

Supervisionado pela Profa. Dra. Helen de Castro Silva Casarin  
UNESP-Marília

São Carlos, out. 2024



## Lista de Figuras, Gráficos, Quadros, Tabelas

Figura 1 – Quantidade de registros recuperados na WoS, Scopus, LISA e Google Acadêmico para “information literacy”, de 2003 a 2024	p.9
Figura 2 - <i>International Journal of Digital Literacy and Digital Competence</i> (open access desde 2023)	p.10
Figura 3 – <i>Nordic Journal of Digital Literacy</i> (open access)	p.10
Figura 4 – Expressão de busca da pesquisa na WoS	p.38
Figura 5 – Expressão de busca da pesquisa na SCOPUS	p.39
Figura 6 – Expressão de busca da pesquisa na LISA	p.39
Figura 7 – Expressão de busca da pesquisa na Dimensions	p.40
Gráfico 1 – Abstracts com a frequência de $\geq 2$ o termo “digital_literacy”	p.42
Quadro 1 – Diferenças entre os três tipos comuns de revisão	p.35-6
Quadro 2 – Termos em formato aceitável para o software Iramuteq	p.41
Quadro 3 – Metadados dos 16 artigos que mais atendem aos critérios da expressão de busca	p.43-4
Quadro 4 – Agrupamento temático dos artigos recuperados	p.45-6
Tabela 1 – Total de registros recuperados, sem duplicatas	p.40
Tabela 2 – Frequência dos termos-chave em 20 Resumos ( <i>Abstracts</i> )	p.42-3
Tabela 3 - Autoavaliação do nível de experiência em mídia digital e conhecimento sobre ameaças eletrônicas	p.58

## SUMÁRIO

Apresentação: Atividades desenvolvidas durante o período pós-doutoral	p.1
1. Introdução	p.5
2. Evolução do conceito de competência digital – digital literacy	p.12
3. Privacidade e segurança online	p.23
3.1 Paradoxo da privacidade	p.31
4. Procedimentos metodológicos adotados	p.33
5. Análise dos resultados	p.47
5.1 Revisão dos artigos recuperados	p.49
5.1.1 Crianças, adolescentes, jovens	p.49
5.1.2 Professores e competência digital	p.57
5.1.3 Universitários e competência digital visando a privacidade e segurança	p.61
5.1.4 Idosos e competência digital para segurança online	p.65
5.1.5 Cidadãos e competência digital para a segurança online	p.69
6. Considerações finais	p.74
7. Referências	p.77

Apêndice A – Planilha Excel dos metadados 83 registros finais depois da remoção de duplicatas

Apêndice B – Corpus dos *Abstracts* para Iramuteq

Anexo A – Carta University of Sheffield

Anexo B – Certificado curso POCA

## Resumo

Habitamos sociedades nas quais pouco ou nada permanece intocado pelas tecnologias digitais, onde a fronteira entre online e offline está se tornando cada vez mais tênue – *onlife* nos termos de Floridi. A privacidade e a segurança online, no entanto, tornaram-se requisitos de rotina para todos os usuários de computadores, dispositivos móveis e do software e aplicativos que eles suportam. Governos ao redor do mundo têm reconhecido a gravidade das violações de segurança online, tanto para instituições governamentais, indústrias e corporações privadas na forma de ataques cibernéticos massivos, quanto principalmente para cidadãos na forma de golpes, phishing, violações de dados, propagação de malware e quebra de senhas por atores maliciosos. Este cenário suscita a necessidade de iniciativas para o desenvolvimento contínuo de competências digitais e competência em informação. A capacidade de navegar pelos benefícios e riscos da conectividade digital depende, em grande parte, da competência digital. No entanto, há uma relativa falta de literatura sobre competência digital/*digital literacy* que foca na segurança e privacidade online, falta essa que moveu a pesquisa aqui relatada. Diante do exposto, a pesquisa teve como objetivo geral realizar uma revisão sistematizada da literatura científica e cinzenta acerca dos temas que se interseccionam: competência digital e segurança e privacidade online. A pesquisa teve como questão norteadora: Qual é o estado de literatura dos estudos da área de competência digital em relação à segurança e privacidade online nos últimos cinco anos (2019-2024)? Quais são os conceitos propostos pelos estudos das áreas de competência digital (*digital literacy*) nos últimos cinco anos? No mesmo período, quais foram as abordagens e enquadramentos do problema de segurança e privacidade online na literatura? Os objetivos específicos foram: 1. Analisar, diferenciar e discutir os termos e conceitos de competência digital como aparecem na literatura identificada; 2. Levantar e descrever a literatura (incluindo a literatura cinzenta) dos últimos cinco anos que trata dos temas competência digital em relação à privacidade e segurança online; 3. Fazer destaque sobre os principais achados e informações novas e relevantes dentre os estudos levantados para poder traçar novas perspectivas para a Ciência da Informação. Esta pesquisa é exploratória com abordagem quali-quantitativa, com base na coleta, análise e síntese de documentos escritos. Os metadados dos 83 documentos coletados (cobrindo o intervalo de tempo de 2019 a 2024) das bases de dados Scopus, Web of Science, Dimensions e LISA foram organizados em planilhas Excel e filtrados por relevância temática usando o software IramuTeq, reduzindo a quantidade a ser estudado para 16 artigos. Para analisar a abordagem do tema de competência digital visando a segurança e privacidade online de grupos específicos, os 16 artigos foram agrupados em 5 categorias mais amplas: Crianças e adolescentes e jovens; Universitários; Professores; Idosos e Cidadãos. A análise foi descritiva e interpretativa, adotando-se também uma perspectiva comparativa do fenômeno sob estudo, dada a natureza internacional das fontes coletadas. Esta pesquisa projetou-se como um esforço teórico-reflexivo, visando abrir espaço para subsidiar o desenvolvimento de mais pesquisas, inclusive empíricas, que relacionem as temáticas de competência digital com a privacidade e segurança online, fomentando o diálogo e possíveis parcerias para a realização de levantamentos empíricos futuros.

**Palavras-chave:** competência digital; segurança online; privacidade online; infoesfera; revisão sistematizada da literatura.

## Abstract

We inhabit societies in which little or nothing remains untouched by digital technologies, where the boundary between online and offline is becoming increasingly blurred – “onlife” in Floridi's terms. Online privacy and security, however, have become routine requirements for all users of computers, mobile devices and the software and applications they support. Governments around the world have recognized the seriousness of online security breaches, both for government institutions, industries and private corporations in the form of massive cyber attacks, and especially for citizens in the form of scams, phishing, data breaches, the spread of malware and password cracking by malicious actors. This scenario raises the need for initiatives to continuously develop digital skills and information competence. The ability to navigate the benefits and risks of digital connectivity depends to a large extent on digital competence. However, there is a relative lack of literature on digital competence/digital literacy that focuses on online security and privacy, a lack that prompted the research reported here. In view of the above, the general aim of the research was to carry out a systematized review of the scientific and grey literature on the intersecting themes of digital competence and online security and privacy. The research's guiding question was: What is the state of the literature of studies in the area of digital competence in the period of 2019-2024? What concepts have been proposed by studies in the area of digital competence (digital literacy) over the last five years? In the same period, what were the approaches and framings of the problem of online security and privacy in the literature? The specific objectives were: 1. to analyze, differentiate and discuss the terms and concepts of digital competence as they appear in the identified literature; 2. to survey and describe the literature (including grey literature) of the last five years that deals with the themes of digital competence in relation to online privacy and security; 3. to highlight the main findings and new and relevant information among the studies surveyed in order to draw up new perspectives for Information Science. This is an exploratory study with a qualitative-quantitative approach, based on the collection, analysis and synthesis of written documents. The metadata of the 83 documents collected (covering the time interval from 2019 to 2024) from the Scopus, Web of Science, Dimensions and LISA databases was organized in Excel spreadsheets and filtered by thematic relevance using the IramuTeq software, reducing the quantity to be studied to 16 articles. In order to analyze the approach to the topic of digital competence aimed at the online safety and privacy of specific groups, the 16 articles were grouped into 5 broader categories: Children and adolescents and young people; University students; Teachers; Senior citizens and Citizens. The analysis was descriptive and interpretative, adopting also a comparative perspective of the phenomenon under study, given the international nature of the sources collected. This research was designed as a theoretical-reflective effort, with the aim of opening up space to support the development of further research, including empirical research, relating the themes of digital competence to online privacy and security, fostering dialogue and possible partnerships for future empirical surveys.

**Keywords:** digital competence; digital literacy; online safety; online privacy; infosphere; systematized literature review.

## **Apresentação: Atividades desenvolvidas durante o período pós-doutoral**

É inevitável, na transição da rotina de docente universitária *full-time* para pesquisadora pós-doutoral, que hajam tarefas e compromissos que sobram do período de docência. Por isso, a fase inicial do estágio pós-doutoral, com afastamento integral de um ano (sem bolsa) concedido pela minha instituição de vínculo empregatício, a Universidade Federal de São Carlos (onde estou lotada no Departamento de Ciência da Informação), foi uma de adaptação de rotina e fechamento de resquícios de tarefas. Embora pareça trivial, tal adaptação não foi trivial levando em consideração que este afastamento foi o primeiro para fins de pesquisa me concedido durante mais de 30 anos de serviço na UFSCar.

Assim, durante essa fase, continuei com algumas orientações de pós-graduação (5 mestrandas) e a fase final da orientação de um projeto de Iniciação Científica com financiamento da FAPESP (bolsa IC para a orientanda). Continuei com minha colaboração como uma das organizadores de um livro comemorando os 30 anos da Editora da UFSCar (EdUFSCar), a ser lançado neste fim de ano de 2024. Também dei prosseguimento a minha participação em uma equipe de trabalho de um projeto de extensão na UFSCar, com colegas servidoras do Sistema Integrada de Bibliotecas da UFSCar (SiBi-UFSCar) sobre usuários do Sistema. Esses dois envolvimento implicaram no máximo de 8 horas semanais, até o fim de 2023. Esporadicamente, ao longo do estágio pós-doutoral, também participei de bancas de pós-graduação, qualificações e defesas (6 no total). Continuei com a emissão de pareceres (30 no total) para eventos no Brasil, e para artigos submetidos a periódicos científicos (11 no total) e 2 pareceres para FAPESP. Prossegui com minha participação em reuniões de discussão sobre a elaboração de proposta de pesquisa para a FAPESP, em conjunção com a Profa. Helen da UNESP e Profs. David Haynes, Bruce Ryan e Peter Cruickshank da Universidade Edinburgh Napier no Reino Unido, eles apresentando via a UKRI. Recebemos a notícia em 30 de agosto que infelizmente, a proposta foi denegada. Mas deve ser ressaltado aqui o esforço de trabalho e tempo que esse tipo de submissão exige.

A pesquisa apresentado à UNESP-Marília como minha pesquisa de pós-doutorado também

foi iniciada nesses meses. O projeto original sofreu alguns ajustes, sempre após consulta e conversa com minha supervisora, Profa. Dra. Helen de Castro Silva Casarin, principalmente no que diz respeito aos procedimentos metodológicos adotados. A intenção inicial tinha sido de realizar uma revisão integrativa da literatura, mas decidimos que fosse mais apropriada de realizar um “simples” revisão da literatura. A revisão feita e apresentada no relatório, pode ser nominado como uma “revisão sistematizada da literatura”, denominação esta que detalho no Relatório.

No início de janeiro deste ano (2024), enfrentei problemas de saúde na família (que é da Inglaterra) e então, tive que ir para lá, mais especificamente para a cidade do norte do país, Sheffield. Como tive que me deslocar para aquela cidade, e como a Universidade de Sheffield possui um iSchool<sup>1</sup> de renome, e após conversa com minha supervisora, Profa. Helen, entrei em contato com uma professora e pesquisadora de lá, Dra. Pamela McKinney, para averiguar se houvesse possibilidade de forjarmos alguma colaboração, não necessariamente limitada à minha pesquisa de pós-doutorado. A professora Pamela foi muito receptiva, e a Universidade de Sheffield formalizou minha ligação com a iSchool como “Associate” por um período de 5 meses (Anexo A). Esta ligação me deu acesso às bibliotecas e às bases de dados, além de, claro, acesso aos prédios. A iSchool está localizada num prédio novíssimo e muito bonito, que se chama “*The Wave*”, por ter uma estrutura arquitetônica ondulada (de um lado dele). Enquanto conectada à iSchool da Universidade de Sheffield, participei de 5 reuniões do grupo de pesquisa “Libraries and information Society – LIS”<sup>2</sup> coordenada pela professora Sheila Webber, que foram extremamente interessantes e instigantes. Os participantes permanentes desse grupo são, além da coordenadora: Pam McKinney, Nigel Ford, Stephen Pinfield e Briony Birdi. Além dessa participação, no 4 de junho (2024), participei de uma oficina com duração de um dia, realizada entre a Information School e a School of Journalism, Media and Communication da Universidade de Sheffield (*Research Away Day Programme*) o tema da qual foi o envio de propostas de pesquisa para os principais órgãos de fomento à pesquisa. A oficina consistiu em apresentações, discussões, leituras de *cases* em grupos menores e discussões em sessão

---

<sup>1</sup> Para maiores informações sobre a rede internacional de iSchools, entre em: <https://www.ischools.org/>

<sup>2</sup> <https://www.sheffield.ac.uk/is/research/groups/libraries-information-society>

de plenário. Foi realizada num prédio que pertence à Universidade de Sheffield (Halifax Hall) mas que fica afastado dos principais prédios da universidade, para garantir foco e concentração no tema em pauta.

O contato com o pessoal da iSchool significou que pude ser a facilitadora na organização de uma palestra proferida (online) pela professora Pam McKinney, no 12 de abril (2024) como aula inaugural do PPGCI-UNESP. O título da apresentação dela foi: “Quantified Self + Community Voice: A Dual Focus of Health Information Literacy Research in Sheffield.”<sup>3</sup> Entendo que sua apresentação foi muito bem recebida pelo público, e está disponível no YouTube em: [https://www.youtube.com/watch?v=\\_5uiw8ujgSU](https://www.youtube.com/watch?v=_5uiw8ujgSU). Professora Pam ficou extremamente contente com o convite e também está muito interessada em estreitar as relações de pesquisa entre UNESP e UFSCar.

Como pós-doutoranda da UNESP, pude participar, como ouvinte, no dia 18 de abril (2024) no 1º Encontro do Programa de Pós-Doutorado da Unesp, também transmitido online via YouTube. Isto deu aos espectadores a possibilidade muito valiosa de ter conhecimento de pesquisas de pós-doutoramento já realizadas na UNESP. Também está disponível no YouTube em: <https://www.youtube.com/watch?v=1WkcuraAuP8>.

Acabei terminando a pesquisa, mas preciso frisar aqui que não foi com a dedicação mental, emocional e cognitiva – além de a dedicação de tempo – que eu tinha imaginado que eu conseguiria ter. Isto, como mencionado acima, deve-se à enfermidade de meu filho, que ainda está em curso, e será prolongada, necessitando da minha dedicação intensa.

A partir deste relatório e resultados, será elaborado pelo menos um artigo, um em co-autoria com a professora Pam McKinney da Universidade de Sheffield.

Nesse meio tempo, **as publicações que tive com minha supervisora** são as seguintes:

1. LIMA, T.A.; **FURNIVAL**, A.C.M; **CASARIN**, H.C.S.; PAGAN, M. Competência em informação na escrita acadêmica para evitar o plágio: um estudo com universitários brasileiros. **Inf. Inf.**, Londrina, v. 28, n. 3, p. 255-279, jul./set. 2023. (publicado em 2024)

---

<sup>3</sup> Com uma mudança imprevista da data previamente combinada para esta apresentação, não pude mais participar como a coordenadora de mesa, pois tive que acompanhar meu filho a uma consulta psiquiátrica na mesma data e hora.

2. DIAS, F.B.C.; **FURNIVAL**, A.C.N.; **CASARIN**, H.C.S. Desinformação e fake news: avaliação das competências de alunos do ensino superior. **AtoZ: novas práticas em informação e conhecimento**, v.13, 1-12, 2024. <http://dx.doi.org/10.5380/atoz.v13.89709>

**Outras publicações no período do estágio pós-doutoral:**

3. PEREIRA, V.; **FURNIVAL**, A. C. M. ; SILVA, S. L. . Knowledge and information management in a solidarity economy nucleus: a case study. **Information Development**, v. 40, p. 1-13, 2024.

4. ROMANIN, C. O.; **FURNIVAL**, A. C. M. . Dados Abertos para Sustentabilidade Ambiental avaliando a abertura usando FAIR e W3C. **Brazilian Journal of Information Science**, v. 18, p. 1-21, 2024.

5. COELHO FRANÇA, M; **FURNIVAL**, A. C. M. . Information behaviour of Deaf people in university libraries. **Canadian Journal of Information and Library Science-Revue Canadienne Des Sciences De L'Information Et De Bibliothéconomie**, v. 47, p. 120-127, 2024.

6. ANDRADE, T. H. N.; **FURNIVAL**, A. C. M. ; MARTINELLI, M. Mobilidade Estudantil Internacional como promotora de laços educacionais e institucionais: o caso dos Institutos Confúcio no Brasil. **PRÓ-POSIÇÕES** (UNICAMP. ONLINE), v. 35, p. 1-28, 2024.

**Submissões de manuscritos a periódicos no período do estágio pós-doutoral (aguardando pareceres):**

7. ANGELON, E.M; **FURNIVAL**, A.C.M. "Clubes de Leitura: Livremente, um estudo de caso." Submetido ao periódico **Perspectivas em Ciência da Informação** em 04/09/2024.

8. BONFIM, M.A.; **FURNIVAL**, A.C.M. "Uso da internet por universitários brasileiros pela perspectiva da segurança e privacidade: um estudo de caso" Submetido ao periódico **Ciência da Informação** em 30/07/2024.

## 1. Introdução

É fato incontestável que o mundo tem passado por extensiva e intensiva informatização, com a concomitante resultado disso sendo que todos os ramos da indústria informacional se tornando parte integral das economias nacionais enquanto simultaneamente mudando a forma com a qual as pessoas interagem com e dependem da informação no seu dia-a-dia. A informação, principalmente em formato digital, contribui diretamente para o desenvolvimento social e econômico de países: Em nenhum momento da história o bem-estar e o progresso humanos dependeram tanto da gestão eficiente da informação e dados como hoje (Floridi, 2009; 2014; Widén et. al., 2023).

Habitamos sociedades nas quais pouco ou nada permanece intocado pelas tecnologias digitais. Nossa realidade está se tornando cada vez mais digital e nossa interação social é cada vez mais digital. São sociedades nas quais a fronteira entre online e offline está se tornando cada vez mais tênue (Floridi, 2014). A evolução rápida das tecnologias hoje significa que estamos numa fase madura de digitalização (Hilbert, 2022; Holmström Olsson; Bosch, 2020) – o que também tem sido denominado “pós-digital”, pelo qual as ferramentas e tecnologias digitais fazem cada vez mais parte da nossa vida cotidiana, bem como da nossa vida profissional, afetando a forma como comunicamos, interagimos e realizamos diferentes atividades (Dufva, 2020). Floridi (2014, p.63-9) fala na geração “hyper-self-conscious” composta por pessoas que gastam muitas horas do dia curando suas identidades online – o que ele também rotula como “*onlife*”. É rotineira a mineração de dados pessoais no setor de varejo: esta vigilância comercial de clientes ficou normalizada por narrativas de marketing que recompensam a colheita de dados em massa com o engajamento dos consumidores – os “bons compradores” – com cartões e *apps* de lealdade. Assim, personalizar a experiência do cliente não é um simples ato de benevolência ou boa vontade, mas sim o resultado da implantação de softwares sofisticados para analisar dados a partir de gerenciar a experiência e a lealdade do cliente. (Savirimuthu, 2017)

Aprofundada e alargada com o uso das tecnologias de inteligência artificial (IA), a digitalização vai de mãos dadas com o intensivo “algoritimização” do ecossistema informacional. A digitalização tornou o nosso dia-a-dia e trabalho mais associável, editável, interativo, programável, rastreável, comunicável e distribuível e, portanto, molda o local de trabalho e sua lógica organizacional (Kallinikos; Aaltonen; Marton, 2013).

Com as Tecnologias Digitais de Informação e Comunicação (TDIC) se tornando onipresentes em nossas vidas, também devemos ficar de olho em como ela é implantada, para quem e por quem (por qual empresa). Pois, como se sabe de décadas de pesquisa no campo de estudos sociais da C&T, a tecnologia não é neutra, mas é constituída pelos valores dos seus inventores, desenvolvedores, promovedores (Feenberg, 2017). A tecnologia pode aumentar ou diminuir a desigualdade, dependendo de quem tem acesso a ela, quem sabe como usá-la e quem consegue influenciá-la. A crise da pandemia do Sars-Cov-2 (o coronavírus) acelerou as soluções digitais em particular, ao mesmo tempo em que tornou o "fosso digital" ainda mais evidentemente visível. Testemunhamos durante a pandemia no Brasil, por exemplo, estudantes universitários indígenas obrigados a voltar para suas aldeias, sem um *laptop*, *smartphone* ou uma boa conexão de internet, excluídos assim, da continuidade da sua formação, que migrou para plataformas online. Ou vemos como idosos ficam excluídos porque muitos não são (ou não se vêem como) proficientes no uso das TDIC, ou por motivos fisiológicos de idade, suas mãos tremem ou o uso de dispositivos inteligentes fica difícil por algum outro motivo.

Mudanças nas TDIC influenciam e modificam significativamente a maneira como estudamos e trabalhamos, exigindo adaptação permanente, o que aponta para a necessidade do desenvolvimento contínuo de competências digitais e em informação. Uma dessas adaptações e modificações necessárias surge dos riscos crescentes de segurança e privacidade sempre presentes em atividades online, sejam elas de trabalho, estudo, lazer ou atividades relacionadas ao consumidor. Por isso, o *DigComp 2.0 European Framework* que foi desenvolvido em 2015 para explicar a professores, formuladores de políticas, pais e usuários finais a natureza multifacetada e complexa do conjunto em constante mutação de competências digitais e para estimular/encorajar o desenvolvimento contínuo dessas competências – dedica uma dimensão inteira de suas quatro dimensões de competências digitais, ao risco e à segurança online.

Paradoxalmente, ao mesmo tempo em que participamos ativa e intencionalmente na infoesfera (Floridi, 2014) nas redes "sociais", as informações hospedadas nas plataformas dessas redes tem ficado fragmentada, e o acesso a elas também está se tornando mais individualizado, dependendo, por exemplo, de quem você é, quem você segue e com quem você interage. A extensão das personalizações e seus efeitos sociais são invisíveis para o usuário individual. Ninguém sabe ao certo o que os outros encontram, qual combinação exclusiva de aplicativos, mecanismos de pesquisa e mídias sociais compõe o ecossistema de

informações de outras pessoas, como elas chegaram a quais termos para inserir em qual mecanismo de busca, ou como o *feed* se reconfigurará na próxima recarga, em resposta ao próximo deslize, após a próxima busca ou engajamento. O posicionamento da fragmentação das informações no nível da experiência destaca a intimidade da fragmentação contínua da compreensão coletiva da base de conhecimento da sociedade com a infraestrutura de informações na qual tudo acontece, desde a vida cotidiana até a política. (Haider; Sundin, 2022). Esses autores (2022, p.5) afirmam que a cultura digital é constituída por uma série de desafios inter-relacionados, que:

[...] contribuem para a desestabilização da informação - fragmentação, individualização, emocionalização e a erosão da base coletiva de confiança - , todos eles claramente não criados, mas exacerbados pela infraestrutura de informação algorítmica e comercial da sociedade e por uma forma qualitativamente nova de politização da informação, em que esta é cada vez mais adaptada à forma fornecida pelas plataformas multilaterais e à sua lógica específica de amplificação. A importância dos algoritmos, dos dados dos utilizadores e, cada vez mais, dos sistemas baseados em IA para a cultura contemporânea, mais especificamente para as plataformas multifacetadas, como os motores de pesquisa, os sistemas de recomendação, os assistentes domésticos inteligentes, os serviços de *streaming* ou as aplicações de encontros, não pode ser subestimada. É cada vez mais importante compreender como funcionam os sistemas algorítmicos e como são treinados para funcionar em situações específicas, ao mesmo tempo que se tornam cada vez mais esquivos e integrados na sociedade e na vida quotidiana a todos os níveis. Uma forma de abordar esta questão é utilizar o termo “cultura digital”, não como um período histórico com uma definição clara em detrimento de outros entendimentos da cultura e da sociedade, mas como uma perspectiva que nos permite colocar em primeiro plano a prevalência de certas socialidades e formas de conhecer e estar no mundo que estão incorporadas na organização da sociedade a diferentes níveis. Tomando como empréstimo o investigador dos meios de comunicação social Ted Striphas, a “cultura algorítmica” é aquela em que “os seres humanos têm vindo a delegar o trabalho da cultura - a ordenação, classificação e hierarquização de pessoas, lugares, objetos e ideias - em processos computacionais intensivos em dados” (Striphas, 2015, p. 396; ver também Lloyd, 2019). A cultura digital como perspectiva tem isto em conta, mas também a forma como os algoritmos, juntamente com as plataformas em que estão incorporados e os dados extraídos dos usuários, existem no âmbito de racionalidades e programas de mudança social mais amplos (ver também Beer, 2017).

Como toda a organização do conhecimento e sistemas de informação, as plataformas multifacetadas, os algoritmos e os dados são sempre contingentes e nunca imparciais. Por outras palavras, as configurações algorítmicas e as plataformas multifacetadas são ativas e co-constitutivas do tecido social mais vasto. A co-constituição implica não só que não se trata de uma relação unidirecional, mas também que as pessoas, a sociedade, os algoritmos, os

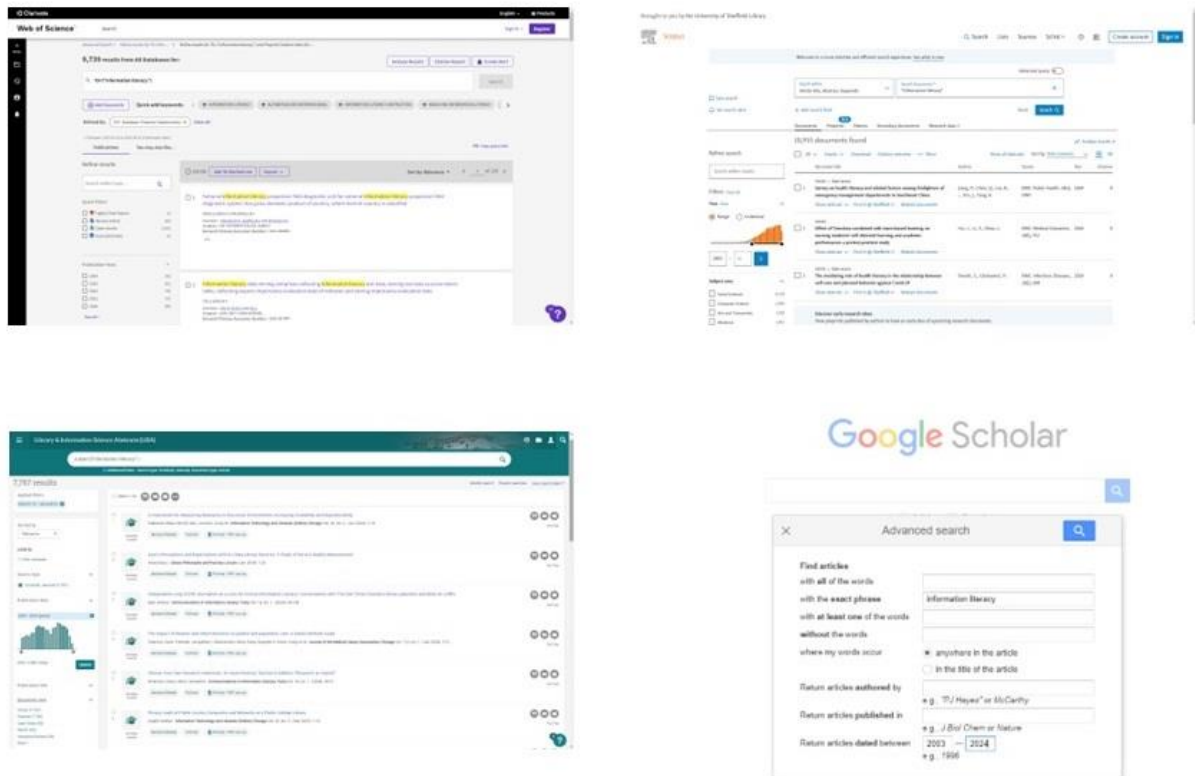
dados, as plataformas, os reguladores, etc., são todos constitutivos uns dos outros (Barad, 2003; 2007; Orlikowski; Scott, 2015). Para efeitos de compreensão da sociedade do ponto de vista da cultura digital, não é possível separá-los de forma significativa. As pessoas criam sentido a partir das plataformas e dos algoritmos nas várias práticas em que estão envolvidas, mas também lhes resistem de formas mais ou menos conseqüentes. As plataformas e os seus algoritmos não influenciam as pessoas apenas numa direção, mas através das suas interações com estes sistemas as pessoas também os alteram.

Mais recentemente, governos ao redor do mundo têm reconhecido a seriedade da/potencial interrupção causada por violações de segurança online, não apenas para instituições governamentais, indústrias e corporações privadas na forma de ataques cibernéticos massivos, mas principalmente para cidadãos comuns – e particularmente para as gerações mais velhas e mais jovens – na forma de golpes por e-mail e mídia social, *phishing*, violações de dados, propagação de malware, quebra de senhas por atores maliciosos. A privacidade e a segurança online, no entanto, tornaram-se um requisito de rotina para todos os usuários de computadores, dispositivos móveis e do software e aplicativos que eles suportam. Apesar do crescente reconhecimento por parte dos governos de que eventos maliciosos online podem incorrer em custos massivos para as economias nacionais, e que a atividade criminosa na dimensão digital tem que ser tratada em pé de igualdade com a atividade criminosa no “mundo real” – em outras palavras, que o digital é parte integrante da vida física – há uma consciência aguda de que governos, sistemas judiciais e a aplicação da lei estão jogando um jogo de “recuperação” contínua quando se trata de legislar para salvaguardar a segurança e privacidade online e proteger os cidadãos de atores maliciosos online. A tarefa para as autoridades é de Sísifo.

Os termos “competência informacional” e “competência em informação” (este último mais usado no Brasil) já são consagrados na literatura da Ciência da Informação e Biblioteconomia. Existe uma plethora de artigos acadêmicos sobre essas temáticas, desde que o termo “*information literacy*” (traduzido para os dois termos supracitados em português) foi cunhado pelo bibliotecário norteamericano Paul Zurowski em 1973. Em 2002, Rader (2002) observou que mais que 5 mil artigos sobre competência em informação e instrução de usuários de bibliotecas tem sido revisados (*reviewed*) num período de 30 anos. Continuando aqui com esse tipo de levantamento quantitativo, uma busca rápida, realizada em 4 de agosto de 2024, nas principais bases de dados bibliográficas, especificando o intervalo de janeiro, 2003 a agosto, 2024 (ou seja, um período de 21 anos) e filtrando para artigos de

periódicos, recuperou 9.739 registros na Web of Science; 10.935 registros da Scopus; 7.767 da LISA e 8.720 registros da Google Acadêmico, como demonstra a figura 1.

Figura 1 – Quantidade de registros recuperados na WoS, Scopus, LISA e GoogleAcadêmico para “information literacy”, de 2003 a 2024

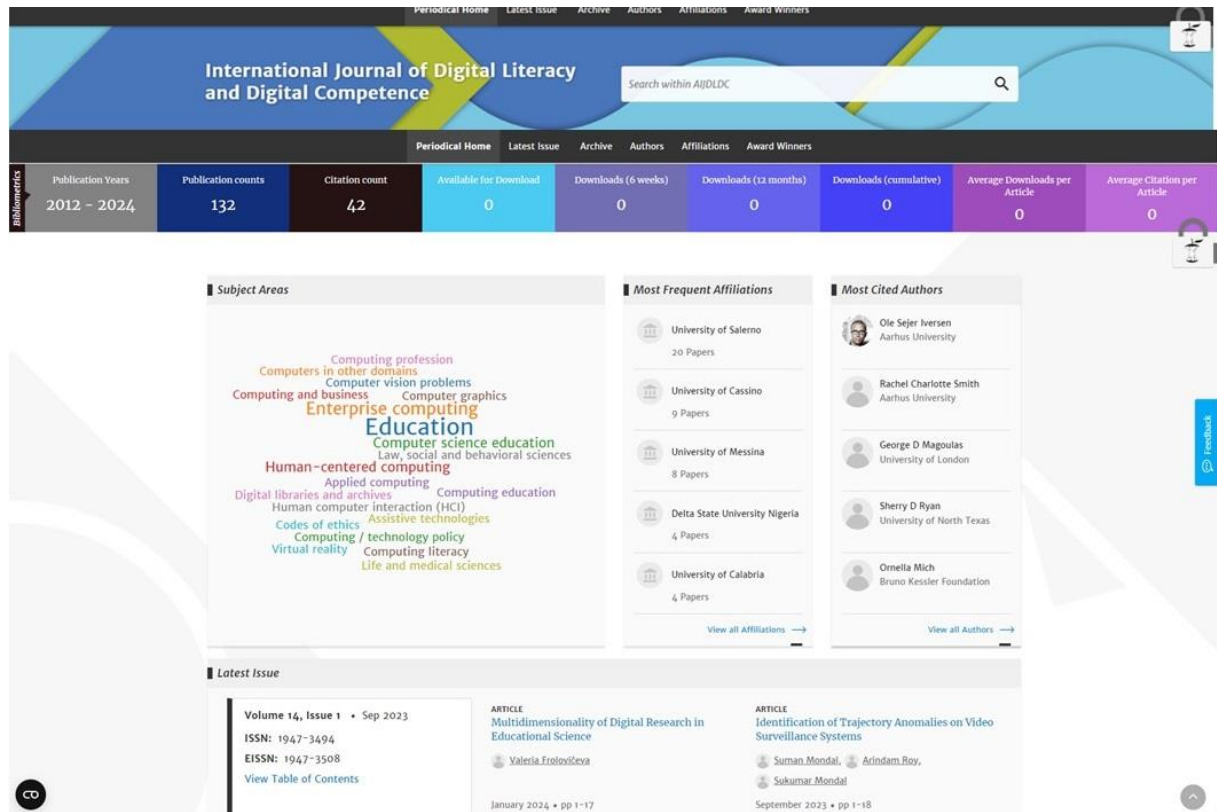


Fonte: Dados da pesquisa (2024)

Como estas buscas rápidas revelam, a literatura sobre a competência em informação não cessa de crescer. No entanto, desde o fim da década de 1990, tem havido um aumento em paralelo na quantidade de publicações – tanto na literatura branca quanto na literatura cinzenta – sobre a “competência digital”, “alfabetização digital” ou em inglês, *digital literacy*. Nas mesmas bases de dados citadas acima, buscas simples, cobrindo o período 2003 até o presente (2024), recuperaram 7.993 registros da Web of Science, 5.402 da SCOPUS, 7.767 da LISA e do Google Scholar, 13.800. De fato, o tema de letramento digital (*digital literacy*) tem sido cada vez mais debatido e discutido desde a publicação, em 1997, da obra homônima *Digital Literacy* de Paul Gilster. É, no entanto, um termo complexo baseado em estudos e pesquisas concomitantes sobre outras e novas alfabetizações/letramentos, entre eles a midiática e a computacional. Não foi o objetivo desta pesquisa realizar uma revisão sobre o termo *digital literacy*, embora seja abordado sucintamente numa seção abaixo neste relatório. O fato que este tema seja foco intelectual independentemente do seu tema

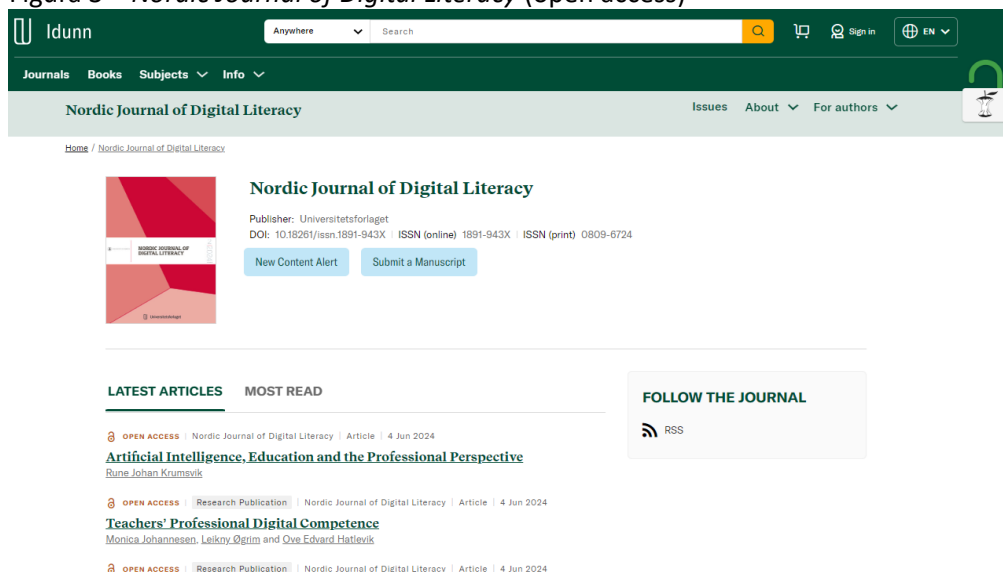
congênere, competência informacional, é ressaltado pelo fato que existem publicações exclusivamente dedicados ao *digital literacy*, como se vê nas figuras 2 e 3.

Figura 2 - *International Journal of Digital Literacy and Digital Competence* (open access desde 2023)



Fonte: Dados da pesquisa (2024) <https://www.igi-global.com/journals/open-access/table-of-contents/international-journal-digital-literacy-digital/1170>

Figura 3 – *Nordic Journal of Digital Literacy* (open access)



Fonte: Dados da pesquisa (2024) <https://www.idunn.no/journal/njdl>

A cultura digital possui duas faces já muito bem conhecidas: por um lado, temos a disponibilidade do conhecimento e da informação mais democrática. O potencial de conexão entre culturas, ideias e pessoas. A oportunidade de experimentar, aprender, criar novas formas de expressão e divertir-se. O lado negativo são os perigos relacionados com o discurso de ódio, a discriminação, a desinformação e a erosão da privacidade. Ainda existe a exclusão digital de pessoas que não têm ligação à Internet ou que não sabem utilizar as TDIC. Além disso, existe a possibilidade de nos tornarmos dependentes das grandes empresas tecnológicas – as *big techs* – que gerem uma grande parte da nossa vida na Internet (Lemos, 2024). A capacidade de navegar pelos benefícios e riscos da conectividade digital depende, em grande parte, da competência digital. No entanto, é a relativa falta de literatura existente sobre competência digital/*digital literacy* focando na segurança e privacidade online que moveu a pesquisa aqui relatada. A lacuna pode ser derivada em parte pelo uso intercambiável de termos como “privacidade”, “segurança” e “*online safety*” e aos diferentes usos e entendimentos atribuídos a esses conceitos. Portanto, entendemos que há uma necessidade de uma revisão de literatura que preencha essa lacuna e identifique maneiras de abordar a competência digital – *digital literacy* – especificamente no contexto da segurança e privacidade online.

Do exposto, a pesquisa objetivou responder à seguinte **questão norteadora**: “Qual é o estado de literatura dos estudos da área de competência digital em relação à segurança e privacidade online nos últimos cinco anos (2019-2024)?” Desdobrando em questões pontuais e específicas, temos:

- Quais são os conceitos propostos pelos estudos das áreas de competência digital (*digital literacy*) nos últimos cinco anos?
- No mesmo período, quais foram as abordagens e enquadramentos do problema de segurança e privacidade online na literatura?

Diante do exposto, a pesquisa teve como **objetivo geral** realizar uma revisão da literatura científica e cinzenta acerca dos temas que se interseccionam: competência digital e segurança e privacidade online. Por “online”, queremos dizer o uso das ferramentas e plataformas hospedadas na Internet, entre elas e-mail, bases de dados institucionais, mídias e redes sociais, áreas de aprendizagem virtual.

Os **objetivos específicos** foram:

1. Analisar, diferenciar e discutir os termos e conceitos de competência digital como aparecem na literatura identificada;

2. Levantar e descrever a literatura (incluindo a literatura cinzenta) dos últimos cinco anos que trata dos temas competência digital em relação à privacidade e segurança online;

3. Fazer destaque sobre os principais achados e informações novas e relevantes dentre os estudos levantados para poder traçar novas perspectivas para a Ciência da Informação.

Esta pesquisa projetou-se como um esforço teórico-reflexivo, visando abrir espaço para subsidiar o desenvolvimento de mais pesquisas, inclusive empíricas, que relacionem as temáticas de competência digital com a privacidade e segurança online, fomentando o diálogo e possíveis parcerias para a realização de tais levantamentos empíricos futuros.

## **2. Evolução do conceito de competência digital – *digital literacy***

Cabe ressaltar que há um debate contínuo no campo da Ciência da Informação sobre definições e terminologia nesta área. As divisões entre os termos literacia digital, mediática e informacional são confusas e há variações adicionais na aplicação de termos como literacia, competência e habilidades (Lloyd, 2017; Tinmaz et al., 2022). No mundo de língua portuguesa há um debate sobre 'competências', 'letramento', 'literacia' e 'alfabetização', algumas delas refletindo diferenças regionais entre Brasil e Portugal e outras facetas do debate focadas nas perspectivas disciplinares do assunto (Gasque, 2013; Mbandje; Loureiro; Lucas, 2023). Esta pesquisa segue a terminologia utilizada na iniciativa DigComp (Vuorikari et al., 2016), que se refere à “competência digital” (*digital competence*).

De modo geral, podemos afirmar que a competência em informação (*information literacy*) tem focado nos componentes voltados para habilidades do cidadão, em uma variedade de contextos (estudo, trabalho, lazer, saúde) para: a busca pela informação, avaliar criticamente o conteúdo informacional encontrado, identificar as ideias-chave e sintetizar, assimilar e apropriar a informação para resolver problemas. No ecossistema informacional atual, este conjunto de atividades é designado como “competências de pesquisa online” (*online inquiry competences – OIC*) (Gonzalez-Ibanez; Shah, 2012). Discutivelmente, atenção menor tem sido dada para as competências e habilidades voltadas para aspectos de segurança e privacidade ao realizar essas pesquisas online.

Entendimento radicalmente alternativa dessa perspectiva da competência informacional é encontrado nos textos da Lloyd (2010), que a entende a competência informacional como uma prática, situada num dado contexto (entre eles, acadêmico, profissional, contexto de lazer) que vai determinar as formas de se tornar informado, as formas de conhecer – é o *locus* ontológico e as práticas desse *habitus* (e Lloyd refere a Bourdieu para reforçar esta ideia da relevância do campo da prática) que molda a competência informacional; como ela explica:

[...] a competência em informação é reformulada como uma prática de informação manifestamente complexa que é tecida através da teia de práticas integradoras que constituem o sítio e lhe dão a sua forma e característica. Aqui, a competência em informação não é vista como uma prática descontextualizada, porque está inserida nos processos de se tornar informado e de conhecer. [...] A competência em informação não é constituída por uma única forma de saber sobre a informação, mas é um produto das muitas formas de saber, que se interligam para formar a prática. A competência em informação está ligada e torna-se visível através da sua localização o que sugere que está ligada ao domínio social, ou seja, ao seu contexto. Ganha significado através da forma como se manifesta como ações e atividades, centradas na informação e no conhecimento que é e conhecimento que é prefigurado e moldado por dimensões históricas, sociais, culturais, económicas e políticas dimensões históricas, sociais, culturais, económicas e políticas. (Lloyd, 2010, p.253)

Para Lloyd, a competência em informação é acima de tudo, uma prática sociocultural arraigada no sítio, contexto onde é praticada. Enquanto prática sociocultural, a prática da competência em informação reflete os conhecimentos específicos e formas específicas de saber que são uma parte central de um sítio social ou profissional, esse sítio não sendo meramente assim um “pano de fundo”, mas um constituinte de formas de conhecer, de definir o que é considerado a informação.

A transformação digital é principalmente sobre mudança, o que por sua vez, requer mudanças de atitudes, habilidades e conjuntos de conhecimentos – de formas de trabalhar e estudar. É nesse sentido que a competência digital é uma lente importante por meio da qual as dimensões de privacidade e segurança podem ser contempladas. Sharma et al. (2018) nós lembram que foi Lanham que, em 1995, primeiramente conceituou o letramento digital como a habilidade de compreender informações, independentemente do meio, uma definição que focou na habilidade do usuário de navegar entre os vários meios online e offline. Como já mencionado, Paul Gilster publicou, em 1997, o livro *Digital literacy* - livro esse acessado para a realização desta pesquisa, a partir do *Internet Archive*, donde foi possível emprestar o livro por um período de tempo para a exclusiva leitura online. Nele, Gilster define a competência digital (*digital literacy*) como “a capacidade de compreender e

utilizar informação em múltiplos formatos, proveniente de uma grande variedade de fontes, quando apresentada através de computadores” e, em particular, através do meio da Internet (Gilster, 1997, p. 33). A afirmação do Gilster de que o letramento digital é sobre “*mastering ideas, not keystrokes*” - “o domínio de ideias e não de tecladas” (Gilster, 1997, p.15) é muito frequentemente citado em todas as revisões sobre o tema, com a observação que ele já via a competência digital com foco nas capacidades cognitivas, críticas e reflexivas de que restrita às competências. Como Pangrazio et al. (2020) observam, é relevante lembrar que Gilster estava escrevendo num momento histórico da emergência da Internet, quando havia muito foco nas habilidades técnicas de navegar (*surf*) essa nova tecnologia de informação e comunicação (TIC). Mesmo assim, Gilster já percebia que haveria necessidade também de saber confrontar fontes encontradas nessas plataformas digitais com as fontes não-digitais (*analogue sources*) e sobretudo, de saber adotar uma postura crítica diante das primeiras. Gilster é tido como o primeiro estudioso a conceitualizar o termo, porém, na revisão de Reddy et al (2020), é recuperado o texto de Martin (2006), que afirmou que o conceito (e menos o termo) remonta a um passado mais distante, da década de 1970, quando falava-se em “alfabetização tecnológica” que era vista como a “capacidade de usar as novas tecnologias que eram eficientes e apropriadas para produzir informações com novos insights.” No entanto, a ênfase estava nas habilidades de se usar as tecnologias, e o termo “alfabetização tecnológica” facilmente veio a ser substituído pelo termo “alfabetização computacional” ou *computer literacy*. Este termo “tomou conta” dos anos 1980, quando empresas como a Apple e a Microsoft, com o lançamento do software Windows, entraram em cena e revolucionou o próprio conceito de computador, tornando-o um dispositivo indispensável para cada domicílio. Os seus usuários certamente tiveram que adquirir habilidades no uso de um *mouse*, um GUI (*Graphical User Interface*), menus e uma pletera de outros recursos inerentes a essas tecnologias. Reddy et al. (2020) observam que o termo *computer literacy* foi, na década de 1980, substituído com o termo *ICT literacy* (letramento em TIC), e que, comparado com *computer literacy* (visto como a habilidade de usar o computador como uma ferramenta para apenas acessar conhecimento), o *ICT literacy* pôs ênfase na criação desse conhecimento. Reddy et al. (2020, p.82) citam Lankshear e Knobel) que definem “[...] *ICT literacy* como o uso da tecnologia digital, ferramentas de comunicação e redes para acessar, gerenciar, integrar, avaliar e criar a informação com a finalidade de funcionar numa sociedade baseada no conhecimento.”

Embora esteja em constante evolução, a perspectiva da competência digital inclui tanto a capacidade de acesso como o conhecimento da utilização de ferramentas tecnológicas (Gilster 1997). O dinamismo do conceito é realçado por esta mistura de capacidade e acesso. É possível utilizar um terminal de computador numa biblioteca pública sem saber enviar e receber correio eletrônico, ou ser bastante proficiente na comunicação digital sem ter acesso a um dispositivo em rede (Jaeger et al. 2012, apud Johnson; Lasher, 2021). As competências de pensamento crítico também são importantes para a competência digital; a informação e os recursos necessários para operar dispositivos digitais continuam a ser relevantes para a avaliação e a utilização diária (Thompson, 2008). Iloäki et al. (2016) enumeraram 34 termos usados para descrever as habilidades e competências relacionadas à tecnologia digital. Os mais comuns foram “alfabetização digital”, “multiliteracia” e “alfabetização midiática”. Cada um deles tem um significado diferente, dependendo de onde foram encontrados. Os termos sugeriam a definição de alfabetização digital como: (1) competência técnica; (2) alfabetização no uso de tecnologias digitais de forma significativa - para trabalhar, estudar e realizar tarefas diárias; (3) a capacidade de avaliar informações de forma crítica no contexto das tecnologias digitais; e (4) a motivação para participar e se envolver na cultura digital.

Como se percebe da revisão ampla do termo e conceito de competência digital, é abrangente e complexo, relacionado ao desenvolvimento de várias áreas de competência, incluindo alfabetização em informações e dados, comunicação e colaboração, alfabetização em mídia, criação de conteúdo on-line, segurança on-line e bem-estar digital, bem como resolução de problemas, pensamento crítico e inovação com ferramentas e tecnologias on-line. As competências digitais abrangem não apenas as ferramentas de informação e comunicação e as habilidades relacionadas à tecnologia, mas também as atitudes e o comportamento relacionados ao ambiente de informação e comunicação on-line, que abordam o uso e a disseminação responsáveis, éticos e seguros das informações, bem como o desenvolvimento de abordagens criativas e inovadoras ao usar a mídia digital para aprendizado, trabalho e participação social na vida cotidiana para atingir objetivos pessoais, sociais ou comerciais (Carretero et al., 2017; Laurillard et al., 2016). Os autores Fu (2013), Sarkar (2012) e Martin e Grudziecki (2006) focam em como o contínuo crescimento das TDIC exige que os indivíduos tenham as habilidades e competências necessárias para executar tarefas e resolver problemas em ambientes digitais (Fu, 2013; Martin; Grudziecki, 2006), sendo que o posse desse conjunto de habilidades apontaria para o letramento digital. De

acordo com Fu (2013), a competência digital é “um conjunto de habilidades exigidas por indivíduos do século XXI para usar ferramentas digitais para dar suporte à realização de objetivos em suas situações de vida.” É certamente plausível imaginar que a maioria das pessoas ia concordar com esta definição ampla. Martin (2006, p.19) elaborou uma definição geral da competência digital como:

[...] a consciência (*awareness*), a atitude e a capacidade dos indivíduos utilizarem adequadamente as ferramentas e os recursos digitais para identificar, aceder, gerir, integrar, avaliar, analisar e sintetizar recursos digitais, construir novos conhecimentos, criar expressões mediáticas e comunicar com os outros, no contexto de situações específicas da vida, a fim de permitir uma ação social construtiva; e refletir sobre este processo.

Outro conjunto de textos identificados nas várias revisões sobre a temática, aponta para a relevância de localizar a competência digital num espectro de outros letramentos (*literacies*). Na sua revisão sistemática, Stordy (2014) descreveu a paisagem terminológica densa do século 21 constituída pela proliferação de nada menos que 35 termos e conceitos em torno de uma variedade de *literacies* (“literacias” ou “letramentos”) necessárias para navegar e usar ferramentas e plataformas da Web 2.0. Entre estes termos, tem-se: *computer literacy*, *e-literacy*, *Internet literacy*, *media literacy*, *cyber-literacy*, *technological literacy*, *transliteracy*, *metaliteracy* e *multimodal literacy*. Nessa mesma linha – muito mais usual entre os estudiosos provenientes do campo de Educação –, Covello, escrevendo em 2010 (*apud* Reddy et al, 2020, p.83), identificou o letramento digital como um letramento guarda-chuva – uma *metaliteracy* – que engloba seis outros letramentos, a saber:

1. Letramento informacional: usar tecnologia digital para encontrar, localizar, analisar e sintetizar recursos, avaliar a credibilidade desses recursos, técnicas de citação apropriadas, respeitar as questões legais e éticas que cercam o uso desses recursos e formular perguntas de pesquisa de maneira precisa, eficaz e eficiente.
2. Letramento em informática: uma compreensão de como usar computadores, tecnologias digitais e suas aplicações para uso prático.
3. Letramento midiática: ter a capacidade de usar tecnologias digitais para acessar, analisar, avaliar e comunicar informações em uma variedade de plataformas digitais.
4. Letramento em comunicação: usar tecnologias digitais para se comunicar efetivamente como indivíduos e trabalhar colaborativamente em grupos, usando tecnologias de publicação, a Internet e ferramentas e tecnologias da Web 2.0.

5. Letramento visual: ter a capacidade de usar tecnologia digital para "ler", interpretar e entender informações apresentadas em imagens pictóricas ou gráficas, comunicar essas informações e converter as informações em representações visuais.

6. Letramento tecnológica: Ter a capacidade de usar a tecnologia digital para melhorar o aprendizado, a produtividade e o desempenho.

Na revisão sistemática de artigos de revisão realizada por Tinmaz et al. (2022), os autores identificaram nada menos que 35 diferentes letramentos (*literacies*) mencionados nos 43 artigos que analisaram, entre eles “*tagging literacy*”, “*mobile literacy*”, “*data literacy*” e “*publishing literacy*”. Além da variedade de competências (letramentos) que esses autores identificaram na sua revisão, também agruparam as definições de competência digital em torno de outros três eixos: competências, habilidades (*skills*) e pensar (*thinking*). Sob a categoria competências, os pesquisadores identificaram 14 categorias, incluindo direitos digitais, uso de IA, uso de *big data*, resolução de problemas. As 35 categorias agrupadas sob o eixo “habilidades”, que foram predominantemente reunidas em torno de habilidades de letramento informacional – competência em informação –, principalmente nas etapas de processamento de informações; descoberta, localização, avaliação, utilização, comunicação, uso ético. Por fim, os autores identificaram 8 categorias sob o eixo “pensamento” (*thinking*) nos artigos que recuperaram sobre competência digital: pensamento crítico, sistêmico, computacional, interdisciplinar, analítico, proposital (*purposeful*), inovador e pensamento rápido. Sobre o pensamento digital – e relevante para o foco na segurança online da presente pesquisa – os autores observam que o pensamento digital foi observado como sendo principalmente relacionado ao pensamento crítico e ao pensamento computacional, a criatividade e inovação, os textos recuperados e analisados apontam a necessidade urgente de pensamento digital no “combate” a notícias falsas, desinformação, câmaras de eco e para garantir a segurança cibernética. Por fim, a amplitude de categorias sob grandes eixos que os autores identificaram na sua revisão sistemática os levaram a concluir que “a competência digital é muito mais ampla do que tarefas específicas, abrangendo toda a esfera de operação de computador e uso de mídia em um contexto cultural.” Nessa linha, citamos a Julien (2018), que define a competência digital como “o conjunto de habilidades, conhecimentos e atitudes necessários para acessar, criar, usar e avaliar informações digitais de forma eficaz, eficiente e ética” (Julien, 2018, p. 2248). À primeira vista, esta definição não a distingue muito da competência em informação (*information literacy*), e então, resta saber se são

meramente as plataformas e ferramentas que mudam na concepção de competência digital, ou se existem diferenças mais substantivas entre as duas modalidades de competência.

Reddy et al. (2020) relacionam as etapas da evolução das TIC e TDIC e a Internet nas suas fases Web 1.0, 2.0, 3.0, 4.0, com estilos de ensino e aprendizagem em instituições de ensino de todos os níveis. Na Educação 1.0 – que corresponde à fase da Web 1.0 – o aprendizado era principalmente orientado ao professor, com os alunos tomando notas e contando com livros didáticos como sua principal fonte de informação. A Web 1.0 era meramente um meio somente leitura – uso de páginas estáticas, e-mails, sites e HTML. Na Educação 2.0, que surgiu com a evolução da web para a Web 2.0, o aprendizado se tornou mais interativo e colaborativo. Os alunos começaram a se envolver com o conteúdo da web por meio de redes sociais, blogs, podcasts e outras tecnologias de participação. Essa mudança foi influenciada pelo construtivismo, enfatizando a comunicação, a contribuição e a colaboração. A Educação 3.0, que é a fase atual, é caracterizada pelo aprendizado baseado na Internet, autodeterminado e em ritmo próprio. Ele se concentra na resolução de problemas, inovação e criatividade. Os alunos têm mais autonomia em seu processo de aprendizado e podem acessar uma ampla gama de recursos e ferramentas digitais. A Educação 3.0 promove o aprendizado ao longo da vida e incentiva os alunos a serem aprendizes autodirigidos. No geral, a evolução da educação da Educação 1.0 para a Educação 3.0 viu uma mudança da aprendizagem centrada no professor para a aprendizagem centrada no aluno, com uma ênfase crescente na colaboração, criatividade e aprendizagem autodirigida. Mesmo publicando seu artigo em 2020, Reddy et.al (2020) escrevem no tempo verbal do futuro ao falar na Web 4.0, que “será” uma internet que viabiliza criar relacionamentos simbióticos entre humanos e máquinas. “De acordo com Solanki & Dongaonkar, 2016, a Web 4.0 terá todos os dados e sistema operacional na nuvem e conectará todos os dispositivos no mundo real e virtual em tempo real.” Os autores falam na IoT – *Internet of Things* ao falar na Web 4.0, sem mencionar a IA, as ferramentas da qual certamente hoje caracteriza a Web 4.0 hoje e nossa interação e imbricação com ela, o que nos lembra a afirmação de Mård e Hallin (2024, p.15) de que nós nos encontramos numa era *pós-digital*, em que humanos são “inextricavelmente interligado com as tecnologias digitais.”

Por fim, cabe ressaltar que perdura até hoje uma questão em aberto acerca de se a competência digital deveria ser pensado como uma lista de habilidades ou se ela se refere a algo mais amplo, como práticas socioculturais e valores sociais. De fato, nos anos 1980s e 1990s, surgiu, na academia, um movimento que se chamou os “*the New Literacy Studies*”

(NLS) que visou ir além do paradigma focando nas habilidades, sublinhando a dimensão social de letramento (*literacy*), enfatizando intercâmbio crítico e aplicação de pensamentos e ideias entre indivíduos. Como Ray (2018, p. 2231) observa, “O arco da competência digital passou do seu foco original nos computadores para as tecnologias e, finalmente, para a ideia de agência humana.” Nessa concepção da competência digital, há uma crítica do constructo das habilidades, da possibilidade de avaliar e medir tais conjuntos de habilidades – pois são vistas como conjuntos de “benchmark skills” (Ray, 2018, p.2224). Ser competente em termos digitais (*digitally literate*) implica, então, o alcance determinista “da medida” do que significa ser competente. A crítica repousa na crença, nesse paradigma, da neutralidade das tecnologias, da visão das tecnologias como meios ou instrumentos que precisam ser apreendidas. Por outro lado, o paradigma sociocultural vê as tecnologias como Sistemas complexos que não são isentos de valores e vieses sociais, culturais e políticos. De acordo com Ray (2018), esta privilegia uma visão instrumental da competência digital implicada na noção de aquisição de um limiar ou de um conjunto genérico de competências técnicas. Isto perpetua o paradigma padronizado da aquisição de competências, e estabiliza o ensino e a aprendizagem como um conjunto de práticas prescritivas e duradouras que têm unidades fixas de tempo e lugar, nas quais o papel da tecnologia é considerado neutro.

A perspectiva sociocultural da competência em informação (*information literacy*) elaborada por Annemaree Lloyd (2010) no seu artigo intitulado “Framing information literacy as information practice: site ontology and practice theory” também pode ser aplicada à competência digital. Na base dos argumentos da Lloyd é que uma pessoa tem de entender e usufruir das instituições políticas, económicas e culturais de uma sociedade para ser considerada “alfabetizada/letrada/competente”, o que só é significativo num dado contexto social. As competências (literacias) alteram as capacidades cognitivas humanas, para além de darem às pessoas as ferramentas e capacidades para interagirem com materiais escritos. Novas ferramentas técnicas ou cognitivas - como a escrita - ou ferramentas - como as tecnologias digitais - estão na origem desta capacitação intelectual. Para Lloyd (2010), uma vez que a competência em informação está enraizada nos processos de aprendizagem e de informação, não é vista como uma disciplina descontextualizada. Os funcionários, estudantes, profissionais todos obtêm informação do seu trabalho e combinam-nos com outras informações para criar a inteligibilidade prática (saber-fazer – *know how*) necessária para funcionar bem e conviver com os outros numa comunidade de prática (Lloyd refere ao

*habitus* do Bourdieu). O relevante é o contexto (Lloyd fala na “ontologia do sítio”) da informação:

Independentemente da forma como se situa a competência em informação, o ponto importante a salientar é que ela não é constituída por uma única forma de saber sobre a informação, mas é um produto das muitas formas de saber, que se interligam para formar a prática. A competência em informação está ligada e torna-se visível através da sua localização o que sugere que está ligada ao domínio social, ou seja, ao seu contexto. Ganha significado através da forma como se manifesta como ações e atividades, centradas na informação e no conhecimento que é prefigurado e moldado por dimensões históricas, sociais, culturais, económicas e políticas. Para compreender a competência em informação, é necessário entender como a prática é formada e atuada no local e através das interconexões que são feitas entre o sítio, o seu conhecimento, as pessoas e os objetos materiais que criam. (Lloyd, 2010, p.253)

Isto implica que a competência em informação não pode ser visto como um “conjunto reificado e descontextualizado de competências, lançado à deriva e distante dos discursos e práticas que influenciam e conduzem a atividade e a interação humanas” (Lloyd, 2010, p.252). Vários estudiosos têm adotado esta perspectiva também para a competência digital, entendendo-a acima de tudo como uma prática sociocultural (Ray, 2018; Sharma et al., 2018; Mård; Hallin, 2024). Por exemplo, Sharma et al. (2018) nos trazem os autores Gilster (1997), Bélisle (2006), Bawden (2008) para subsidiar seu argumento daquilo que chamam “novas abordagens” da competência digital que alargam a sua definição de modo a incluir conceptualizações orientadas para o conhecimento, bem como conceptualizações orientadas para a prática. Integram uma consciência sofisticada das interações entre a ferramenta, o ambiente e o ator, indexando o conceito de competência digital como um discurso. Os quadros examinam o conceito de participação social na esfera digital e apresentam a competência digital como uma “competência de sobrevivência”. Acima de tudo, a transição de um paradigma centrado nas ferramentas para um paradigma orientado para o conhecimento crítico ilustra a aprendizagem como um fenómeno social que existe fora das ferramentas e das máquinas. As inovações nas TDIC exigem novos conhecimentos, capacidades, consciencialização e estratégias de utilização. Os novos letramentos evoluem constantemente à medida que as tecnologias que as definem mudam: eles são multidimensionais e multimodais, e a nossa competência tem impacto positivo em nossa participação social. (Leu e outros, 2007). Os indivíduos são capacitados como cidadãos globais através de componentes de letramento.

Tendo em conta a rápida evolução do panorama tecnológico e a mudança de condições, Bawden desenvolve um paradigma para a competência digital. Compreende (a)

fundamentos, que incluem o letramento em informática/TIC e o letramento em geral; (b) conhecimentos de base, que incluem a complexidade da informação e a natureza dos recursos e fontes de informação; (c) competências centrais, que incluem capacidades fundamentais como a curadoria de conhecimentos, a avaliação da informação e a leitura e compreensão de formatos digitais e não digitais; e (d) atitudes e perspectivas, que servem como conceito subjacente que une os valores do letramento mais antiga com a ideia moderna de letramento através da aprendizagem independente e das responsabilidades morais/sociais (p. 29-30). De modo semelhante, Yoram Eshet-Alkalai (2004) fornece um quadro para cinco tipos diferentes de competência digital: letramento foto-visual, que é utilizado para interagir com interfaces gráfico-visuais; letramento da reprodução, que é utilizado para reproduzir significados através da reutilização e recombinação de elementos de informação pré-existentes; competência em informação, que é utilizada para avaliar a confiabilidade das fontes de informação online; letramento de “ramificação” (*branching literacy*), que é utilizado para navegar em estruturas não lineares da Web; e letramento socio-emocional, que é utilizado para proteger os interesses pessoais no contexto mais vasto da colaboração e da interconexão em rede possibilitada pelas TDIC.

Para Bélisle (2006), o letramento – em qualquer modalidade, seja midiática, textual ou digital – só é relevante quando é contextualizada no tecido cultural da sociedade. Por isso, seria mais correto falar hoje explicitamente em letramento digital como sociocultural. O objetivo final do letramento é cumprir um propósito que é, de acordo com Bélisle (2006, p.53), “[dá] acesso a, e compreensão de, estruturas de poder e autoridade através do domínio de textos escritos e números.” Compreender o contexto apropriado para cada uma das crenças, atitudes, costumes e comportamentos de uma sociedade é uma componente crucial do letramento sociocultural. Dado o aumento das vias de envolvimento e comunicação que o mundo digital oferece, isto é significativo em termos de letramento digital. O aspeto sociocultural do letramento digital permite que as pessoas se envolvam e participem nos sistemas sociais e económicos da sociedade digital. Assim, ao referir-se especificamente ao letramento digital, pode ser mais correto considerar a dimensão sociocultural do letramento como uma função “socioeconómica”, o que captaria seu impacto nos usuários e seu “empoderamento” (*empowerment*) nas comunidades online. Bélisle também descreve a dimensão transformacional do letramento digital. Esta “traz um enriquecimento profundo e acaba por implicar uma transformação das capacidades de pensamento humano” (Bélisle, 2006, p.54). A capacitação intelectual dos indivíduos através

do letramento pode ter o poder de transformar a sociedade, especialmente quando a capacidade cognitiva criativa leva à criação de novas ferramentas cognitivas (Bélisle, 2006). Sharma et al. (2018) vêem o letramento digital transformadora de Bélisle em sintonia com o letramento socio-emocional de Eshet-Alkalai, o que oferece novas oportunidades de colaboração e criação em comunidades e interações online. Na mesma linha da Bélisle e Lloyd anteriormente discutidos, as autoras Mård e Hallin (2024) enfatizam a perspectiva de letramento como uma prática sociocultural e contextual do letramento/competência digital e concordam com Tuominen, Savolainen e Talja (2005), quando propõem uma abordagem de prática sociotécnica para a competência em informação para desviar “o foco do comportamento, ação, motivos e competências de indivíduos monológicos” (2005, 339) e, em vez disso, centrar-se “nos contextos sociais, ideológicos e físicos e nos ambientes em que a informação e os artefatos técnicos são utilizados” (340). Porém, Mård e Hallin (2024) vão um pouco mais além, e, com ecos de Floridi (2014) anteriormente citado neste relatório, observam como as tecnologias digitais são mais de que “ferramentas” com as quais os seres humanos interagem, “manuseiam”, mas que, no contexto da cultura digital, estão inextricavelmente entrelaçadas com os humanos nas práticas cotidianas: os objetos materiais, as ferramentas tecnológicas e os algoritmos digitais têm de ser considerados como agentes na produção de práticas de competência digital. Seguem a linha do Bruno Latour, que elaborou, com Callon, a Teoria Ator-Rede (TAR), em que os agentes humanos e não-humanos possuem o mesmo status, implicando que o social e material são constitutivamente emaranhados: "o social e o material são considerados inextricavelmente relacionados - não há social que não seja também material, e não há material que não seja também social" (Mård; Hallin, 2024).

No caso da competência digital, isso significa que, em vez de se concentrar nas habilidades que são exigidas dos indivíduos, em como essas habilidades são compreendidas ou em como os seres humanos usam as tecnologias digitais, uma compreensão sociomaterial da competência digital envolve a atenção para como os seres humanos e as tecnologias são configurados na prática, ou seja, por meio da promulgação da competência digital (consulte Baptista et al, 2020; Grønsund e Aanestad, 2020; Suchman, 2012); à natureza situada e incorporada dessas práticas; e como elas são importantes (consulte Berkelaar, 2017; Clarke e Knights, 2018). (Mård; Hallin, 2024, p.19)

O que esta breve revisão sobre a evolução e conceitualização do termo competência digital (*digital literacy*) mostra, é que se é vista como uma lista de habilidades ou se ela se refere a algo mais amplo, como práticas e valores sociais, continua sendo um ponto discutido

e paradigmático na literatura. Por isso, Pangrazio et al (2020) não concordam com a tendência de “universalizar” e “padronizar” medidas e comparações de competência digital em contextos e culturas tão diversas (quando o contexto deve ser enfatizado). Sinteticamente, esses autores comparam o letramento digital com o letramento midiático que aponta para a questão que nos interessa aqui, citando o Centre for Digital and Media Literacy do Canadá: "a competência midiática geralmente se concentra em ensinar os jovens a serem consumidores de mídia engajados de forma crítica, enquanto a competência digital se concentra mais em permitir que os jovens participem da mídia digital de forma sábia, segura e ética" (Media Smarts, 2010). Assim, dizem Pangrazio et al (2020), a competência digital engloba questões de privacidade, segurança e uso ético da tecnologia.

### **3. Privacidade e segurança online**

Nesta seção do relatório, abordarei, de forma sintética e com base na literatura levantada, questões relacionadas à privacidade, e por extensão, segurança online. De fato, neste relatório, usarei os termos privacidade e segurança quase de forma sinônima, lembrando que quando os profissionais de informática falam de privacidade, referem-se a um tipo especial de segurança da informação, nomeadamente, a confidencialidade de informações pessoais (Pieters, 2011). Assim, adiro à linha de pensamento de Weinberger e Bouhnik (2023) que entendem o conceito de “privacidade” como um componente do termo mais amplo “segurança da informação”.

Nissenbaum, já em 2011, delineou um cenário relacionado à privacidade e segurança online que nós é muito familiar nos dias de hoje, possivelmente apontando para como a resolução da privacidade online tem avançado pouco nos últimos anos. Ela observou que a privacidade offline é ainda mais complexa online devido à:

[...] deslocação dos destinatários, tipos de informação e das restrições a que estão sujeitos os fluxos de informação. Compreendemos que, mesmo quando interagimos com partes conhecidas e familiares, podem existir terceiros à espreita, envolvidos em parcerias comerciais com as nossas partes conhecidas. A informação sobre nós, que outrora poderia ter ficado em armários de arquivos empoeirados, é agora localizada num instante através de pesquisas efetuadas por qualquer pessoa em qualquer lugar. Nestes ambientes altamente informatizados (ou seja, ricos em informação), novos tipos de informação permeiam todas as nossas ações e relações. (Nissenbaum, 2011, p.33)

Floridi (2005) observou que os aumentos significativos das capacidades de processamento de dados das TDIC (P), a velocidade (ou ritmo, *pace* em inglês - P) a que podem processar os dados e a quantidade e qualidade dos dados que podem recolher, registar e gerir, agravam as questões de longa data relativas à privacidade da informação. Ele refere a esta convergência de fenômenos como a “hipótese 2P2Q”. A consolidação desta hipótese está diretamente relacionada àquilo que Floridi (2005; 2009) refere como a “reontologização da infosfera<sup>4</sup>” (*re-ontologization of the infosphere*) caracterizada pelas seguintes tendências:

1. A digitalização do ambiente informacional [...]A transição dos dados analógicos para os digitais.
2. A homogeneização do processador e do processado [...] a convergência fundamental entre recursos digitais e ferramentas digitais.
3. A evolução de novos agentes informacionais [...] o surgimento de agentes artificiais e híbridos (ou seja, parcialmente artificiais e parcialmente humanos).
4. A informacionalização das interações. Na infosfera reontologizada, povoada por entidades e agentes ontologicamente iguais, onde não existe uma diferença ontológica entre processadores e processados, as interações tornam-se igualmente digitais.
5. a mutação de agentes antigos em agentes informacionais. Por fim, ao reontologizar a infosfera, as TICs digitais também trouxeram à tona a natureza intrinsecamente informacional dos agentes humanos. (Floridi, 2005, p.188)

Essa reontologização da infosfera traz consigo a inserção dos seres humanos nesse ambiente: entre outros agentes informacionais (talvez artificiais), os humanos são agentes informacionais dentro da infosfera. Existem, trabalham num ambiente que é mais propício às “criaturas digitais”: humanos têm o estatuto ontológico de entidades informacionais (Floridi, 2005; 2009). É nesse sentido, também, que Floridi fala não na vida online, mas fala em *onlife* (2014). A relevância para a privacidade dessa migração – tão reconhecível à maioria das pessoas hoje, cuja multiplicidade de atividades da vida cotidiana é inextricavelmente entrelaçada com o uso da internet – é que, como afirma Floridi (2005), não há diferença entre a “esfera informacional” de uma pessoa e a sua identidade pessoal, porque na Infoesfera, uma pessoa é a sua informação. Como Floridi explica (2005, p.194):

---

<sup>4</sup> Gonzalez de Gomez [c.2020,p.6] cita Durante (2017,p.24) para definir o conceito de Infoesfera desenvolvido por Floridi como: “[...] o ambiente informacional visto como uma totalidade e constituído por: 1) entidades informacionais; 2) suas propriedades; 3) suas interações; 4) seus processos; e 5) suas relações mútuas. [...] Infoesfera é, de fato, uma categoria abrangente que inclui o espaço analógico e digital, bem como os espaços off-line e on-line de informações. (DURANTE, 2017, p. 24). Relevante notar que a Infoesfera é digital e analógica ao mesmo tempo.

[...] ainda se pode argumentar que um agente “possui” a sua informação [...] mas o “meu” em “a minha informação” não é o mesmo “meu” que em ‘meu carro’, mas sim o mesmo ‘meu’ que em “o meu corpo” ou ‘os meus sentimentos’: exprime um sentido de pertença constitutiva, não de propriedade externa, um sentido em que o meu corpo, os meus sentimentos e a minha informação fazem parte de mim mas não são meus bens (legais). [...] A natureza de uma pessoa como sendo constituída pelas informações dessa pessoa permite que se entenda o direito à privacidade informacional como um direito à imunidade pessoal contra mudanças desconhecidas, indesejadas ou não intencionais em sua própria identidade como uma entidade informacional.

Do ponto de vista exclusivamente legal, de acordo com o especialista jurídico William Prosser, as preocupações com a privacidade enquadram-se num dos quatro “delitos” relacionados, que são os seguintes: 1) Uma definição de intrusão é a invasão muito ofensiva (física ou outra) da liberdade ou privacidade de alguém. 2. Fatos relacionados com a privacidade: divulgação de informações pessoais sobre um indivíduo que não suscitam “preocupação legítima” de ninguém. 3. Falsa luz: divulgação de informações inexatas e “extremamente ofensivas” sobre outras pessoas. 4. Apropriação: utilização da identificação de outra pessoa (nome, imagem) sem o seu consentimento, a fim de beneficiar da mesma (Barrett-Maitland; Lynch, 2020). A violação da privacidade informativa pode afetar: a solidão (o direito de ser deixado em paz), a intimidade (o direito de não ser monitorado) e o anonimato (o direito de não ter uma identidade pessoal pública e, por extensão, a privacidade física) (Hicks, 2019; Pieters, 2017). O artigo 12 da Declaração Universal dos Direitos Humanos indica claramente que "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação.

Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.” (ONU, 1948). A privacidade pode ser vista como um direito universal, mas igualmente à percepção de risco, a sua percepção pode ser culturalmente relativa. Um exemplo dado pelas autoras Barrett-Maitland e Lynch (2020) sobre Singapura e seu empreendimento nacional para criar *smart cities* ilustra esta afirmação. Naquele país, o governo está trabalhando para criar sistemas que melhorem a vida dos seus cidadãos, utilizando o “novo ouro” dos dados. Está trabalhando para desenvolver um sistema de transportes inteligente e um sistema de saúde inteligente, empregando sensores e robótica para monitorizar a qualidade da água nos seus reservatórios. Neste caso, a privacidade pode ser descrita como “culturalmente racional” e as leis em geral podem variar consoante às estruturas políticas e a evolução tecnológica.

Uma discussão sobre privacidade e segurança online precisa ser contextualizada pelos lados positivos e negativos que a Internet e as TDICs trazem no seu rasto. É indiscutível que a Internet revolucionou a comunicação, permitindo a qualquer pessoa com acesso ligar-se globalmente e acessar instantaneamente grandes quantidades de informação e dados. Este fato conduziu a uma maior liberdade de associação, expressão e inovação. Plataformas como a Wikipédia e o Facebook demonstram a coordenação descentralizada tornada possível pela Internet, e de um modo geral, a sociedade beneficiou muito com estes avanços. O lado negativo dessa descentralização é que os hackers e outras pessoas mal-intencionadas utilizam várias técnicas e ferramentas para explorar as características de abertura e partilha de informações da Internet, obtendo acesso não autorizado a computadores e redes. Uma vez lá dentro, lançam ameaças como ataques de negação de serviço, *sniffing*<sup>5</sup> de pacotes e roubo de identidade. Para combater esta situação, a tônica deve ser colocada na melhoria da qualidade do software e na eliminação do *malware*. Mas atualmente, as práticas de desenvolvimento de software facilitam a infiltração de hackers nos sistemas e as defesas contra *malware* são inadequadas. No entanto, é essencial encontrar um equilíbrio entre segurança e flexibilidade, uma vez que o aumento das medidas de segurança pode limitar a inovação e tornar o software e o acesso à Internet mais caros. O desafio consiste em encontrar o equilíbrio certo para prevenir a criminalidade na Internet e, ao mesmo tempo, manter os benefícios de um ambiente tecnológico em rápida evolução. As sugestões para melhorar a segurança incluem o reforço da qualidade do software e a luta contra o software malicioso, como os vírus e os *worms*<sup>6</sup>. De acordo com um estudo global sobre as percepções de risco online (Gregoire, 2023), 69% das pessoas entrevistadas em 2023 experimentaram um risco online causados por esse tipo de ação nefasta.

Mas como Sloan e Warner (2017) observam, muitas atividades na Internet caem numa zona cinzenta (*“in the in-between”*) que deixa as pessoas desconfortáveis, levando a uma reação do tipo *“é complicado”* em vez de *“é mau”*. A vigilância legal do governo e das empresas suscita preocupações quanto à privacidade, ao mesmo tempo que oferece benefícios em termos de serviços e eficiência. Esta vigilância legal apresenta uma mistura de aspectos positivos e negativos que é ambígua. Os estudos mostram que as pessoas desejam tanto benefícios de personalização como proteção da privacidade online, o que leva à necessidade de soluções de compromisso que equilibrem estes desejos contraditórios. O

---

<sup>5</sup> *Sniffing* refere-se à prática de interceptar pacotes de dados à medida que eles percorrem uma rede.

<sup>6</sup> *Worms* são programas maliciosos que se replicam, se espalhando automaticamente por uma rede.

equilíbrio destas soluções é crucial para garantir tanto os benefícios da personalização como a proteção da privacidade na Internet. Esses autores explicam que a intimidade, o companheirismo, a individualidade, as interações humanas, a liberdade, o autodesenvolvimento, a independência, a excentricidade, a criatividade, a democracia, a reputação, a saúde psicológica e a personalidade dependem da privacidade. Esta época caracteriza-se por uma vigilância generalizada. Além disso, a ideia orwelliana de um governo que utiliza instrumentos de vigilância (câmaras, microfones, etc.) não é o único aspecto da vigilância moderna. Para distinguir as pessoas e decidir como lidar com cada uma delas, as organizações recolhem atualmente informações de forma metódica. O desafio é de como pode ser limitado este tipo de vigilância generalizada por parte de atacadistas, corretores de informação, prestadores de cuidados de saúde e uma infinidade de outras entidades privadas.

Mas como vários autores observam, limitar (o risco online) não significa erradicar. As empresas que deixassem de praticar a vigilância em massa abdicariam das suas muitas vantagens, como o aumento da produtividade, a disponibilidade de crédito, a segurança, a transparência e as relações com os clientes, bem como a capacidade de processar pagamentos eletronicamente e facilitar uma série de interações comerciais. Temos de escolher a quantidade de privacidade a manter e a quantidade de privacidade a abdicar, a não ser que queiramos abandonar totalmente estas vantagens, o que quase ninguém faria. O desafio se torna encontrar uma abordagem geral para encontrar soluções de compromisso (*trade-offs*) adequadas entre a proteção da privacidade da informação e a obtenção dos benefícios do processamento moderno da informação. Sloan e Warner (2017) alertam que a mera distinção entre informações que são ou não identificáveis pessoalmente não pode ser a base de tal abordagem, e delineiam três argumentos por essa posição deles. Primeiramente, é difícil distinguir entre informações pessoalmente identificáveis e informações não pessoalmente identificáveis, uma vez que a simples remoção das referências de identificação pode não ser suficiente. Os algoritmos modernos de “desanonimização” são suficientemente poderosos para identificar indivíduos mesmo a partir de informações sem referências de identificação. Isto torna quase toda a informação identificável pessoalmente, o que coloca um problema, uma vez que a nossa economia e cultura dependem do livre fluxo de informação. Restringir o acesso a quase toda a informação não é uma solução viável.

Em segundo lugar, as leis de privacidade definem normalmente a informação pessoal identificável enumerando tipos específicos de dados, como nomes, números de segurança

social e números de cartões de crédito. As empresas adaptaram-se criando perfis de clientes que eliminam estas informações, mas que continuam a permitir a publicidade direcionada. E por fim, as informações de identificação pessoal são frequentemente utilizadas na publicidade. A publicidade visa frequentemente pessoas específicas. O marketing direto tradicional sempre defendeu esta ação, e é evidente que uma grande parte da publicidade moderna na Internet também o faz. As empresas de publicidade online destacam a sua capacidade de identificar pessoas de uma forma única para comercializar os seus serviços junto das empresas. Há poucas probabilidades de inverter a utilização maciça de informações de identificação pessoal pela publicidade. Os autores finalizam afirmando que:

[...] uma abordagem realista da proteção da privacidade tem de encontrar uma forma de equilibrar as preocupações com a privacidade e os benefícios da vigilância, independentemente do facto de uma determinada informação poder identificar inequivocamente um indivíduo. (Sloan; Warner, 2017, p.78)

Frequentemente, hoje, tal equilíbrio é supostamente encontrado no recurso de obter do usuário de um serviço ou plataforma online seu consentimento livre e informado às empresas para a utilização dos seus dados. É a prática de “aviso e escolha” (“*notice and choice*”) (Nissenbaum, 2011) pela qual são apresentados ao usuário os termos de uso em políticas de privacidade ou acordos de termos de uso e os usuários devem tomar decisões e medidas, normalmente clicando num botão “Concordo”, para os aceitar. Isto é o caso com a instalação de softwares. Hoje, no uso de websites, o usuário deve escolher quais conjuntos de *cookies*<sup>7</sup> aceitar ou não. Apesar do consenso de que a prática de notificação e a escolha não garantem o consentimento livre e informado, continua a ser o paradigma dominante do consentimento online. A ação e decisão tomada pelo usuário, sua “escolha”, não indica necessariamente um consentimento livre. Mesmo que a pessoa muito provavelmente não concorde no seu íntimo, acaba clicando no botão “Concordo”. Como os clientes frequentemente não leem os contratos, políticas ou as regras de privacidade (que comumente são documentos extensos numa linguagem muito legalista), o aviso e a escolha não garantem o consentimento. Parece que a maioria dos consumidores não acha que a leitura cuidadosa de avisos de privacidade valha o investimento de tempo; dito de forma simples, os benefícios percebidos são demasiados pequenos (Nissenbaum, 2011; Sloan; Warner, 2017). Por isso, a tendência é de aceitar os termos e “continuar com a vida.” Críticos

---

<sup>7</sup> *Cookies* são pequenos arquivos que os websites armazenam no seu computador para ajudar a rastrear a sua atividade. Os *cookies* de terceiros representam o maior risco para a privacidade, uma vez que rastreiam a sua atividade em vários websites.

assim propõe avisos e políticas muito mais curtos e legíveis e compreensíveis para os leigos, mas Nissenbaum (2011) questiona esta proposta ostensivamente louvável, devido àquilo que ela denomina o “paradoxo de transparência”. Este refere à necessidade de o usuário saber, sim, dos detalhes sobre quem são os associados comerciais e quais dados serão partilhados com eles; quais são os seus compromissos; que medidas são tomadas para anonimizar a informação; como é que essas informações serão processadas e utilizadas. Porém, esse nível de detalhamento implica que seja pouco provável que o aviso (sob a forma de uma política de privacidade) seja compreendida, quanto mais lida.

Nissenbaum (2011; 2015) fala em “normas de informação” que são contextuais e relativos ao momento histórico-social. As normas de informação ditam o tipo de informação pessoal que partilhamos com diferentes grupos de pessoas. Por exemplo, é mais provável que revelemos pormenores íntimos a amigos próximos do que a conhecidos profissionais. O contexto é a base da estrutura de integridade contextual de Nissenbaum (2011; 2015). As tecnologias digitais transmitem informações, muitas vezes de formas inovadoras, e a integridade contextual defende que a privacidade surge quando essa informação flui de uma de adequada às normas de um determinado contexto. Por exemplo, se um professor dá instruções aos alunos para realizarem um trabalho no seu computador portátil durante a aula, o professor pode andar pela sala e olhar para as telas dos computadores portáteis dos alunos para verificar se estes estão cumprindo a tarefa. Olhar para as telas das pessoas sem autorização explícita é normalmente considerado uma invasão de privacidade. No entanto, como a atribuição de tarefas e a verificação do seu cumprimento são ações normais no contexto educativo, este fluxo de informação (da tela do computador portátil) não parece problemático. Mas se um professor verificasse os perfis no TikTok dos alunos durante o fim de semana, este fluxo de informação bem provavelmente suscitaria questões, uma vez que não parece estar relacionado com objetivos educativos. É claro que, se o professor atribuisse aos alunos a realização de um vídeo do TikTok como trabalho de casa, o fluxo de informação poderia ser considerado adequado. Estes exemplos indicam que ações como olhar para a tela do aluno ou para o perfil de um aluno numa rede social não são automaticamente violações da privacidade. Pelo contrário, os fluxos de informação devem ser considerados no contexto e avaliados até que ponto em que medida estão em conformidade com as normas desse contexto.

Estas normas ajudam a regular as interações sociais e a manter os limites em vários tipos de relações. Clientes reconhecem que as empresas e firmas apenas recolhem, utilizam

e divulgam informações de forma adequada às suas funções/papéis – denominada *role appropriate information norms* (“normas de informação apropriadas ao papel”). Quando (e apenas quando) o processamento de informação de uma empresa está em conformidade com as regras e regulamentos relacionados com a posição dessa empresa, é considerado apropriado à sua função ou ao seu papel. Estes salvagam a privacidade ao permitirem apenas o processamento adequado à função, mas permitem algum processamento de informação e, por conseguinte, asseguram alguns dos seus benefícios. O processamento de informação adequado ao papel/à função aproxima o processamento ótimo da informação. Um cenário que ilustra isso é dado por Sloan e Warner (2017), cenário típico de um cliente frequente de loja, no caso, loja de vinhos: Uma vez que beneficia de um melhor serviço ao cliente e de uma maior eficiência, a cliente permite que a empresa recolha algumas informações pessoais. De bom grado, ela fornece à loja o seu endereço de correio eletrónico e o seu CEP para que possam acompanhar as suas compras. A cliente beneficia diretamente da recepção de mensagens de correio eletrónico com anúncios de vendas e, ocasionalmente, com um vale de desconto. Ao utilizar os dados que recolhe para analisar melhor a sua clientela, a empresa consegue armazenar os vinhos que mais interessam aos seus consumidores. Graças a esta eficiência, a loja pode até colocar preços ligeiramente reduzidos. Porém, seguindo a norma informacional de ser apropriado à função/papel, os autores afirmam que os clientes, muito corretamente, fazem certas suposições sobre os limites de como a loja coleta, usa e distribui informações:

**Coleta:** Você supõe que a loja não solicitará informações sobre sua função hepática, não registrará o tipo de roupa que você está usando nem se você está na loja com seu cônjuge ou outro acompanhante. **Uso:** você supõe que a loja não analisará seus padrões de compra para prever sua orientação sexual - mesmo que os pesquisadores de marketing direto tenham estabelecido correlações entre os padrões de seleção de vinhos e a orientação sexual. **Distribuição:** Ao consultar a loja sobre uma festa que está planejando, você presume que a loja não publicará os detalhes da festa em seu site. (Sloan; Warner, 2017, p.83-4).

Porém, há de se reconhecer que todos os clientes terão uma opinião diferente sobre quais devem ser as contrapartidas ao divulgar seus dados pessoais, e tal variedade grande é um problema para todos os clientes da loja porque a loja (de vinhos) certamente não vai fornecer uma política de processamento de dados e informação distinta para cada cliente. No geral, é provável que as decisões das empresas sobre a forma de tratar dados pessoais “conduzam a um compromisso unilateral que favoreça as empresas, em vez de um compromisso que estabeleça um equilíbrio ótimo entre a privacidade e as vantagens do

tratamento da informação” (Sloan; Warner, 2017, p.85). Até um certo ponto, os clientes precisam exigir, então, a coleta exclusiva de dados exclusivamente apropriados à função da empresa (e questionar quando essa coleta não seja apropriada à função).

A privacidade refere ao direito, de todos os seres humanos, de desfrutar da liberdade contra intrusões não autorizadas. Nessa linha, uma definição da privacidade intuitiva é fornecida por Barrett-Maitland e Lynch (2020, p.3) como “[...] a capacidade de controlar as informações sobre si mesmo, bem como a liberdade de não ser vigiado, seguido, monitorado e espionado. Nesse sentido, ignorar os direitos de privacidade geralmente leva à violação dos direitos naturais.” As autoras continuam especificando a “privacidade informacional” como:

[...] a capacidade de controlar o acesso a informações pessoais. O direito de controlar o acesso a fatos ou informações pessoais é, na nossa opinião, um direito natural e inalienável e todos devem ter controle sobre quem vê as suas informações pessoais e como estas são divulgadas. Barrett-Maitland; Lynch, 2020, p.3)

De fato, esses princípios são subjacentes às leis gerais passadas neste século em vários países, como a Lei Geral de Proteção de Dados Pessoais (LGPD- 13709) no Brasil, em 2018 e no mesmo ano, a *General Data Protection Regulation* (GDPR) da União Europeia. Ambas estas leis, como as semelhantes de muitos países pelo mundo afora, regulam a forma como pode-se utilizar, processar e armazenar dados pessoais (informações sobre uma pessoa viva e identificável).

### **3.1 O paradoxo da privacidade**

Na sua revisão da literatura sobre o fenômeno conhecido como o “paradoxo de privacidade”, Kokolakis (2015) nos lembra que foi Brown (2001) que descobriu este paradoxo após uma série de entrevistas aprofundadas com consumidores que compram na Internet. Apesar de as pessoas manifestarem a sua preocupação com a violação da sua privacidade, estavam dispostas a fornecer as suas informações pessoais aos sites comerciantes da Internet se se sentiram que pudessem beneficiar com isso. Outro estudo com consumidores da Internet revelou que, apesar de declararem num questionário pré-experimento que a privacidade é uma das principais preocupações, as pessoas não agem dessa forma quando fazem compras online. Acquisti (2004, *apud* Kokolakis, 2015) e a sua “abordagem de economia comportamental” são citados pelo autor porque defendem que “as pessoas podem não ser capazes de agir como agentes economicamente racionais quando se trata de

privacidade pessoal”. Acquisti desenvolveu um modelo econômico que ajuda a explicar as discrepâncias entre as atitudes e os comportamentos em matéria de privacidade. A tendência para a gratificação imediata é tida em conta neste paradigma, pela qual a propensão para dar maior ênfase às vantagens atuais do que aos potenciais perigos futuros em termos de perdas de dados, informações pessoais – perda de privacidade. De acordo com a avaliação heurística das pessoas, as vantagens da divulgação de informações (*information disclosure*) ultrapassam os futuros riscos para a privacidade. Kokolakis (2015) apresenta 18 estudos na sua revisão que fornecem provas que apoiam a hipótese do paradoxo da privacidade. Entre eles, tem os estudos de Tufekci (2008, *apud* Kokolakis, 2015) que, por meio de um questionário, investigou o comportamento de auto-revelação (*self-disclosure*) dos estudantes nos sítios de redes sociais, e descobriu pouca ou nenhuma relação entre a exposição da sua informação pessoal e as preocupações com a privacidade online. A discrepância entre atitude e comportamento também foi identificada validada por Lee et al. (2013, *apud* Kokolakis, 2015). Avaliaram o impacto do perigo esperado e do ganho esperado no desejo dos usuários de divulgar informações pessoais através de uma experiência e de uma série de entrevistas semiestruturadas aprofundadas: chegaram à conclusão de que os usuários divulgam ativamente informações pessoais, apesar das suas reservas, porque pesam os benefícios esperados da partilha em relação ao perigo (perda de privacidade). Por outro lado, Kokolakis (2015) também sumariza 11 estudos que contestam a hipótese do paradoxo da privacidade. Numerosos estudos no domínio das redes sociais online põem em dúvida a crença generalizada de que os jovens não protegem os seus dados pessoais. Os jovens recorrem a uma série de técnicas de proteção, incluindo a utilização de pseudónimos e o fornecimento de informações falsas (Miltgen; Peyrat-Guillard, 2014 *apud* Kokolakis, 2015), a limitação dos pedidos de amizade, a remoção de *tags* e fotografias e a limitação do acesso aos seus perfis e às definições de privacidade (Boyd; Hargittai, 2010 *apud* Kokolakis, 2015). Nas redes sociais online, o controle da informação e a divulgação/revelação (*disclosure*) não estão diretamente relacionados. A procura de popularidade é o que motiva a divulgação, razão pela qual os jovens divulgam frequentemente informações sensíveis. Por outro lado, a baixa confiança resulta em táticas de controle, como a rejeição de pedidos de amizade para limitar o acesso a perfis pessoais (Christofides et al., 2009 *apud* Kokolakis, 2015).

Por fim, é relevante observar que a maioria das pesquisas sobre este fenómeno tem sido realizado nas redes sociais ou em websites de compras comerciais, mas Kokolakis (2015)

nos lembra que o comportamento de privacidade é um fenômeno altamente contextual, sendo que não devemos esperar que os indivíduos demonstrem o mesmo comportamento em contextos diferentes. Nessa linha, Barrett-Maitland e Lynch (2020) nos lembram como o próprio *modus operandi* dos sites das redes sociais é altamente dependente do compartilhamento intensivo de informações e dados pelos usuários, já que o próprio compartilhamento desses é a forma principal de participar nessas redes e comunidades online. Isto leva à situação em que os usuários estão “normalmente mais dispostos a fornecer informações pessoais e mais privadas nas redes sociais do que em qualquer outro lugar da Internet. Isso pode ser atribuído ao sentimento de comunidade, conforto e família que esses meios de comunicação proporcionam, em sua maioria.” Ao mesmo tempo, esses participantes das redes sociais são eles mesmos responsáveis para proteger seus dados e informações pessoais da coleta de dados por terceiros. Os usuários/participantes podem estar frequentemente *oversharing* (partilha excessiva) informações enquanto realizam atividades do seu dia-a-dia ou atividades nas suas férias, mas ao se utilizarem de serviços baseados em geolocalização, que significa que sua localização em tempo real pode ser identificada com muita precisão, entregando para terceiros seus padrões de movimentação, se tornando um “alvo” para marketing, ou para outras ações que potencialmente infringem mais profundamente sua privacidade e segurança.

#### **4. Procedimentos metodológicos adotados**

Nesta seção, será apresentado e analisado o propósito em torno do método científico denominado “revisão de literatura”. Assim, pretende-se deixar transparente nosso posicionamento metodológico, o qual, com base numa breve revisão da literatura sobre revisão da literatura, explicará a terminologia aqui adotada. Esta pesquisa é exploratória com abordagem quali-quantitativa, e evidentemente, de caráter bibliográfico. Conforme Creswell (2007), a pesquisa é exploratória quando há pouca discussão e trabalhos sobre o tema. A pesquisa tem como base a pesquisa secundária, de síntese, o “trabalho de campo” da qual está baseado na coleta, análise e síntese de documentos escritos. Desse modo, o foco é no estudo teórico-analítico, que, ao focar nos estudos e pesquisas já disponíveis nas bases e sites pesquisadas, buscam um olhar amplo e profundo sobre um determinado tópico. De acordo com Demo (2000, p. 20) “este tipo de pesquisa propõe reconstruir teoria,

conceitos, ideias, ideologias, polêmicas, considerando-se em termos imediatos, aprimorar fundamentos teóricos".

Antes de descrever as etapas da pesquisa bibliográfica realizadas, na sub-seção a seguir, será delineada a discussão acerca da terminologia em torno dos termos “pesquisa bibliográfica” e “revisão da literatura.” Grosso modo, como observa Snyder (2019, p.33): “Uma revisão de literatura pode ser descrita como uma forma mais ou menos sistemática de coletar e sintetizar pesquisas anteriores.” A revisão de literatura pode assumir diferentes funções consoantes com o problema que é objeto da pesquisa. Pode servir para:

Fazer uma descrição recente e atual do corpo de conhecimento relacionado com o tema da pesquisa, dando uma visão geral de um corpo de pesquisa com o qual o pesquisador não está familiarizado;

Revelar o que já foi bem-feito, para que o pesquisador não perca tempo "reinventando a roda".

Fornecer novas ideias que o pesquisador pode usar em sua própria pesquisa.

Ajudar a determinar onde há lacunas, problemas ou falhas na pesquisa existente.

Permitir que o pesquisador coloque sua pesquisa em um contexto maior, para mostrar quais novas conclusões podem surgir;

Explicar os resultados de investigações anteriores, demonstrando como os resultados de um estudo em particular (por exemplo, da pesquisa sendo realizada) se comparam com todos os outros (Knopf, 2006; Creswell, 2007; Snyder, 2019; Codina, 2020; Fink, 2014).

No projeto apresentado para a pesquisa aqui relatada, foi originalmente proposta uma “revisão integrativa” da literatura. De fato, ao longo das leituras iniciais, foi também cogitado realizar uma “revisão sistemática”, e nessa direção, foi seguido um curso online da POCA-UFSCar intitulado “Revisão Sistemática Bibliográfica” com duração de 12 horas (Anexo B). Debrucemo-nos brevemente aqui, então, sobre os diferentes tipos de revisão consideradas e a conseqüente terminologia adotada.

Grant e Booth (2009, p.91) observam que:

[...] embora a necessidade de sintetizar evidências de pesquisa tenha sido reconhecida por mais de dois séculos, foi somente no século XX que os pesquisadores começaram a desenvolver métodos explícitos para essa forma de pesquisa.

No seu artigo, Grant e Booth (2009) identificam nada menos que 14 tipos de revisão nos domínios de saúde e informação, devido à expansão da prática baseada em evidências nesses setores e profissões (por exemplo, fala-se em *Evidence-based Librarianship* e

*Evidence-Based Library and Information Practice* (EBLIP). Usando o framework SALSA (Search, Appraisal, Synthesis, Analysis – Busca, Avaliação, Síntese, Análise) para avaliar os tipos de revisões, identificaram, em artigos de revisão publicados no *Health Information and Libraries Journal*: *critical review*; *literature review*; *mapping review (systematic map)*; *meta-analysis*; *mixed studies review*; *overview*; *qualitative systematic review*; *rapid review*; *scoping review*; *state-of-the-art review*; *systematic review*; *systematic search and review*; *systematized review*; e *umbrella review*. Curioso observar que não encontraram menções de revisões integrativas (*integrative review*).

Toronto e Remington (2020) observam que na literatura, as revisões integrativas e as sistemáticas são frequentemente confundidas, principalmente porque ambas adotam uma abordagem sistemática, diferentemente de uma revisão narrativa, que não adotam tais procedimentos sistemáticos de localização, seleção e avaliação de fontes, pois nas narrativas: “Evidências selecionadas encontradas sobre um determinado tópico geralmente apoiam as opiniões de um revisor ou suposições a priori de um problema (Conner 2014, *apud* Toronto e Remington, 2020, p.2). A revisão integrativa diferentemente da narrativa, contempla fontes de várias comunidades de prática, como ressaltam Cronin e George (2020, p.7): “A revisão integrativa se diferencia ao reunir o que é conhecido sobre um tópico de uma variedade de diferentes comunidades de prática e justapor essas perspectivas para gerar novas áreas de pesquisa. É a integração entre comunidades que é o principal propósito de uma revisão integrativa.” Se se pode, como pesquisador, responder no afirmativo à questão “Você está tentando conectar (*to bridge*) várias comunidades de prática?” (Cronin; George, 2020, p.8), então seria a revisão integrativa que se busca realizar. Por contraste, uma revisão narrativa “desempenha uma função importante ao fazer um balanço do estado da pesquisa dentro de uma comunidade de prática específica e, então, sugerir maneiras pelas quais essa comunidade pode melhorar.”

Não foi o propósito da pesquisa aqui relatada aprofundar as definições e literatura sobre os diferentes tipos de revisão e pesquisa bibliográfica. Porém, cabe ressaltar que esta “mini incursão” nesse campo da literatura foi relevante para o desenho da pesquisa. Pela definição acima da revisão integrativa, e dado a natureza inter-comunidade do tópico da pesquisa (a saber: competência informacional e digital; privacidade e segurança online), este tipo de revisão parecia ser a mais apropriada. Toronto e Remington (2020, p.3) delineiam as diferenças entre as revisões narrativas, integrativas e sistemáticas, algumas das quais seguem no Quadro 1 a seguir:

Quadro 1 – Diferenças entre os três tipos comuns de revisão

	<b>Narrativa</b>	<b>Integrativa</b>	<b>Sistemática</b>
Propósito	Fornecer uma visão geral sobre um tópico de investigação.	Análise crítica da literatura empírica, metodológica ou teórica, que chama a atenção para necessidades futuras de pesquisa.	Responde a uma única questão clínica.
Protocolo de revisão a priori (plano)	Não	Não	Sim — protocolo registro encorajado
Pergunta de revisão	Não	Objetivo amplamente definido e/ou questão(ões) de revisão	Pergunta clínica única geralmente no formato de PICO: P = population, I = intervention, C = comparison, O = outcomes
Uso de uma metodologia de busca sistemática (permite a replicação)	Não	Sim	Sim
Análise e síntese	Análise narrativa	Análise narrativa e/ou temática com síntese descritiva e qualitativa	Análise narrativa e/ou temática com síntese descritiva e qualitativa - pode incluir síntese quantitativa (meta-análise)

Adaptado de Toronto e Remington (2020, p.3)

Fica claro da literatura sobre a revisão da literatura / revisão bibliográfica como método que, dada a complexidade e quantidade da literatura científica que existe hoje, a revisão tem que seguir etapas metódicas, visando a sua possível replicação. Porém, nem sempre uma revisão sistemática é a apropriada, sendo que este tipo tem raízes fortes na área de saúde, emprega protocolos (do tipo PICO) e necessita de no mínimo três pesquisadores para etapas de validação (Codina, 2020; Toronto; Remington, 2020). Adotaremos aqui, então, o termo “revisão *sistematizada*” que, como observam Grant e Booth (2009, p.102-3) “tenta[m] incluir um ou mais elementos do processo de revisão sistemática mas não chegam a afirmar que o resultado é uma revisão sistemática.” Será a fase de pesquisa em bases de dados e outros recursos e fontes que “possui os elementos de sistematicidade mais facilmente identificados [...]”, fase essa em que o pesquisador pode demonstrar sua “conhecimento de todo o processo e sua proficiência técnica” para a recuperação dos

registros e fontes. Esses autores continuam explicando as fraquezas percebidas das revisões sistematizadas que não possuem:

[...] a abrangência tão fundamental para o método de revisão sistemática. [...] Para tais revisões, a avaliação de qualidade e a síntese podem ser menos identificáveis. Isso significa que esses processos não são descritos, que são modelados usando um pequeno conjunto de artigos elegíveis ou que estão completamente ausentes. Embora a tentativa de sistematicidade seja bem-vinda, tais revisões possuem uma maior probabilidade de viés do que aquelas que aderem mais estritamente às diretrizes sobre a conduta de revisões sistemáticas (Grant; Booth, 2009, p.103).

Por outro lado, podemos argumentar aqui que estas revisões sistematizadas, na sua maior flexibilidade, possuem uma maior robustez. Esta robustez pode também ser garantida explicitamente reconhecendo a “bibliodiversidade” da Ciência da Informação, refletida na “diversidade, complexidade e riqueza de propósitos, métodos e perspectivas” (Suri, 2002, p.3) identificáveis na pesquisa publicada nesse campo, os pesquisadores do qual frequentemente têm que “beber em fontes” fora das “fronteiras” disciplinares dela. Suri (2002) reconheceu este ser o caso para o campo da Educação, e então, viu-se diante da necessidade de elaborar um *framework* para “Síntese de Pesquisa Metodologicamente Inclusiva” (MIRS – Methodologically Inclusive Research Syntheses). O modelo MIRS é caracterizado por sua inclusividade metodológica, pois facilita a integração de pesquisa primária que emprega várias orientações metodológicas. Ele acomoda diversos métodos e técnicas de pesquisa primária e é fundamentado em abordagens delineadas em sínteses de literatura que abrangem uma gama de perspectivas metodológicas. Como Suri (2002, p.6) nota: “Within the MRS framework, methodological inclusivity is perceived as an important step to enhance the compatibility between the contemporary methods of primary research and research synthesis.” As recomendações do Suri (2002) são que o pesquisador deve fornecer uma explicação de sua subjetividade e reflexividade, indicando sua posição em relação ao tópico de pesquisa e as implicações que isso pode ter em suas abordagens metodológicas. Além disso, é crucial estabelecer critérios de inclusão claros para garantir um processo de seleção metodologicamente sólido. Assim, advocamos a transparência quanto às tomadas de decisão, explicitação de critérios de inclusão e exclusão de itens de pesquisa usados nesta pesquisa.

Primeiramente – à época de elaborar a proposta de pesquisa – conduzimos uma pesquisa bibliográfica preliminar, com a finalidade de ter uma visão preliminar da produção de literatura sobre o tópico especificamente no campo de Ciência de Informação e de

verificar quais as tendências relativas ao assunto. Com base em uma primeira busca nas bases de dados bibliográficas *Web of Science* (WoS) e *Library and Information Science Abstracts* (LISA), foi possível verificar que havia relativamente poucas publicações sobre o tópico com os termos conjugados (digital literacy AND privacy). Nesse momento, decidimos não aplicar o *framework* PCC – *participants, concept, context* – mais comumente usado nas revisões da literatura do tipo *scoping* (Peters et al., 2020) para estruturar a questão de pesquisa e portanto, estruturar a expressão de busca, sendo que tratava-se da fase mais aberta e exploratória, e o PCC é justamente usado para estreitar o foco num grupo ou população específico (P) atuando num contexto (C) específico, afetado pelo fenômeno (conceito C) sobre estudo. Esta fase ajudou numa familiarização geral sobre o tópico de pesquisa.

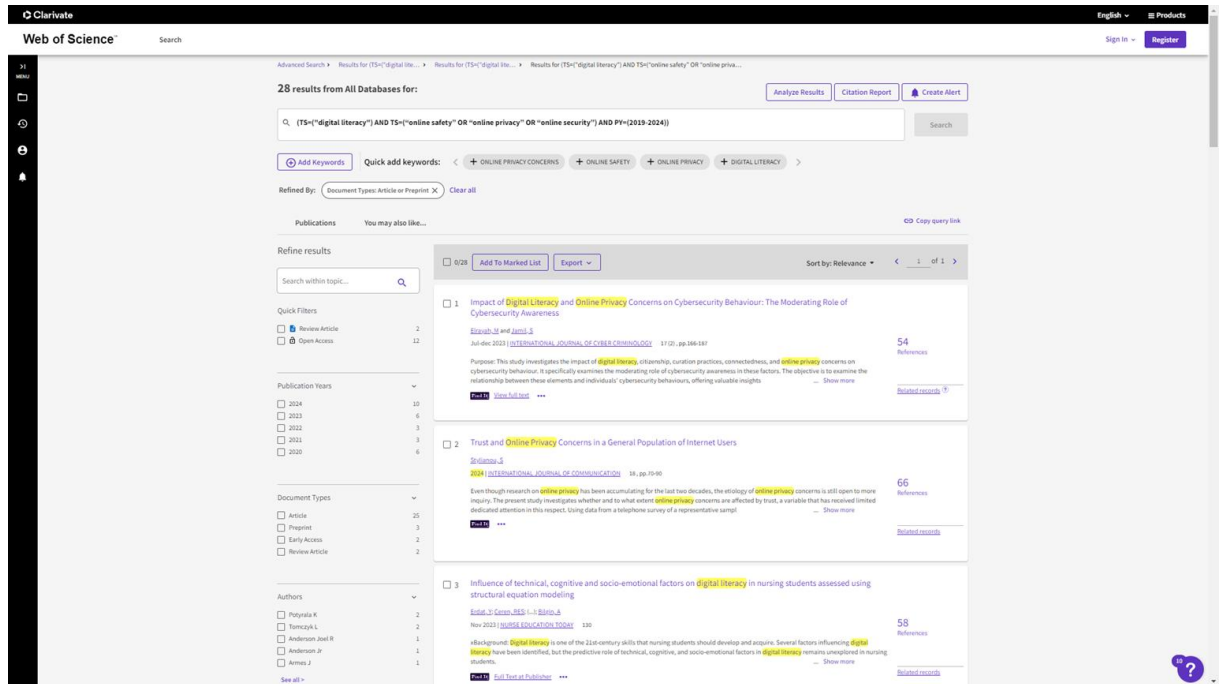
A expressão de busca adotada visou localizar ambos os artigos publicados e não publicados, os *preprints* e a literatura cinzenta sendo incluídos na categoria de não publicados. Uma busca inicial na WoS foi realizada para identificar os primeiros artigos sobre o tópico. Os termos contidos nos títulos e abstracts desses primeiros artigos considerados relevantes foram usados para desenvolver uma estratégia plena (expressão de busca – *search string* – mais filtros e intervalo de tempo) para a WoS. Testada essa expressão de busca na WoS para verificar que recuperasse resultados relevantes, foi então adaptada para cada uma das outras bases de dados pesquisadas: Dimensions, LISA e SCOPUS. Seguem a expressão de busca (*search string*) usada na WoS e a expressão de busca geral usada e adaptada às outras bases:

(TS=("digital literacy") AND TS=("online safety" OR "online privacy" OR "online security") AND PY=(2019-2024))  
 "digital literacy" AND ("online security" OR "online safety" OR "online privacy")

O intervalo de tempo pesquisado foi 2019 – 2024 e filtros como tipo de publicação (artigos, artigos de revisão, livros) e grande área de conhecimento (Ciência da Informação e afins, como Biblioteconomia) foram aplicados.

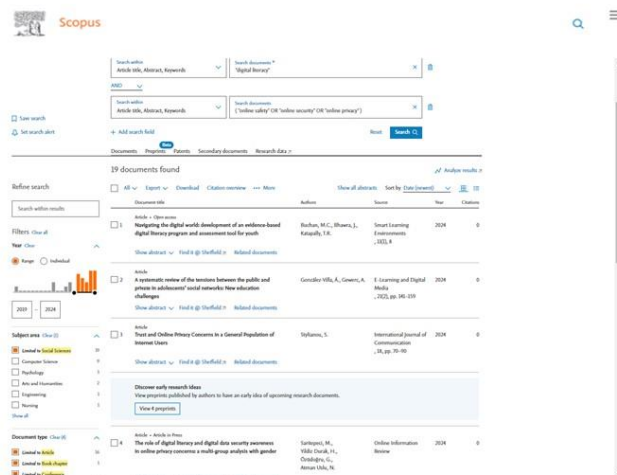
Seguem *printscreens* dessa expressão de busca e filtros aplicados nas bases pesquisadas:

Figura 4 – Expressão de busca da pesquisa na WoS



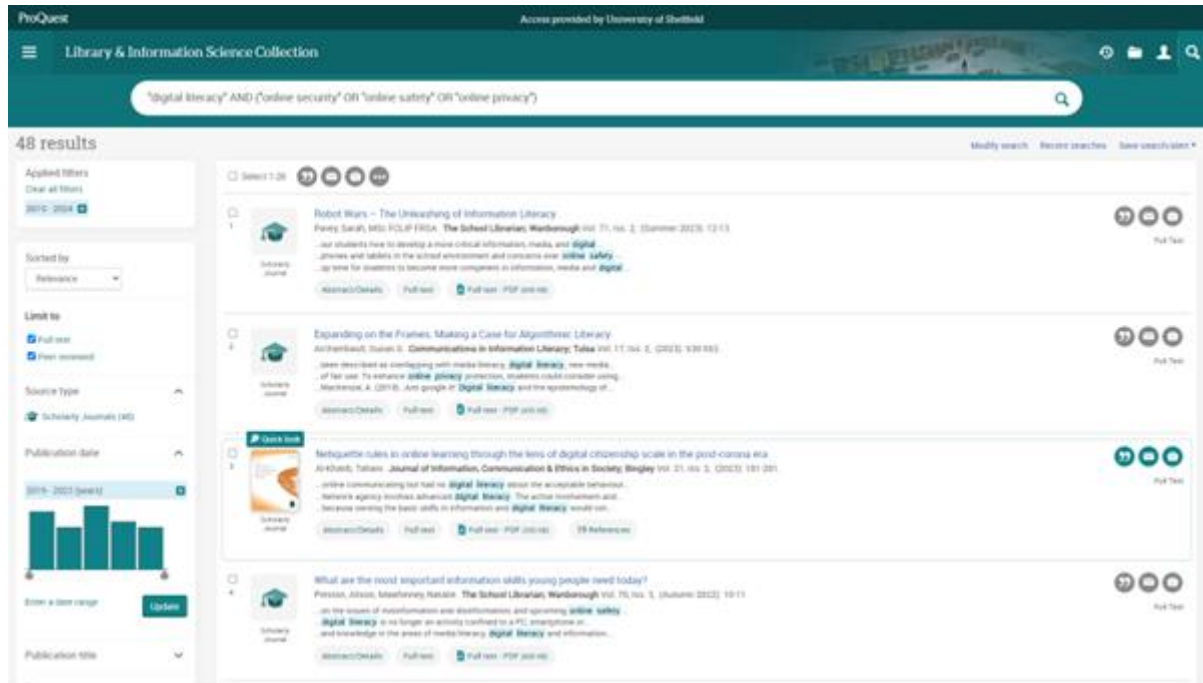
Fonte: Dados da pesquisa (2024)

Figura 5 – Expressão de busca da pesquisa na SCOPUS



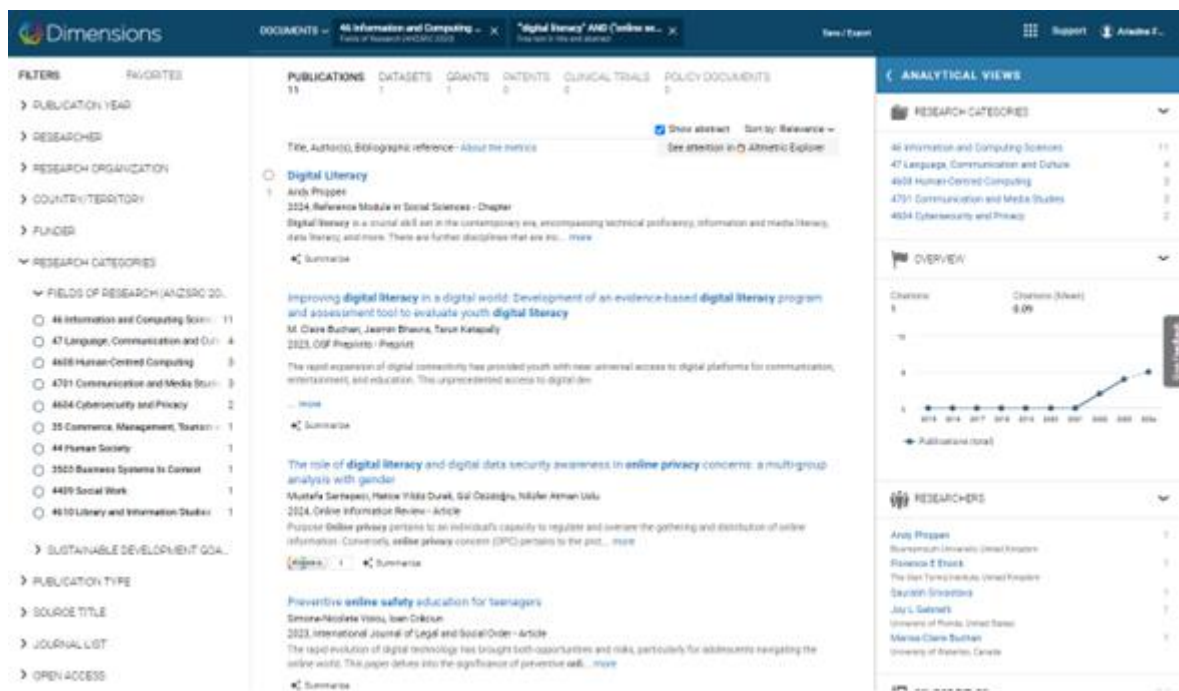
Fonte: Dados da pesquisa (2024)

Figura 6 – Expressão de busca da pesquisa na LISA



Fonte: Dados da pesquisa (2024)

Figura 7 – Expressão de busca da pesquisa na Dimensions



Fonte: Dados da pesquisa (2024)

Os metadados recuperados em cada base de dados foram salvos em planilhas Excel, inicialmente separadamente, e depois, numa planilha só para eliminar as duplicatas. A tabela 1 a seguir apresenta os resultados quantitativos para cada base e o total depois da remoção das duplicatas:

Tabela 1 – Total de registros recuperados, sem duplicatas

Base de dados	Qtde. de registros recuperados com a expressão de busca
Web of Science (WoS)	28
Scopus	19
LISA	48
Dimensions	11
Total	106
<b>Total depois da remoção de duplicatas</b>	<b>83</b>

Fonte: Dados da pesquisa (2024)

O Apêndice A consiste na planilha Excel contendo a lista e metadados dos 83 registros finais depois da remoção das duplicatas. Para uma pesquisadora só, a revisão de 83 artigos ainda representa uma quantidade substancial de artigos – um desafio intelectual. Decidimos, então, usar o software livre Iramuteq<sup>8</sup> para analisar a frequência de termos considerados os mais relevantes para esta pesquisa. Para o uso desse software, é necessário fazer a preparação do *corpus* a ser tratado pelo software. Para tal, primeiramente foi criado um arquivo contendo apenas os textos dos resumos (*abstracts*), cada um precedido pela linha de comando exigida pelo Iramuteq, a saber: \*\*\*\* \*Abstract\_01 até \*\*\*\* \*Abstract\_83 (Apêndice B). Antes de inserir esse corpus no software Iramuteq para processamento, também foi necessário realizar uma “limpeza manual” dele, tirando, por exemplo, marcações de pontuação como aspas, dois pontos e hífenes, para que, por exemplo, um termo como e-Government foi substituído com eGovernment, COVID-19 com COVID\_19, e assim em diante. Outro passo importante nessa limpeza é de escolher termos recorrentes nos resumos que mais descrevem o tópico da pesquisa e juntá-los com o *underline* usando o recurso do editor de texto “encontrar e substituir”. O *underline* funciona assim, como se os termos compostos estivessem entre aspas, o que se faz comumente em pesquisas em bases de dados e no

<sup>8</sup> Disponível em [www.iramuteq.org](http://www.iramuteq.org). Para aprender seu uso básico, assisti às Partes 1 & 2 do minicurso “Análise textual com auxílio do software IRAMUTEQ: noções básicas” organizado pelo Grupo de Pesquisa Kaizen – ESUFRN disponível em: <https://www.youtube.com/watch?v=VD5BC8IJrOk>

Google. Nessa linha, os seguintes termos presentes no *corpus* dos resumos foram ajustados para o formato na segunda coluna do Quadro 2 a seguir:

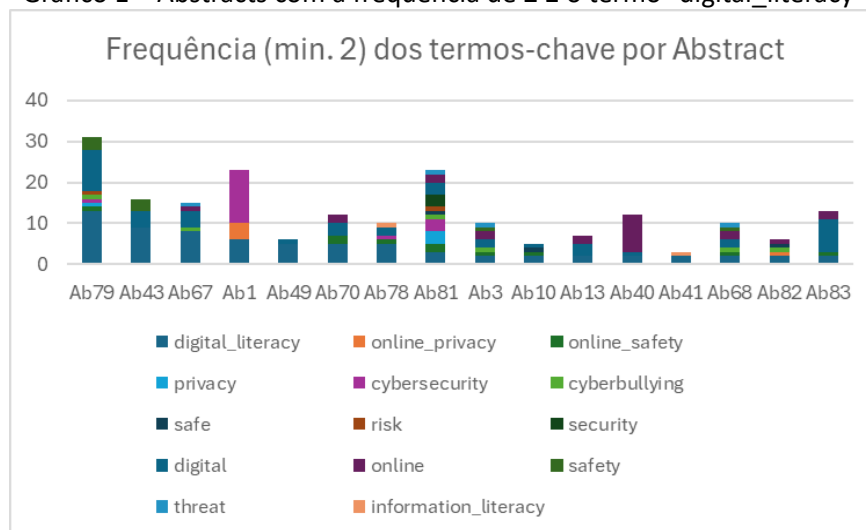
Quadro 2 – Termos em formato aceitável para o software Iramuteq

Termo como aparece no resumo	Termo no formato necessário para Iramuteq
digital literacy	digital_literacy
online privacy	online_privacy
online safety	online_safety
online security	online_security
information literacy	information_literacy
digital media literacy	digital_media_literacy
media literacy	media_literacy
privacy literacy	privacy_literacy
data privacy	data_privacy
digital safety	digital_safety

Fonte: Dados da pesquisa (2024)

Foi utilizado o recurso do software Iramuteq que realiza a contagem da frequência de termos, o que auxiliou na redução do número de artigos a serem lidos, para uma quantidade factível para uma pesquisadora só. Decidimos, nessa primeira etapa, efetuar a “nota de corte” de no mínimo frequência de 2 vezes o termo “digital\_literacy”, significando que reduziu-se a quantidade de resumos para 16 resumos (*abstracts*), como se vê no Gráfico 1 e na Tabela 2 que seguem.

Gráfico 1 – Abstracts com a frequência de  $\geq 2$  o termo “digital\_literacy”



Fonte: Dados da pesquisa (2024)

Na Tabela 2 incluímos, para fins demonstrativos, até o *Abstract* número 20, sendo que os últimos 4 dessa lista contém apenas 1 frequência do termo “digital\_literacy”, mas na

listagem completa, havia 18 resumos que contém o termo *digital\_literacy* uma vez, e o restante (n=49) não o contém que é algo notável, dado a expressão de busca usada para a recuperação dos artigos.

Tabela 2 – Frequência dos termos-chave em 20 Resumos (*Abstracts*)

Abstract Resumo	digital_literacy	online_privacy	online_safety	privacy	cybersecurity	cyberbullying	safe	risk	security	digital	online	safety	threat	ormation_literacy
n.79	13	0	1	1	1	1	0	1	0	10	0	3	0	0
n.43	9	0	0	0	0	0	0	0	0	4	0	3	0	0
n.67	8	0	0	0	0	1	0	0	0	4	1	0	1	0
n.01	6	4	0	0	13	0	0	0	0	0	0	0	0	0
n.49	5	0	0	0	0	0	0	0	0	1	0	0	0	0
n.70	5	0	2	0	0	0	0	0	0	3	2	0	0	0
n.78	5	0	1	0	1	0	0	0	0	2	0	0	0	1
n.81	3	0	2	3	3	1	1	1	3	3	2	0	1	0
n.03	2	0	1	0	0	1	0	0	0	2	2	1	1	0
n.10	2	0	1	0	0	0	1	0	0	1	0	0	0	0
n.13	2	0	0	0	0	0	0	0	0	3	2	0	0	0
n.40	2	0	0	0	0	0	0	0	0	1	9	0	0	0
n.41	2	0	0	0	0	0	0	0	0	0	0	0	0	1
n.68	2	0	1	0	0	1	0	0	0	2	2	1	1	0
n.82	2	1	0	0	0	1	1	0	0	0	1	0	0	0
n.83	2	0	1	0	0	0	0	0	0	8	2	0	0	0
n.02	1	1	0	8	0	1	0	1	0	4	2	0	0	0
n.04	1	0	2	0	0	0	0	4	0	2	4	0	0	0
n.05	1	0	2	0	0	0	0	0	0	3	2	2	3	0
n.08	1	1	0	2	0	0	0	1	0	2	1	0	0	0

Fonte: Dados da pesquisa (2024)

O Quadro 3 apresenta uma relação dos metadados dos 16 artigos considerados os que mais parecem atender aos critérios da pesquisa. Apêndice C contém os resumos desses 16 artigos.

Quadro 3 – Metadados dos 16 artigos que mais atendem aos critérios da expressão de busca

Abstract	Referência
79	BUCHAN, M. Claire; BHAWRA, Jasmin; KATAPALLY, Tarun. Improving digital literacy in a digital world: Development of an evidence-based digital literacy program and assessment tool to evaluate youth digital literacy. <b>OSF Preprints</b> . 2023.
43	OH, Sarah Soyeon; KYOUNG-A, Kim; KIM, Minsu; OH, Jaeuk; Sang Hui Chu; CHOI, JiYeon. Measurement of digital literacy among older adults: systematic review. <b>Journal of medical Internet research</b> , v. 23, n. 2, p. e26145, 2021.
67	TOMCZYK, Lukasz; EGER, Ludvík. Online safety as a new component of digital literacy for young people. <b>Integration of Education</b> , v.24, n.2, p.172-184. 2020.
01	ELRAYAH, Musaddag; JAMIL, Saima. Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness. <b>International Journal of Cyber Criminology</b> , v. 17, n. 2, p. 166–187.2023.
49	IGBO, Harriet Uche. Undergraduates’ Digital Literacy and Access to Information in Nigerian University Libraries: Does Subject Background Make a Difference?. <b>Library Philosophy and Practice</b> , Oct. 2020. p.1-25
70	NABHAN, Salim. Pre-service teachers’ conceptions and competences on digital literacy in an EFL academic writing setting. <b>Indonesian Journal of Applied Linguistics</b> , v. 11, n. 1, p. 187-199, 2021.
78	PHIPPEN, Andy; BOND, Emma. Online safeguarding and personal cyber skills for students. In: <b>The Emerald Handbook of Higher Education in a Post-Covid World: New Approaches and Technologies for Teaching and Learning</b> . Emerald Publishing Limited, 2022. p. 245-264.
81	FAZIL, Abdul Wajid et al. Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. <b>American Journal of Education and Technology</b> , v. 2, n. 4, p. 50-61, 2023.
03	JULIEN, Heidi; GERSTLE, David; DETLOR, Brian; LA ROSE, Tara; SERENKO, Alexander. Digital Literacy Training for Canadians, Part 1: “It’s... Just Core Public Works”. <b>The Library Quarterly</b> , v. 91, n. 4, p. 437-456, 2021.
10	Kang, Eun Jin; Kim, Amie; Lee, Jiun. International Comparative Study on Digital Media Literacy Elements in National Early Childhood Curricula in Finland, Canada, Australia, and South Korea. <b>Korean Journal of Child Studies</b> , v. 43, n. 4, p. 525-537, 2022.
13	ASLAN, Ayse; MOLD, Freda; VAN MARWIJK, Harm; ARMES, Jo. What are the determinants of older people adopting communicative e-health services: a meta-ethnography. <b>BMC Health Services Research</b> , v. 24, n. 1, p. 60, 2024.
40	MARTZOUKOU, Konstantina. Academic libraries in COVID-19: a renewed mission for digital literacy. <b>Library management</b> , v. 42, n. 4/5, p. 266-276, 2021.
41	JOHNSON, Matthew Weirick; LASHER, Meggie. The community workshop series: A case study for community-engaged learning in LIS. <b>Library Trends</b> , v. 69, n. 4, p. 752-767, 2021.
68	POTYRAŁA, Katarzyna; TOMCZYK, Łukasz. Teachers in the lifelong learning process: examples of digital literacy. <b>Journal of Education for Teaching</b> , v. 47, n. 2, p. 255-273, 2021.
82	TRIRATNAWATI, Atik; HIDAYAH, Sita; LAZUARDI, Elan. 'Menjadi Pelajar Cakap Digital': Proyek Bersama Webinar dan Sosialisasi Kecerdasan Digital di Madrasah Muallimat Muhammadiyah Yogyakarta. <b>Bakti Budaya: Jurnal Pengabdian kepada Masyarakat</b> , v. 5, n. 1, p. 10-24.
28	KUMAR, Priya C; BYRNE, Virginia L. The 5Ds of privacy literacy: a framework for privacy education. <b>Information and Learning Science</b> , v.123, n.7/8, p.445-461, 2022.

Artigo número 10 tinha que ser imediatamente excluído porque é escrito na língua coreana, embora o resumo estruturado e palavras-chave recuperados estivessem na língua inglesa, tal como alguns dos resultados desse artigo, apresentados em quadros. Este estudo teria sido particularmente interessante a analisar, pois propôs analisar o currículo nacional coreano para a primeira infância (*Korean national early childhood curriculum - Currículo Nuri*) do Coreia do Sul, visando uma direção para a sua revisão para incorporar aspectos relevantes para o que denominam “letramento midiático digital.” Os autores realizaram um estudo comparativo desse conteúdo presente nos currículos da primeira infância na Finlândia, no Canadá (Ontário) e na Austrália. Artigo 82 também foi excluído porque é escrito na língua indonésia, embora o resumo estivesse na língua inglesa, e as palavras-chave desse artigo exibem bastante pertinência para a pesquisa à mão: *data privacy; digital literacy; cyberbullying; time management; young people*. Cabe ressaltar que o filtro nas bases de dados pesquisadas foi ativado para somente selecionar textos na língua inglesa ou portuguesa. Cabe observar, também, que ambos estes artigos excluídos foram recuperados usando a base de dados Dimensions, o que possivelmente aponta uma falha com esta base de dados.

A recursividade inerente ao método adotado levou, e após leitura cuidadosa dos 14 resumos restantes, à decisão de agrupá-los em subconjuntos temáticos para fins de revisar esses subconjuntos, inclusive de forma comparativa. Identificamos artigos que trataram de competência digital e privacidade/ segurança online relacionada a: 1) Crianças, adolescentes, jovens, da idade escolar; 2) Professores do primeiro e segundo grau; 3) Universitários; e 4) Idosos e 5) Cidadãos - pessoas da comunidade em geral. No quadro 4 que segue, é apresentado esse agrupamento.

Quadro 4 – Agrupamento temático dos artigos recuperados

Grupos estudados	Referência
1. Crianças, adolescentes, jovens	79. BUCHAN, M. Claire; BHAWRA, Jasmin; KATAPALLY, Tarun. Improving digital literacy in a digital world: Development of an evidence-based digital literacy program and assessment tool to evaluate youth digital literacy. <b>OSF Preprints</b> . 2023.
	67. TOMCZYK, Lukasz; EGER, Ludvík. Online safety as a new component of digital literacy for young people. <b>Integration of Education</b> , v.24, n.2, p.172-184. 2020.
	81. FAZIL, Abdul Wajid et al. Enhancing Internet safety and cybersecurity awareness among secondary and High School students in Afghanistan: A case study of Badakhshan Province. <b>American Journal of Education and Technology</b> , v. 2, n. 4, p. 50-61, 2023.

Grupos estudados	Referência
	28. KUMAR, Priya C; BYRNE, Virginia L The 5Ds of privacy literacy: a framework for privacy education. <b>Information and Learning Science</b> , v.123, n.7/8, p.445-461, 2022.
2. Professores	68. POTYRAŁA, Katarzyna; TOMCZYK, Łukasz. Teachers in the lifelong learning process: examples of digital literacy. <b>Journal of Education for Teaching</b> , v. 47, n. 2, p. 255-273, 2021. 70. NABHAM, Salim. Pre-service teachers' conceptions and competences on digital literacy in an EFL academic writing setting. <b>Indonesian Journal of Applied Linguistics</b> , v. 11, n. 1, p. 187-199, 2021.
3. Universitários	40. MARTZOUKOU, Konstantina. Academic libraries in COVID-19: a renewed mission for digital literacy. <b>Library management</b> , v. 42, n. 4/5, p. 266-276, 2021. 49. IGBO, Harriet Uche. Undergraduates' Digital Literacy and Access to Information in Nigerian University Libraries: Does Subject Background Make a Difference?. <b>Library Philosophy and Practice</b> , Oct. 2020. p.1-25 78. PHIPPEN, Andy; BOND, Emma. Online safeguarding and personal cyber skills for students. In: <b>The Emerald Handbook of Higher Education in a Post-Covid World: New Approaches and Technologies for Teaching and Learning</b> . Emerald Publishing Limited, 2022. p. 245-264.
4. Idosos	13. ASLAN, Ayse; MOLD, Freda; VAN MARWIJK, Harm; ARMES, Jo. What are the determinants of older people adopting communicative e-health services: a meta-ethnography. <b>BMC Health Services Research</b> , v. 24, n. 1, p. 60, 2024. 43. OH, Sarah Soyeon; KYOUNG-A, Kim; KIM, Minsu; OH, Jaeuk; Sang Hui Chu; CHOI, JiYeon. Measurement of digital literacy among older adults: systematic review. <b>Journal of medical Internet research</b> , v. 23, n. 2, p. e26145, 2021.
5. Cidadãos	01. ELRAYAH, Musaddag; JAMIL, Saima. Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness. <b>International Journal of Cyber Criminology</b> , v. 17, n. 2, p. 166–187.2023. 03. JULIEN, Heidi; GERSTLE, David; DETLOR, Brian; LA ROSE, Tara; SERENKO, Alexander. Digital Literacy Training for Canadians, Part 1: "It's... Just Core Public Works". <b>The Library Quarterly</b> , v. 91, n. 4, p. 437-456, 2021. 41. JOHNSON, Matthew Weirick; LASHER, Meggie. The community workshop series: A case study for community-engaged learning in LIS. <b>Library Trends</b> , v. 69, n. 4, p. 752-767, 2021.

## 5. Análise dos resultados

A escola é a instituição que, mais do que qualquer outro ator social, organização ou instituição, encarregada de educar e manter níveis de competência (letramento) em várias dimensões - seja em meio digital, informacional ou midiática, entre outras. As escolas desempenham um papel especial, principalmente porque o atendimento escolar é obrigatória na maioria dos países. O sistema educacional em todas as nações desempenha um papel em estabelecer normas, valores e padrões comuns. Durante a escolaridade, os alunos são ensinados a discernir o que é visto como conhecimento para participar produtivamente da sua sociedade. Ademais, nas democracias, a escola é normalmente considerada não apenas um local de instrução, mas também como uma que promove a democracia, e a competência digital desempenha um papel crucial em relação a esse duplo objetivo. Mesmo assim, os alertas constantes de pais, especialistas e legisladores sobre como o entretenimento virtual nas redes sociais, os rastreadores da web e os algoritmos de recomendação aumentam o radicalismo político e o acesso fácil a conteúdo ilícito e ilegal geralmente não levaram a um ajuste de como as escolas abordam a educação em mídias digitais. Este paradoxo leva Buckingham (2015, p.24) a observar que os políticos e legisladores rapidamente fomentam

[...] ansiedades sobre pornografia online e pedófilos, ou jovens assistindo a vídeos de recrutamento do Isis, ou *'fake news'*, mas são de alguma forma incapazes de digerir a ideia de que podemos ensinar os jovens a serem críticos da mídia. Eles estão ansiosos para despejar muita tecnologia de mídia nas escolas, mas resistem à ideia de que podemos usá-la como algo diferente de uma ferramenta instrumental.

Os alunos têm tido, de forma consistente, tarefas escolares que os obrigam a obter dados sem a ajuda de ninguém, por exemplo, visitando a biblioteca ou consultando um livro de referência. Muitas nações têm visto uma mudança nos métodos de ensino que colocam mais ênfase nas investigações dos alunos do que na pedagogia centrada no professor ("giz-e-conversa"). Essa mudança coincidiu com o aumento da popularidade das teorias de aprendizagem socioculturais e construtivistas, que ressaltam, respectivamente a necessidade de avanço individual dos alunos na construção de conhecimento (construtivismo) ou a necessidade de aprender junto com outros em ambientes naturais (teorias socioculturais). A ênfase na própria investigação e aprendizagem independente dos alunos torna o educador em maior medida um tutor ou gerente, enquanto a instrução convencional face-a-face relega o professor ao trabalho de um "contador de verdades" definitivas (ensino bancário, nos

termos freirianos). Por outro lado, mesmo os educadores mais progressistas e construtivistas têm auxiliado seus alunos com a avaliação de fontes aplicando critérios de qualidade e confiabilidade, e fidelidade fatural (Sundin; Francke, 2009). Durante e desde a década de 1990, novos avanços de aprendizagem computadorizada foram introduzidas nas escolas. Livros de referência em CD-ROM e outras bases de informações controladas por qualidade, foram logo suplantados por versões online. A última parte da década de 1990, ferramentas de busca na web amplamente úteis e, mais tarde, a Wikipedia, tornaram a pesquisa por informações muito mais direta, e simultaneamente, “a obrigação em relação ao controle de qualidade foi transferida, até um certo grau, de distribuidores (*publishers*) e educadores para alunos” (Haider; Sundin, 2022, p.93). De acordo com essa reviravolta, os pesquisadores se tornaram progressivamente interessados em como os alunos se organizam para buscar e avalia as fontes digitais de informação para trabalhos escolares, e, no caso da Kuhlthau (2004), por exemplo, como alunos escolares (no contexto norteamericano) realizam tais tarefas cognitiva e emocionalmente. Hoje, diante da concorrência intuitiva da web gratuito (que frequentemente leva os alunos à Wikipédia), os recursos informacionais editados e produzidos de forma controlada ficam, para todos os efeitos, deixados para trás.

Embora seja incentivado a adquirir uma atitude crítica em relação a conteúdo e informação que são tidas como certas, o chamado currículo baseado no conhecimento pode ser visto como um desafio a essa abordagem crítica. Mas um olhar crítico não foi aplicado à própria infraestrutura de informações até recentemente, se é que foi aplicado. Ser capaz de fazer uma pesquisa rápida no Google é uma coisa; entender a função do Google e como a "mundan-ificação" e a "pesquisa-ificação" da vida cotidiana (Sundin et al., 2017) reorganizam constantemente as hierarquias sociais do conhecimento na sociedade moderna é bem diferente: Saber como avaliar criticamente uma notícia é uma coisa, mas compreender o ecossistema de notícias no qual as plataformas de mídia social funcionam é outra bem diferente.<sup>9</sup>

---

<sup>9</sup> Estas preocupações dos vários stakeholders tem sido recorrentemente apresentadas e discutidas nas séries de seminários promovidos pelo Nic.br: "TIC Kids Online Brasil" disponíveis em: <https://www.youtube.com/watch?v=v8-CkzBzIA8> e a série "Privacidade e proteção dos dados" disponível em: <https://www.youtube.com/watch?v=odQZ9ospfPQ>

## 5.1 Revisão dos artigos recuperados

### 5.1.1 Crianças, adolescentes, jovens

No estudo realizado (na segunda parte do ano 2016) por **Tomczyk e Eger (2020)** com jovens na faixa etária de 15 a 21 anos na Polónia, os autores objetivaram avaliar o nível de conhecimentos, habilidades e atitudes relacionados com a segurança online desse grupo de usuários. Os autores aderem à definição do letramento digital como necessário para aumentar a competência dos alunos na área de habilidades virtuais, conhecimento, conscientização e uso de mídias sociais. Subscrevem às definições do termo que enfatizam a tríade – competências, habilidades e atitudes. Para eles, o DL se refere ao conjunto de habilidades técnicas, mas também à capacidade de reconhecer os problemas relacionados às TDIC como o *cyberbullying*, *sexting* e a proteção da imagem. Para medir essas competências relacionadas à segurança online, os autores desenvolveram uma ferramenta de avaliação focando nessas dimensões de DL. Essa ferramenta foi na forma de um questionário dividido em duas seções, a primeira cobrindo aspectos do perfil demográfico do respondente, e a segunda mediu o nível de DL em relação à segurança digital nas seis áreas: 1. criação e gestão de imagem pessoal na Internet; 2. *sexting* e invasão de privacidade (incluindo conhecimento das consequências jurídicas da roubo de identidade, violação da imagem e imagem e aspectos técnicos da proteção de dados, remoção de fotografias indexadas pelo motor de busca mais popular da Polónia); 3. violação dos direitos de autor; 4. cyberbullying (sensibilização para os mecanismos ligados ao cyberbullying, tipos de ciberassédio e capacidade de assegurar as respectivas provas); 5. operações financeiras na Internet; 6. capacidade de avaliar a confiabilidade da fonte de informações e dos vendedores em lojas on-line. O questionário foi preenchido por 1.693 alunos com idade entre 15 e 21 anos (média = 16,8, DP = 1,17). A amostra consistiu de 848 meninas (50,1%) e 845 meninos (49,9%), embora os resultados mostraram que o gênero não determina os médios gerais da competência. Além disso, as escolas que implementaram programas para melhorar o nível de Letramento Digital em termos de segurança obtiveram resultados semelhantes àqueles em que tais programas não foram introduzidos. A análise detalhada dos componentes do LD relacionados à segurança digital revela que o gênero influencia o conhecimento e as habilidades para determinados elementos. As meninas obtiveram resultados um pouco mais altos nas áreas como *sexting*, credibilidade das informações e *cyberbullying*. Os meninos, por sua vez, detêm de mais conhecimento das questões técnicas, como proteção da propriedade

intelectual e segurança das operações financeiras. No geral, 41,41% dos respondentes lidam com ameaças digitais relativamente bem, conhecem os mecanismos e as *e-threats*, bem como as medidas de prevenção e proteção. No entanto, os autores identificaram que 24.5% dos respondentes obtiveram os resultados mais baixos em quase todas as áreas – não ultrapassaram o nível de 40% de respostas corretas em quatro das seis áreas constituintes da dimensão do letramento digital para segurança online.

O fortalecimento das competências úteis no mundo on-line se traduz em outras habilidades úteis off-line (p.180). Este texto apresenta os resultados da pesquisa entre os adolescentes. Esse grupo mostra o nível avançado de LD em comparação com pessoas em estágios anteriores de educação, mas, ao mesmo tempo, devido à idade, esses entrevistados estão expostos a ameaças eletrônicas adicionais [27-29]. A natureza desse estágio de desenvolvimento exige o fortalecimento do LD, especialmente nas áreas em que os resultados dos testes foram mais baixos, como os direitos autorais [30]. Essa área refere-se principalmente ao download e ao compartilhamento de músicas, vídeos, software ou e-books. As questões de segurança digital geralmente não fazem parte do escopo de interesses dos jovens usuários de TIC. No entanto, os altos resultados obtidos, por exemplo, na área de operações financeiras on-line podem sugerir que as atividades que os jovens realizam com frequência (como procurar informações sobre vendedores, fazer compras, enviar transferências seguras de dinheiro) são a base para a construção de conhecimento nessa área (conforme comprovado pelos resultados de nossa pesquisa). As diferenças estão também relacionadas com o local de residência. Os resultados gerais do teste foram muito mais baixos nas zonas rurais do que nas cidades. À luz do crescente uso problemático da Internet (tempo excessivo de tela, levando ao uso do neologismo "screenagers"), o DL também significa a capacidade de exercer autocontrole sobre o uso da mídia digital. Assim, o DL torna-se um novo construto, dinamicamente transformador, usado para descrever as mudanças que estão ocorrendo na sociedade da informação.

No texto de **Buchan, Bhawra e Katapally (2023)**, os autores fazem um mapeamento dos programas de letramento digital existentes no Canadá desenvolvidos especificamente para jovens, bem como as ferramentas de avaliação de letramento digital. Citando vários autores sobre o assunto, observam que o foco nos jovens é deliberado, pois, embora os jovens sejam geralmente considerados como exibindo maior competência digital, sua dependência de plataformas digitais no dia-a-dia os coloca em risco em um cenário digital em rápida mudança. Identificaram 15 programas de letramento digital que visam várias

componentes, como a segurança dos dados, o cyberbullying e os meios digitais. Além disso, foram identificadas 12 ferramentas de avaliação da literacia digital. De todos os grupos demográficos, os jovens têm-se tornado cada vez mais dependentes da tecnologia e da Internet para comunicação, socialização, entretenimento e, mais recentemente, educação (Bach et al., 2018). Desde aplicações de redes sociais a jogos online e recursos educativos, a tecnologia digital tornou-se parte integrante das rotinas diárias de muitos jovens a nível mundial (Pérez-Escoda et al., 2020; The Lancet Child & Adolescent Health, 2018). 80-96% dos jovens canadianos com idades compreendidas entre os 13 e os 24 anos possuem ou têm acesso a smartphones (Rideout et al., 2022; Secretariat & Secretariat, n.d.; Vernon et al., 2018). As estatísticas do Canadá indicam que os estudantes canadianos do 4.º ano são mais propensos a utilizar um computador ou um *tablet* em casa para os trabalhos escolares do que a média mundial (Governo do Canadá, 2020). Em contrapartida, o continente africano apresenta a percentagem mais substancial da sua população (88%) sem qualquer forma de ligação à Internet (UNICEF, 2018).

Os autores observam que apesar da prevalência de riscos online, as pesquisas mostram um baixo nível de letramento digital entre os jovens, principalmente em áreas com conectividade digital limitada, isto é, em áreas rurais (Bhawra et al., 2022; Schreurs et al., 2017). Cabe destacar as questões da pesquisa dos autores aqui, quais sejam: 1. a) Existem programas ou *frameworks* de letramento digital para jovens no Canadá? b) Quais são as principais áreas temáticas (por exemplo, segurança de dados, cyberbullying) dos programas/*frameworks* de letramento digital? 2) Quem é o público-alvo dos programas/*frameworks* de letramento digital existentes? E por fim: 3. a) Quais ferramentas de avaliação e/ou questionários estão sendo usados atualmente para avaliar os níveis de letramento digital? b) Há alguma ferramenta de avaliação de letramento digital adaptada para jovens? Como resultados, os autores identificaram 13 *frameworks*, programas e organizações de letramento digital, cobrindo tópicos como introdução à informática, ética e empatia, cibersegurança, privacidade dos dados, literacia de dados, envolvimento da comunidade, saúde digital, sensibilização dos consumidores (*consumer awareness*), meios de comunicação e artes digitais e inteligência artificial. Disponibilizam, ao final do texto num apêndice, um quadro de detalhes de cada programa. Identificaram uma série de programas no Canadá dedicados a melhorar letramento digital dos jovens, sendo que a maioria desses programas se concentra em equipar os jovens com habilidades em ciência da computação e ciência de dados, programação e desenvolvimento de IA. Ao mesmo tempo em que a experiência

prática proporcionada por muitos desses programas visa preparar os alunos para carreiras nas áreas de ciência, tecnologia, engenharia e medicina, os autores observam que a principal limitação de muitos dos programas parece ser a priorização de habilidades técnicas em detrimento de conceitos essenciais relacionados a comportamento on-line aceitável, ética, propriedade de dados, segurança e privacidade. Uma exceção notável foi a iniciativa "Usar, Entender, Criar" da empresa Media Smarts (2022)

Os autores também desenvolveram um programa de letramento digital direcionado a adolescentes e jovens, sendo que na parte do programa que aborda privacidade e segurança visa educar os jovens sobre o conceito de privacidade em sua vida cotidiana e como ele se relaciona com o uso da Internet, a importância das senhas, os vírus digitais e o roubo de identidade. Com base nos pontos fortes e fracos dos programas identificados, desenvolveram um programa de fácil utilização e flexível do ponto de vista de onde poderia ser ministrado (tanto nas escolas, casas e centros comunitários ou bibliotecas públicas). Ademais, os autores levantaram 18 ferramentas de avaliação do letramento digital, e também desenvolveram sua própria ferramenta de avaliação para avaliar a mudança nos níveis de letramento entre a implementação pré e pós-programa.

No artigo de **Fazil, Hakimi, Sajid, Quchi e Khaliqyar** (2023), os autores abordam o assunto de letramento digital de jovens de uma região de Afeganistão (província de Badakhshan), do ponto de vista da literatura mais específica sobre "educação em cibersegurança" (*cybersecurity education literature*). Isto é, eles focam esta dimensão do letramento digital no seu estudo de caso, que procurou esclarecer o estado atual da educação em segurança cibernética na referida região e examinar o impacto da educação para a cibersegurança no letramento digital e na segurança online entre os alunos lá. Com o olhar para outros países como o Reino Unido, Japão e Índia, eles buscaram, analisar a eficácia de diferentes abordagens e oferecer percepções que poderiam informar o desenvolvimento de diretrizes padronizadas para incorporar a educação em cibersegurança nos currículos escolares do país deles. Os sete objetivos do estudo de caso são bastante amplos, por exemplo: "investigar o tempo médio que os estudantes passam diariamente na Internet diariamente e identificar variações com base no gênero e categorias etárias" (Fazil et al., 2023, p.52), mas o sétimo objetivo – "Investigar a conscientização dos alunos sobre questões de segurança cibernética, suas experiências com ameaças ou incidentes cibernéticos e suas respostas a esses incidentes" – é o que interessou mais a revisão nossa. Mesmo sendo um estudo de caso, Fazil e co-autores basicamente usaram um único

instrumento de coleta de dados (além da revisão teórica) que foi um questionário com 16 questões estruturadas usando uma escala Likert, e questões abertas, a análise das quais usaram o software SPSS. Aplicaram o questionário a 170 estudantes, a distribuição dos respondentes sendo exatamente 50% para cada gênero. Os autores também realizaram uma oficina sobre segurança na Internet e cibersegurança (que infelizmente, não descrevem no artigo, somente mencionam). Observam que depois de administrar a oficina, a sensibilização sobre passos a seguir em relação à cibersegurança pessoal subiu, demonstrada, por exemplo, num salto de consciência sobre a necessidade de se utilizar senhas fortes e seguras – de 67% dos participantes sabendo disso antes da oficina para 82% depois. No que diz respeito à incidência de assédio online (*online harassment*), os dados levantados pelos autores chocam, por causa da sua prevalência: 40% dos pesquisados tinha sofrido falsificação de sua identidade; 32% dos alunos tinha sido afetado pela invasão de contas de redes sociais ou e-mail; 22% dos alunos relataram casos de assédio por manipulação de imagem; 6% dos participantes sofreram assédio por causa da revelação de segredos pessoais; cerca de 16% sofreram extorsão financeira; 4% das respostas dizem respeito a abusos sexuais online. Os autores observam que antes da oficina, os conhecimentos dos alunos eram extremamente baixos e decepcionantes, ao ponto de nem sequer compreendiam o conceito de cyberbullying, e um dado preocupante que identificaram é que 61% dos respondentes mencionaram que não pedem conselhos a ninguém quando sofrem o cyberbullying.

No artigo de **Kumar e Byrne** (2022), o foco é direcionado para o que chamam “letramento da privacidade” (*privacy literacy*) e propõe delinear objetivos e diretrizes de aprendizagem baseados em teorias da privacidade para servir de base às iniciativas de letramento da privacidade que entendem como ausentes nos currículos escolares (nos EUA) para o ensino de pré-adolescentes. Concentram nessa faixa etária porque “os pré-adolescentes estão apenas começando a usar a mídia social (Rideout e Robb, 2019) e estão deixando de confiar nos conselhos dos pais para entender as interações online e passando a fazer seus próprios julgamentos” (p.446). O ponto de vista epistemológico das autoras é que ambas o letramento e a privacidade são práticas sociais, contextuais. O letramento da privacidade não pode ser reduzido a um conjunto de fatos sobre privacidade mas é sobre ter as habilidades para interpretar situações sociais e agir de forma alinhada com a privacidade, é de divulgar informações de uma forma que se alinha com as normas de um determinado contexto, “ adotar um fluxo de informações apropriado.” As autoras aprofunda o conceito da privacidade, trazendo a importante observação que a privacidade é algo muito dinâmica e

contextual, evoluindo constantemente, evolução que corresponde às mudanças nas condições tecnológicas e sociais, que também estão sendo constantemente produzidas e reproduzidas. Por exemplo, a privacidade entra em cena quando informações (textuais, imagéticas) são trocados entre pessoas numa interação social ou quando dados pessoais são analisados por sistemas de IA. Isto implica que a interpretação da informação embute a consideração sobre se tal troca respeita ou infringe a privacidade das pessoas envolvidas. O letramento digital nesses contextos aponta para a compreensão das consequências sociais desses fluxos informacionais. Citando a literatura sobre o tópico, as autoras explicam que as pessoas, incluindo as crianças e pré-adolescentes, As crianças, incluindo os pré-adolescentes (10-13 anos), experimentam a privacidade em três contextos sociais: interpessoal, institucional e comercial. O primeiro engloba

[...] fluxos de informação que moldam as relações com a família e os amigos (por exemplo, uma criança que envia mensagens de texto a um pai ou publica vídeos do TikTok para os amigos verem). Os contextos institucionais incluem fluxos de informação com entidades públicas, como as escolas (por exemplo, um pai que envia os dados pessoais de um filho para registro escolar). Os contextos comerciais envolvem fluxos de informação com atores com empresas, muitas vezes para fins de marketing (por exemplo, um jogo móvel que recolhe os dados de uma criança para publicidade).(p.448)

As crianças e pré-adolescentes predominantemente atuam no contexto interpessoal, e tendem a minimizar (subestimar) os riscos que as ameaçam. As autoras citam pesquisas que demonstram que a preocupação que os pré-adolescentes e crianças têm com privacidade é de proteger sua informação pessoal sendo exposta em situações potencialmente embaraçosas, ao passo que os pais e professores querem proteger a privacidade de crianças e adolescentes, impedindo que suas informações caiam nas mãos de predadores sexuais, o que reflete “uma fissura mais ampla entre as abordagens dos adultos e das crianças à vida digital, em que os adultos veem perigo e necessidades de segurança, as crianças veem a ligação e formas de envolvimento social (Fisk, 2016; Ito et al., 2009; James, 2014)” (p.449)

As autoras citam vários estudos que demonstram que ao ocultar ou excluir informações de espaços on-line, alterar configurações de privacidade, publicar informações enganosas e alternar entre contas e plataformas, os pré-adolescentes adotam a privacidade (Davis e James, 2013; De Leyn et al., 2021; Stoilova et al., 2020). Eles aprendem a tomar decisões sobre privacidade, como quais informações devem ser divulgadas e quando, por meio de conversas com pais, amigos e irmãos (Bauwens et al., 2020; Davis e James, 2013). Eles também absorvem crenças sobre o valor da privacidade de suas famílias (Bauwens et al.,

2020; De Leyn et al., 2021). Além de ouvir sobre escândalos de privacidade notáveis, como o caso da Cambridge Analytica, os alunos também “aprendem fazendo” - investigando e brincando com as ferramentas e os programas que usam (Stoilova et al., 2020). Os pré-adolescentes afirmam ter ouvido falar de assuntos relacionados com a privacidade, como cookies, geolocalização, definições de privacidade e partilha de informações na escola (Stoilova et al., 2020), mas também afirmam que os conselhos dos professores são frequentemente reduzidos a clichés como “Evite interagir com estranhos” ou “Não publique informações pessoais online” (Davis; James, 2013, p. 19). É provável que os pré-adolescentes compreendam que os julgamentos relativos à partilha de informações exigem uma maior profundidade, embora estas orientações universais possam ser úteis para as crianças mais novas (Kumar et al., 2020).

Frente a sua análise dos conceitos de privacidade, as autoras propõe “As 5Ds do letramento em privacidade” que são direcionados não às crianças e pré-adolescentes, mas aos profissionais que elaboram iniciativas educacionais e programas em letramento digital com foco na privacidade. As 5Ds são:

- (1) Definir o fluxo de informações (ou seja, identificar o tipo de informação, o assunto, o remetente, o destinatário e o meio).
- (2) Descrever os papéis sociais, o contexto e as normas envolvidas no fluxo de informações.
- (3) Discernir como o fluxo de informações poderia afetar (positiva e negativamente) outras pessoas em sua comunidade e fora dela.
- (4) Determinar se o fluxo de informações está alinhado com as normas apropriadas do contexto.
- (5) Decidir se deve adotar o fluxo de informações, modificá-lo ou interrompê-lo.

As autoras apresentam um exemplo da “regra universal”: “não compartilhe ou revele senhas”. Aplicando cada uma das 5Ds a um trecho de uma fala de uma aluna de 10 anos, em que ela revela que há certas situações em que ela compartilharia, sim, a sua senha do navegador Chrome se fosse com uma amiga com quem desenvolve um trabalho escolar, as autoras explicam como os 5Ds de letramento em privacidade não são prescrições de comportamento com respostas certas ou erradas. Eles constituem um método para avaliar uma circunstância e fazer uma escolha que seja consistente com as expectativas de cada um num determinado contexto. Trata-se de uma atividade diária que tanto os adultos como as crianças praticam atualmente. As crianças aprendem as normas sociais sobre os fluxos de informação e estabelecem opiniões sobre o que é ou não adequado, como resultado da

tentativa de negociar as circunstâncias sociais. Por exemplo, a jovem de 10 anos defendeu a razão pela qual a partilha de senhas nem sempre é uma violação da privacidade. Mesmo que não tenham a linguagem para o expressar, as crianças moldam ativamente as suas próprias ideias sobre privacidade. Assim, o objetivo da educação para a privacidade não é o de professores, adultos transmitirem – “depositar em” para usar o termo freiriano (que as autoras também citam) – conhecimentos a(em) crianças, mas é o de “ajudar as crianças a abordar o processo de privacidade com mais intencionalidade, considerando ativamente como os fluxos de informação moldam a sociedade.” Para Kumar e Byrne (2022), o letramento da privacidade, é, acima de tudo, um entendimento da privacidade como o fluxo apropriado de informação, entendimento esse que se distingue dos entendimentos “tradicionais” da privacidade como controle e proteção. Nessa linha, é importante destacar que as autoras afirmam que a privacidade *não* deveria ser conjugada com o tema de segurança online (*online safety*). Vale citar diretamente as autoras sobre este ponto importante (elas mesmas baseando-se nas suas revisões de outros autores, como pode ser visto na citação a seguir):

Embora adultos e crianças possam responder visceralmente à importância da segurança, os esforços de segurança on-line "têm sido criticados por perpetuar práticas conservadoras e avessas ao risco que limitam as oportunidades de aprendizado e comunicação digital" (Pangrazio; Cardozo Gaibisso, 2020, p. 50). A segurança on-line pode até se tornar uma justificativa para que adultos e instituições monitorem e restrinjam as atividades digitais das crianças, violando a privacidade delas em nome da segurança (Fisk, 2016; Wisniewski et al., 2022). Para que as lições de privacidade ajudem as crianças a entender como os fluxos de informação moldam a sociedade, conforme refletido nos 5Ds do letramento em privacidade, elas devem ser incorporadas a outros tópicos além da segurança. Esforços recentes para desenvolver materiais educacionais voltados para a privacidade fundamentaram suas lições no letramento digital ou na cidadania digital (James et al., 2021; DiFranzo et al., 2019; Maqsood; Chiasson, 2021), algo que apoiamos, embora também observemos que esses esforços continuam a enquadrar a privacidade como uma questão de segurança ou proteção, em vez do fluxo apropriado de informações. (Kumar; Byrne, 2022, p.453)

As autoras objetivam promover a incorporação dos princípios da privacidade nos currículos escolares existentes (nos EUA), mas reconhecem que será um grande desafio para o professorado porque no geral, não foram preparados para isso. Por isso, elas enfatizam como será importante fomentar espaços de aprendizagem tipo “ensino baseado em problema” e colaborativos para evitar cenários em que os professores são vistos como figuras de autoridade, detentores do conhecimento “certo”. Além disso, as autoras

recomendam a adoção do paradigma de ensino-aprendizagem freireano dialógico para garantir que exista reconhecimento e respeito pelo conhecimento prévio que os jovens já detêm sobre a privacidade, e que este pode ser o ponto de partida de outras oportunidades de ensino-aprendizagem.

### 5.1.2 Professores e competência digital

Os próximos dois artigos do conjunto de 14 abordam a questão dos professores no cenário de letramento digital. O ponto de partida do texto de **Potyrala e Tomczyk (2021)** chama a atenção para o fato que na maioria dos países, a política educacional não fornece aos professores orientação sobre como o letramento digital se traduz em suas habilidades digitais, apesar do interesse crescente nessa área. Muitos educadores se sentem despreparados para ajudar seus alunos a fazer uso eficiente das TDIC como resultado. A questão de pesquisa que norteou o estudo desses autores era “qual é o nível de letramento digital relacionado à segurança digital entre os professores?” Para os autores, o termo “segurança digital” se refere aos seguintes aspectos: conscientização sobre ameaças eletrônicas, capacidade de proteger dispositivos digitais e antecipação de situações problemáticas, como cyberbullying. Aplicaram um questionário a professores de ensino de segundo grau (high school), que coletou dados sociodemográficos e dados sobre seu uso diário das TDIC. A terceira seção foi composta por uma avaliação das habilidades dos respondentes no que tange aos seus conhecimentos e habilidades relativos segurança digital em seis domínios: 1) proteção da imagem on-line (conhecimento sobre: como funciona o *snapchat*, configuração da visibilidade de uma postagem no Facebook, mecanismos de criação de contas em SNS - Social Network Sites); 2) *sexting* (conhecimento sobre os aplicativos mais comuns usados pelos adolescentes para trocar imagens eróticas, as consequências do *sexting* no contexto da disseminação de informações e remoção de imagens da Internet); 3) direitos de propriedade intelectual (conhecimento sobre o download de arquivos protegidos por direitos autorais, reconhecimento das consequências legais do download ilegal de vídeos protegidos por direitos autorais e download de software de repositórios de arquivos populares para apoiar o processo didático); 4) avaliação da confiabilidade das informações disponíveis on-line (conhecimento das tentativas de obtenção de senhas para as ferramentas de administração eletrônica da escola, capacidade de reconhecer plágio nas tarefas dos alunos e verificação da identidade dos proprietários de sites); 5) cyberbullying (capacidade de reconhecer as consequências do cyberbullying,

capacidade de classificar atividades on-line no contexto de cyberbullying e agressão eletrônica e capacidade de garantir evidências de cyberbullying); 6) proteção contra malware (conhecimento sobre vírus e phishing e capacidade de reconhecer protocolos seguros de troca de dados). Responderam 484 professores do terceiro ciclo de ensino (escolas secundárias) na Polónia, sendo 402 mulheres (82,9%) e 82 homens (17.1%), e a idade média dos participantes era de 43,87 anos. A amostragem foi aleatória, e responderam professores da área rural além das cidades grandes. Os professores exibiram conhecimentos e competências mais avançados relacionados com a proteção da imagem online e o sexting, áreas essas conectadas e, de acordo com os autores, as mais comuns nos grupos com que os respondentes trabalham. Os elementos mais fracos do letramento digital são, preocupantemente, a avaliação da confiabilidade da informação online e as questões relacionadas com os direitos de autor. O único tópico que exibiu uma distribuição relativamente homogêneo nas respostas foi aquela sobre seus conhecimentos sobre cyberbullying (DADOS), e os únicos resultados que revelaram uma correlação com o gênero da/da respondente foi aquilo sobre ferramentas para a proteção de dispositivos contra malware (*trojans, viruses, spyware*), com uma diferença de 12% dos respondentes masculinos alcançando um *score* mais alto para essas questões comparados com as mulheres. Nas respostas em torno da sua autoavaliação de seu letramento digital, os autores observam que se os professores se autoavaliam como tendo bons conhecimentos sobre aspectos técnicos, então também tenderam a se autoavaliarem como também tendo bons conhecimentos sobre aspectos de segurança (*e-threats* ou ameaças eletrônicas, como denominam no texto), como mostrado na tabela 3:

Tabela 3 - Autoavaliação do nível de experiência em mídia digital e conhecimento sobre ameaças eletrônicas

	Como você avalia seu nível de alfabetização e conhecimento relacionado a ameaças eletrônicas?		Como você avalia seu nível de alfabetização e conhecimento relacionado ao uso de dispositivos digitais (PC, tablet)?	
	Quantidade	%	Quantidade	%
Não sei	18	3,71	11	2,27
Alto	125	25,82	149	30,78
Médio	253	52,27	244	50,41
Baixo	57	11,77	30	6,19

Muito baixo	13	2,68	5	1,03
Outro	1	0,2	-	-
Muito alto	17	3,51	45	9,29

Fonte: Potyrała; Tomczyk, 2021, p. 264

Como mostra a tabela, a maioria dos participantes autoavaliaram seu DL como “médio”. Observam os autores que se um professor achar que suas habilidades relacionadas à mídia digital são altas em uma área, por exemplo, manutenção técnica, ele também declarará que seu conhecimento e suas habilidades em relação às ameaças eletrônicas estão em um nível semelhante.

Porém, na seção de avaliar as competências digitais dos professores, os autores do estudo destacam que cerca de 49% dos professores não forneceram mais de 60% das respostas corretas. Mais de um em cada 10 revela um nível muito baixo de conhecimentos e competências relacionadas com a utilização dos meios digitais no contexto da segurança (resultados inferiores a 40%). A heterogeneidade dos resultados ficou particularmente elevada entre os professores em início de carreira e estagiários, ou seja, nesse grupo, os conhecimentos e as competências digitais são os mais diversos.

O *sexting* e a segurança das imagens são as duas primeiras áreas da literacia digital que, na maior parte dos casos, são avaliados como satisfatórios. Por terem participado em cursos de auto-aprendizagem e aprendizagem não formal (cursos, formações), os professores que responderam tinham um conhecimento comparativamente avançado destes assuntos. Devido às condições difíceis que podem encontrar no seu trabalho, têm também um conhecimento empírico mais aprofundado sobre a troca de fotografias privadas entre jovens ou sobre o roubo de identidade. De fato, os autores identificaram que os respondentes exibiram menos conhecimento sobre copyright, direitos autorais e avaliação da confiabilidade da informação encontrada online. Os autores verificaram que os resultados do teste de competências digitais foram mais consistentes no domínio do cyberbullying: uma vez que o cyberbullying é uma das ameaças eletrônicas mais bem estudadas, os educadores estão mais conscientes do seu funcionamento e criaram iniciativas preventivas que são cada vez melhores.

Por fim, observam que os professores constroem o seu próprio DL interagindo com os problemas dos jovens e ajudando-os a encontrar respostas adequadas. Mas é também importante reconhecer que existe um subconjunto de educadores que parece “temer”

envolver-se na ajuda aos jovens com os seus problemas relacionados com os meios digitais, apontando para a necessidade de formar professores nessas habilidades cruciais para como atuam, tanto no mundo profissional face-a-face quanto nos ambientes digitais.

No seu artigo, **Salim Nabham** (2021) apresenta os resultados da sua pesquisa, realizada numa universidade na Indonésia, que examinou as concepções de letramento digital dos professores em formação num contexto de escrita acadêmica em *English as a Foreign Language* e identificou as competências dos professores em formação no que diz respeito às dimensões predominantes do letramento digital, que abrangem o pensamento crítico, as competências de segurança online, a cultura digital, a colaboração e a criatividade, a busca pela informação, a comunicação e as competências funcionais. Os dados foram recolhidos através de dois métodos diferentes: qualitativo e quantitativo. Os questionários com questões fechadas e abertas foram preenchidos por 107 professores em formação, e foi realizado um grupo focal com cinco pessoas escolhidas randomicamente. Os **resultados** mostraram que a maioria dos participantes expressaram que a sua percepção do letramento digital permaneceu a um nível básico, focando predominantemente em aspectos técnicos, como usar ferramentas digitais e saber da existência de certas ferramentas e plataformas para a tarefa à mão. Isto é, a ideia de letramento digital não foi totalmente compreendida, de acordo com o autor, no sentido em que incorpora não só o conhecimento de como utilizar plataformas digitais, mas também a criatividade, a segurança eletrônica e as competências de pensamento crítico necessárias para avaliar e analisar a informação.

Porém, observamos que a própria concepção do autor do artigo no que tange à dimensão de competência digital que lida com a segurança online, foge aspectos diretamente relacionados, em nossa opinião, à segurança e privacidade. Especificamente, o autor incluiu enunciados no questionário (com escala Likert de concordância >> discordância) nessa seção que abordam outras questões, a saber:

Q7 Estou ciente dos direitos autorais ou da propriedade de qualquer material on-line. Q8 Consigo entender as questões de segurança quando estou on-line. Q9 Entendo o que é plágio. Q10 Coloco os créditos (autores) ao citar referências on-line, como revistas on-line, livros ou outros. Q11 Verifico meu artigo usando um verificador de plágio on-line antes do envio/publicação. (, 2021, p.193)

Como o autor não explicita sua própria concepção e fontes em que baseia sua concepção de segurança online, e os componentes da mesma, entendemos aqui que é difícil se alinhar com a concepção reducionista dela nesse estudo, que parece focar demasiado em aspectos em torno do plágio e citação de fontes.

De acordo com o estudo de (2021), de modo geral, os resultados indicam que os professores se detêm de uma compreensão do letramento digital limitada a um conjunto de competências, tais como a capacidade de utilizar um dispositivo ou uma aplicação, a pesquisa de informações em linha e a comunicação. Os professores em formação eles mesmos demonstraram competência na procura de informação, na comunicação e nas competências práticas, apesar da sua falta de conhecimento do pensamento crítico e da cultura digital em relação ao letramento digital.

### **5.1.3 Universitários e competência digital visando a privacidade e segurança**

No artigo de **Konstantina Martzoukou (2021)**, a autora foca no papel e atuação que o pandêmico de COVID-19 suscitou para as bibliotecas universitárias pelo mundo afora. As bibliotecas universitárias precisavam se adaptar, com muita celeridade, às novas condições de ensino e aprendizagem que o pandêmico acarretou. A autora observa que as bibliotecas universitárias, pré-COVID-19, já tinham uma longa história de não apenas oferecer serviços e produtos online, mas também oferecer treinamentos e ministrar aula, principalmente na área de letramento informacional, e por causa dessa familiaridade com ambientes online, os profissionais dessas bibliotecas podem aproveitar dessa experiência acumulada, uma oportunidade em termos de gestão, que a autora identifica. Por outro lado, um potencial “risco” apresentado na era pós-pandêmica, é que a oferta de serviços biblioteconômicos convencionais, centrados principalmente em materiais tangíveis e interações presenciais, pode ser questionada ou considerada menos essencial pelos estudantes ou funcionários, já acostumados à interrupção prolongada do funcionamento do campus. Este fato pode ainda ser apoiado pelas falsas crenças generalizadas de que o conhecimento necessário pode ser encontrado livremente em linha com apenas um clique, que são predominantes na sociedade e frequentemente em ambientes educativos. De qualquer modo, a autora afirma que as bibliotecas universitárias têm agora um compromisso redobrado em ajudar os estudantes nos ambientes online a tornarem-se experientes tecnológica, informacional e digitalmente, bem como em fornecer-lhes as ferramentas de que necessitam para colmatar o fosso digital e combater a desigualdade. O desenvolvimento de competências digitais é essencial tanto para a educação dos estudantes como para a luta contra a desinformação, as notícias falsas e a desinformação; no entanto, não existe atualmente um objetivo definido no ensino superior e há interesses concorrentes neste domínio. As bibliotecas universitárias

estão numa boa posição para servirem de fio condutor que fará avançar uma visão estratégica centrada na equidade na educação. A autora observa também que elas podem ajudar os estudantes de diversas origens a ultrapassar as barreiras socioculturais ao acesso à informação em linha e a desenvolver as suas competências digitais. As bibliotecas acadêmicas estão também numa boa posição para mudar a forma como os estudantes usam a informação online para aprender, se envolver, interagir e criar, sensibilizando o pessoal acadêmico para as questões atuais relacionadas com a informação e letramento digital. Porém, no que diz respeito aos temas de privacidade e segurança online especificamente, a autora não se detém no tópico, apenas mencionando o crescimento e exposição à desinformação da “infodemia” que acompanhou a pandemia.

No artigo da **Harriet Uche Igbo** (2020), é apresentados os resultados de um estudo que objetivou determinar se a disciplina acadêmica tem alguma influência na capacidade dos estudantes universitários nigerianos de “aplicarem o letramento digital para acessarem informações” (Igbo, 2020, p.4) nas instituições de ensino superior nigerianas. A pesquisa foi norteada pela seguinte hipótese: O estudo será orientado pela seguinte hipótese: “Não existe uma diferença significativa entre as médias das respostas dos estudantes universitários, em função da sua formação acadêmica, sobre o grau de acesso à informação digital.” (Igbo, 2020, p.5) A população foi constituída por 50.132,00 estudantes de graduação matriculados em 13 universidades federais do sul da Nigéria, sendo que esses estudantes têm acesso a bibliotecas digitais, que permitem aos que não têm computadores pessoais efetuar pesquisas de informação utilizando as instalações e os recursos da biblioteca. Foi utilizada uma técnica de amostragem em várias fases para selecionar uma amostra de 1.506 estudantes universitários, o que representa 5% do número total de 30.121 graduandos de sete universidades do sul da Nigéria. O instrumento utilizado foi um questionário de 37 itens denominado *Digital Literacy and Access to Information Questionnaire – DLAIQ*, e entende-se, implicitamente (porque não há menção de uma fonte externa desse instrumento no texto do artigo sendo revisado aqui) que foi a autora quem desenvolveu esse instrumento. Foram devolvidos 1.375 (90%) dos 1.506 questionários enviados, dos quais 1.274 (85%) foram considerados adequados para o estudo. Em todos os quesitos avaliados no questionário que a autora do estudo entende compreendem “letramento digital” – quais sejam: uso de editor de texto, competências operacionais básicas de PCs, uso de formatos de arquivos e suportes de armazenamento, competências de correio eletrônico, uso de tecnologias para recuperar, organizar, analisar e comunicar informações e utilizá-las para a tomada de decisões

específicas e a resolução de problemas e uso de redes sociais – os estudantes das áreas das humanidades e artes tiveram um desempenho abaixo da média (as pontuações médias gerais sendo 2,73 para Ciências/Tecnologia, 2,47 para Ciências Sociais e 1,99 para Artes/Humanidades), assim refutando a hipótese de que não existiria uma diferença entre competências digitais em função da área de estudo, o que está em acordo com as pesquisas citadas pela autora, de Mahmood (2009), Whitmire (2002) e Kid (2002), segundo as quais os estudantes universitários de ciências possuem, em geral, conhecimentos e competências mais elevados na utilização das tecnologias do que os estudantes de áreas não científicas, e essa diferença se deve “à natureza das suas áreas de estudo”. A autora conclui observando que o principal obstáculo que impede todos os alunos de “utilizarem o letramento digital” (Igbo, 2020, p.20) é a falta ou a inadequação da educação, da formação e dos ambientes de apoio para melhorar a sua capacidade de obter informações para a resolução de problemas na sala de aula. Nesse sentido, ela continua, os resultados têm algumas implicações para as bibliotecas, especialmente na área do planejamento e implementação de programas de formação para os estudantes, com vista ao desenvolvimento de competências digitais aplicadas ao acesso à informação. Crítica do artigo: visão reducionista de letramento digital, focando nas competências em relação a aspectos tangíveis das ferramentas.

O contexto do artigo de **Andy Phippen e Emma Bond** (2022) foi a mudança das aulas universitárias para o ambiente online durante a pandemia do COVID-19 e as implicações dessa mudança particularmente da perspectiva de colocar os universitários em risco como resultado. Os autores iniciam o artigo com a observação de que durante muitos anos, a maioria dos debates educativos e políticos sobre os efeitos negativos da Internet tem-se centrado nas crianças e nos adolescentes em idade escolar, com especial ênfase em questões relacionadas com os meios de comunicação social, como o sexting e a cyberbullying. No entanto, enfatizam que tais efeitos nocivos continuam na idade adulta, mas que as universidades, nos países que estudam (principalmente o Reino Unido e Austrália, Canadá) não foram preparadas para lidar com tais casos entre suas comunidades. Colocam uma crítica da crença generalizada de que os chamados “nativos digitais” (termo cunhado por Prensky nos anos 1990) são “naturalmente” mais adeptos ao uso das tecnologias digitais, e assim sendo, como se fosse um processo osmótico, eles também entenderão dos riscos da vida online, e como mitigá-los. Mesmo se esse estereótipo tenha sido desmascarado, ainda perdura no discurso popular. Ao mesmo tempo que tem existido essa crença infundada, (Veletsianos et al., 2018) os autores chamam a atenção para como, de um modo mais geral,

existe relativamente pouca investigação sobre as experiências dos adultos em matéria de assédio e abuso em linha, sendo dada maior atenção à usurpação de identidade em linha, aos *scams* e fraudes financeiras online. Por meio de um pedido usando a lei FOI (*Freedom of Information*) – equivalente à LAI brasileira – os autores objetivaram identificar se as universidades tinham uma política claramente definida em matéria de assédio, abuso e discurso de ódio online. O raciocínio atrás do levantamento foi que seria impossível para uma instituição de ensino superior responder de forma coerente e uniforme a incidentes reportados sem terem uma política claramente definida que todo o pessoal da instituição siga. Além disso, queriam identificar a frequência dos incidentes registados relacionados com o abuso em linha nas instituições. Para começar, os autores identificaram um pressuposto, por parte das instituições, na época da migração online das atividades de ensino durante a pandemia de que, uma vez que os sistemas online tem sido utilizados para alguns aspectos das atividades universitárias, como o correio eletrónico para comunicação e as plataformas de aprendizagem para a divulgação de materiais didáticos, as pessoas da comunidade estariam, de alguma forma, intuitivamente aptos a passar para a entrega totalmente em linha sem necessidade de formação, mesmo a mais básica. Porém, o que se tornou evidente, foi que havia tanta necessidade de conhecimentos de cibersegurança como de apoio aos estudantes. Um exemplo básico: os servidores das universidades que entrevistaram relataram casos de “Zoombombing” (que se refere ao haqueamento ou sequestro do espaço didático online de sala de aula por atores ilegítimos, com a consequente divulgação de matéria totalmente inapropriado nesse espaço). Os autores foram surpreendidos pelos resultados que levantaram pois em 60% dos casos das instituições que afirmaram possuir políticas e processos administrativos para lidar com assédio moral e sexual, na verdade, essas políticas não mencionaram casos de assédio sexual na modalidade online. Não é tratado como um comportamento abusivo distinto, e naquelas políticas que mencionam as redes sociais, quando tratando do comportamento correto nessas redes, se limitam a descrever comportamento do tipo “pensar antes de publicar” ou “checar seus fatos” do que do abuso, discurso de ódio ou assédio de pessoas. Os autores insistem que o abuso e assédio online são, sim, qualitativamente distintos dos seus semelhantes no presencial. Como os autores explicam:

[...] permite um alcance geográfico muito maior do que o abuso no campus e pode ser mantido através de múltiplas plataformas e dispositivos. No fundo, não há como escapar. Além disso, o “*pile-on*”, quando um agressor encoraja outros a participarem no abuso em linha, não é algo que possa ser facilmente replicado num ambiente offline. Sabemos, através dos nossos muitos anos de investigação nesta

área, que o abuso online é frequentemente considerado como “brincadeira” - algo que deve ser tolerado como um aspeto esperado do envolvimento em plataformas em linha. Considerar o abuso online como uma mera faceta do assédio no seu sentido mais tradicional não contribui em nada para aumentar a sensibilização para estas questões no setor, para avaliar a gravidade do impacto ou para que as universidades estejam mais atentas e levem a sério o abuso online nos seus campus, sejam eles físicos ou virtuais. (Phippen; Bond, 2022, p.11)

Os autores são levados a concluir que as fracas políticas institucionais suscitam procedimentos fragilizados de reportagem de incidentes além da falta das instituições assumirem seu dever de diligência (ou “dever de cuidado” – *duty of care*) para com os seus estudantes. Os autores observaram como muitas das universidades recorreram à “justificativa” de que universitários “não são menores de idade” para se isentarem dessa responsabilidade. Os autores concluem que, pelo menos à época quando realizaram o levantamento, o setor de ensino superior é um setor “em modo reativo.” Os autores são categóricos que este tipo de ensinamento deveria acompanhar estudantes para o lugar de trabalho, e deveria ser ensinado também para os servidores e professores das universidades. Ademais, insistem que não é o tipo de conteúdo que:

[...] possa ser resolvido com um vídeo opcional de formação em linha e um questionário de escolha múltipla, é necessária uma formação sólida ministrada por especialistas, e é crucial que seja realizada numa perspetiva de mitigação dos riscos e de redução dos danos, e não numa perspetiva preventiva. Um aspeto fundamental deste processo tem de ser o conhecimento da cibersegurança. Um estudante que compreenda os princípios básicos da cibersegurança, como as boas práticas em matéria de senhas, a gestão dos seus dispositivos e o controlo do acesso, tem muito menos probabilidades de ser vítima de roubo de identidade ou de abuso online, uma vez que os seus dispositivos digitais estarão mais bem protegidos. O mesmo se aplica ao pessoal [da universidade] - não podemos partir do princípio de que, pelo fato de já possuírem um celular e utilizarem as redes sociais, são magicamente capazes de gerir uma sala de aula em linha sem algum tipo de formação e apoio. (Phippen; Bond, 2022, p.11).

#### 5.1.4 Idosos e competência digital para segurança online

No artigo de **Sarah Soyeon Oh, Kyoung-A Kim, Minsu Kim, Jaeuk Oh, Sang Hui Chu e JiYeon Choi (2021)**, os autores tomam como ponto de partida que o melhoramentos na utilização da tecnologia digital pelos idosos e a sua participação na mesma é crucial para promover a sua saúde e bem-estar geral. A medida que os serviços sociais e de saúde se tornam mais digitalmente conectados, os idosos beneficiarão de muitas maneiras de um melhor acesso, conhecimento e comportamento. De acordo com os autores, o primeiro passo para ajudar os idosos a beneficiar desta tendência de digitalização nos cuidados de saúde é medir o seu nível de letramento digital. No artigo, apresentam os detalhes de uma

revisão sistemática que realizaram que teve como objetivos (1) identificar e avaliar criticamente estudos que envolvam a avaliação do letramento digital entre adultos mais velhos e (2) avaliar como os instrumentos de letramento digital utilizados nos estudos existentes abordam os elementos de letramento digital adequados à idade, utilizando a Comissão Europeia para a Competência Digital (DigComp). Isto é, aderem à ideia de que o letramento digital é composto por cinco áreas: (1) letramento em informações e dados, (2) comunicação e colaboração, (3) criação de conteúdo digital, (4) segurança e (5) solução de problemas (Ferrari; Punie; Brecko, 2013). Os autores são movidos pelo fato que segundo eles, até o tempo que pesquisaram, poucas revisões sistemáticas avaliaram instrumentos de letramento digital direcionados aos adultos mais velhos em geral. Ficou evidente que, embora os autores mencionem no Resumo do seu artigo a questão de segurança e privacidade, a revisão em si não aborda essa dimensão do letramento digital dos idosos em detalhe. O foco do artigo é mapear estudos realizados com idosos para avaliar seu letramento digital, e sendo assim, discutir os vários instrumentos empregados para tais avaliações. Isto é o grande valor deste artigo de revisão, pois traz à luz, de forma sistematizada, esses instrumentos, e os pontos fortes e fracos de cada. Por exemplo, o instrumento eHEALS (*eHealth Literacy Scale*) é de longe o mais utilizado (em 59% dos estudos que revisaram), porém, os autores observam que esse instrumento tem recebido críticas por ser muito simples e superficial (contém apenas 8 questões), mas a predominância de seu uso nesses estudos com idosos aponta para a facilidade da sua aplicação com esse tipo de participante. Interessante observar no contexto da presente pesquisa que o instrumento de avaliação do letramento digital de idosos mais bem avaliado pelos autores do artigo aqui sob análise é o *Mobile Device Proficiency Questionnaire* (MDPQ) – usado apenas em 1 estudo da revisão sistemática – porque mede os cinco componentes de letramento digital do DigComp, “incluindo a criação de conteúdo e segurança digital” (Oh et al, 2021, p.9). Para o DigComp, a capacidade dos adultos mais velhos para criar conteúdos digitais (desenvolvimento, integração e reelaboração de conteúdos digitais; direitos de autor; licenças; programação) pode apontar para informações importantes sobre a capacidade de uma pessoa para contribuir com valor para os novos meios de comunicação e para a auto-expressão e a criação de conhecimento. Os autores lembram que o MDPQ

[...] contém numerosos itens relacionados com a proteção e a privacidade dos dados e à privacidade, tais como “podem ser criadas senhas para bloquear/desbloquear um dispositivo móvel” ou “o histórico de pesquisa e os arquivos temporários podem ser eliminados”, apesar de a segurança ser o

elemento menos medido do DigComp Framework entre os instrumentos do nosso estudo. Apenas o CAS (*Computer Attitude Scale*), o eHEALS, e o MDPQ fornecem itens relacionados com a proteção de dados e a privacidade, o que é preocupante, dado que os adultos mais velhos constituem uma proporção significativa da população-alvo de *scams* na Internet ou ataques por correio eletrônico. (Oh et al., 2021, p.10)

Cabe mencionar uma ressalva que os autores mencionam, que diz respeito à perspectiva cultural da visão dos idosos e sua capacidade no uso das TDIC. Citam os Países Baixos onde a idade é um indicador menos importante para o letramento digital do que as fases da vida e a socialização. Também mencionam um estudo alemão em que foi concluído que, em vez da idade, os principais determinantes da competência digital eram os sentimentos de ameaça provocados pela digitalização e tecnologização: Tal como os jovens com percepções de ameaça mais elevadas podem não ser digitalmente competentes, os adultos mais velhos com percepções de ameaça mais baixas podem ser proficientes em tecnologia digital.

O contexto do artigo de **Ayse Aslan, Freda Mold, Harm Van Marwijk e Jo Armes (2024)**, é a mudança de serviços de saúde para os meios digitais, a partir da pandemia de COVID-19, fenômeno que agravou, então, as desigualdades de acesso digital, ao mesmo tempo em que houve uma rápida aumento de serviços de saúde eletrônica em muitos países. Foi realizada uma meta-etnografia (que é amplamente usada na pesquisa em saúde ao sintetizar estudos qualitativos) para sintetizar qualitativamente a literatura sobre as experiências de adultos mais velhos no uso de serviços de saúde digitais comunicativos (*communicative e-health services*). Definem serviços de saúde digital comunicativos como qualquer serviço de saúde online que um paciente recebe ou procura, que implica a sua interação ativa com um profissional de saúde. Os autores foram movidos pelo fato que não encontraram qualquer revisão da literatura qualitativa que traga as experiências e percepções dos idosos e suas percepções dos serviços de saúde online, e mais especificamente, o aspeto da comunicação dos serviços de saúde online. Assim, eles extraíram as experiências, percepções e opiniões dos idosos dos estudos qualitativos que selecionaram, além das barreiras e facilitadores que impedem ou facilitam a adoção de tais serviços por idosos. Após realizarem uma seleção sistemática da literatura, restaram 10 artigos relevantes para o estudo, aos quais os autores aplicaram as 6 etapas de um estudo meta-etnográfico seguindo as diretrizes eMERGe.

Os autores derivaram dez conceitos cernes dos resultados dos 10 estudos qualitativos analisados, a saber: 1) barreiras de saúde; 2) redes de apoio; 3) interface/design do aplicativo; 4) letramento digital; 5) falta de sensibilização (*awareness*); 6) segurança online; 7) acesso a dispositivos digitais e à Internet; 8) relação com o(s) profissionais de saúde; 9) preferência por atendimento presencial e 10) conveniência. Todos esses conceitos se interagem recursivamente, nenhum deles sendo hierarquicamente mais relevante que os outros. É relevante aqui chamar a atenção para a separação conceitual entre segurança online e letramento digital, mas tal separação fica relativizada pela interação recursiva entre essas facetas. No que diz respeito ao letramento digital, os idosos dos estudos analisados autodeclararam que os seus níveis de letramento digital eram baixos, o que prejudicou a sua capacidade de utilizar serviços de saúde digitais. Os autores distinguem entre “1) a aptidão (*ability*) dos idosos para utilizar serviços de saúde digitais online; 2) a sua capacidade (*capacity*) de compreender como utilizar os serviços comunicativos de saúde online” (Aslan et al., 2024, p.11). Sobre sua aptidão, os idosos reportam que sabem como usar um telefone, inclusive celular, ou certos aplicativos de mensagens mais “simples” como WhatsApp, para contatar médicos. Vários idosos expressaram um desejo de melhorar suas habilidades com as TDIC, entendendo que ficam em desvantagem pela lacuna de conhecimento. No que diz respeito à sua capacidade de compreensão do uso das TDIC, vários idosos manifestaram “medo” em fazer algo errado com a chamada, envio de imagens etc. Além disso (entre outros fatores), sua capacidade no uso das TDIC fica comprometida por questões de saúde física (visão, mãos trêmulas etc.). Relativo à segurança online, os autores observam que os reduzidos níveis de letramento digital impactam a percepção de segurança online expressa pelos idosos, por exemplo, sentindo que o notebook ou PC é mais seguro que o celular, ou temendo infrações e vazamentos dos seus dados pessoais durante consultas online com profissionais da saúde. Por outro lado, idosos dos estudos que já tinha usados esses serviços de saúde online reconheceram a grande conveniência de poder ter acesso aos profissionais de saúde online, com mais agilidade e prontidão. Estes idosos, a nosso ver, fazem um *trade-off* entre conveniência e preocupações com a segurança desses serviços. A partir das percepções e opiniões coletadas dos estudos revisados, exclusivamente dos trechos das falas diretamente dos idosos eles mesmos, os autores desta revisão qualitativa concluem que de modo geral, a maioria das pessoas idosas parece ter experiências e opiniões desfavoráveis sobre os serviços de saúde online e preferiu consultar os médicos e profissionais de saúde

pessoalmente. Antes de consentirem em consultar seus profissionais de saúde virtualmente, online, sentiram que tinham de ter uma relação pessoal sólida com eles.

### 5.1.5 Cidadãos e competência digital para a segurança online

A premissa do artigo de **Musaddag Elrayah e Saima Jamil (2023)** é que o letramento digital e as preocupações com a privacidade impactam diretamente nos comportamentos dos indivíduos no ambiente digital. E afirmam, na parte da revisão da literatura do seu artigo, que pesquisas anteriores têm ignorado predominantemente a potencial influência moderadora da sensibilização para a cibersegurança. Em vez disso, a tônica tem sido colocada na investigação das correlações existentes entre vários aspectos do comportamento em matéria de cibersegurança e o letramento digital. O problema é que estas relações não são suficientemente examinadas em termos da forma como a consciência as influencia ou controla. Além disso, pouco se estudou sobre os elementos ambientais que podem afetar a forma como o comportamento em matéria de cibersegurança e letramento digital interagem. Estas variáveis incluem componentes organizacionais, culturais e educativas que poderiam atenuar as correlações observadas. Desse modo, o estudo de Elrayah e Jamil (2023) objetivou examinar o impacto de várias dimensões do letramento digital, incluindo o conhecimento dos direitos de autor, a curadoria da cidadania, a conectividade e as preocupações com a privacidade online, no comportamento dos indivíduos em matéria de cibersegurança. Também visaram examinar o efeito moderador da sensibilização para a cibersegurança. Com base em sucintas recortes e revisões da literatura, os autores constroem as hipóteses da sua pesquisa, que serão descritas abaixo em conjunto com os resultados da pesquisa. No que diz respeito ao método empregado, a pesquisa é de natureza quantitativa, com análise estatística dos dados coletados a partir de um questionário tipo survey – que é somente mencionado no resumo (abstract) do artigo – que foi aplicado a uma amostra de 235 indivíduos residentes em diferentes cidades da Arábia Saudita. A primeira hipótese “H1 Os direitos de autor (copyright) influenciam positivamente o comportamento em matéria de cibersegurança” - foi a única não comprovada pela pesquisa. Com base numa sucinta revisão da literatura sobre este tema, os autores observam que o conhecimento da legislação sobre direitos de autor faz parte integrante do letramento digital e reforça o uso responsável da Internet. Porém, os resultados da pesquisa exibiram uma associação negativa significativa, indicando que o conhecimento das leis de direitos de autor está ligado a uma

*diminuição* dos comportamentos proativos em matéria de cibersegurança. A segunda hipótese - H2: A cidadania digital influencia positivamente o comportamento em matéria de cibersegurança – foi comprovada pela pesquisa. Os praticantes de uma boa cidadania digital compreendem que todos têm uma responsabilidade partilhada pela cibersegurança e trabalham para melhorar a segurança online, incentivando os utilizadores a adoptarem práticas seguras. Participar ativamente em fóruns online e transmitir conhecimentos aos outros são componentes essenciais para ser um cidadão digital responsável. É fundamental ter cuidado ao divulgar informações pessoais em linha e encorajar outras pessoas com quem se liga online a seguir o mesmo caminho. A terceira hipótese era “H3: A curadoria influencia positivamente o comportamento de segurança cibernética” e os resultados do estudo comprovaram esta hipótese. A cultura digital promove participação ativa e curadoria de conteúdo, avaliação do conteúdo encontrado. Isso implica a implementação de medidas de segurança proativas para proteger a presença online, fazer escolhas bem informadas com relação às informações digitais com as quais se envolve e gerenciar adequadamente os dados pessoais. Esta postura está diametralmente em oposição ao consumo passivo das informações e conteúdo encontrados na Internet. Também foi comprovada a quarta hipótese - “H4: A conectividade influencia positivamente o comportamento de segurança cibernética”. Esta hipótese, em nossa opinião, está relacionada àquela da cidadania digital, pois postula que o ato de networking aprimoram o comportamento de segurança cibernética ao destacar as dimensões sociais da conduta online. Explicam os autores:

As redes aprimoram o comportamento de segurança cibernética por meio da influência do impacto social e do estabelecimento de normas compartilhadas nas comunidades online. Os indivíduos que experimentam um senso de conexão em ambientes on-line têm maior probabilidade de adotar as práticas recomendadas de segurança cibernética devido à influência dos colegas, ao compartilhamento de informações e à adesão às normas sociais. (Elayah; Jamil,2023, p.171)

A quinta hipótese - H5: As preocupações com a privacidade online influenciam positivamente o comportamento de cibersegurança – também foi comprovada pelos resultados da pesquisa. A relação entre as preocupações com a privacidade online de um indivíduo e a sua propensão para implementar medidas de cibersegurança ilustra a relação entre os pontos de vista individuais sobre a privacidade e as medidas proativas tomadas para contrariar os perigos cibernéticos. O comportamento e as atitudes online das pessoas são significativamente influenciados pelas preocupações com a privacidade, especialmente quando se trata de cibersegurança.

Os dois principais pontos fracos do texto de Elrayah e Jamil (2023) é que não descreve com suficiente detalhe o método seguido, parecendo confundir a apresentação dos resultados e sua análise com o método. O outro ponto é que não conceitualiza explicitamente o termo cibersegurança e comportamento de cibersegurança. Como pode ser visto da seguinte citação do texto, o termo quase se confunde, recursivamente, com o letramento digital:

Uma maior conscientização sobre a cibersegurança promove o desenvolvimento de habilidades de letramento digital, incluindo a compreensão das leis de direitos autorais, a prática de uma boa cidadania digital, a participação na curadoria de conteúdo, a promoção da conectividade e a abordagem de questões de privacidade online. O desenvolvimento de um forte senso de conscientização é essencial para traduzir efetivamente as habilidades digitais em práticas online seguras (Elrayah; Jamil,2023, p.181)

O texto de **Matthew Johnson e Meggie Lasher** (2021), bibliotecários da University of North Carolina, (UNC), relata a experiência da realização de oficinas na comunidade oferecendo aulas de “letramento digital e tecnologia de informática” para membros da comunidade em bibliotecas públicas locais. Eram estudantes de pós-graduação em LIS (Library and Information Science) que ministraram as aulas, e também assumiram papéis de liderança e gestão nos cursos. Nesse sentido, envolvimento nas oficinas proveram oportunidades para os estudantes de aprofundar suas experiências de “aprender em serviço” (*service learning*), que faz parte de um ciclo de aprendizagem experiencial, que é um processo cíclico por meio de uma experiência concreta, seguido por reflexão sobre as observações dessa experiência, formação de conceitualizações abstratas e, em seguida, iniciação do ciclo novamente, tudo enquanto os estudantes provêm um serviço à comunidade. O importante é os estudantes participarem em atividades que atendem necessidades humanas e comunitárias, e nesse sentido, a atividade é recíproca. Sinteticamente, os autores descrevem a atividade que descrevem assim: “ O *Community Workshop Series* (CWS) é um programa multifacetado com um impacto direto no letramento digital servindo também como local de aprendizagem para estudantes licenciados interessados no ensino, desenvolvimento comunitário, biblioteconomia pública e extensão” (Johnson; Lasher, 2021, p.747). Os bibliotecários universitários da UNC atuaram como coordenadores gerais do programa. Porém, quando os recursos financeiros para o programa foram cortados pela UNC, os bibliotecários (os dois autores) descobriram, dos seus parceiros (bibliotecas públicas) que o programa era a única fonte de educação em letramento digital

para as bibliotecas envolvidas. Terminar o CWS seria equivalente a “fechar uma ponte para a inclusão digital e oportunidades de ensino significativas para os alunos do MLIS” (mestrado em biblioteconomia e ciência da informação). Os autores relatam que a extinção do programa significou que teriam que se dedicar voluntariamente, mas uma biblioteca pública reuniu com eles e foi criado um cargo de assistente de investigação para pós-graduandos na School of Information and Lib Science SILS da UNC, que ajudou a financiar o programa. Isto permitiu um maior enfoque no desenvolvimento do programa, oferecendo uma bolsa, remissão de pagamentos taxas universitárias e seguro de saúde para estudantes envolvidos. Uma remuneração suficiente garantiu que o programa recebesse o tempo e a atenção necessários. São introduzidos novos cursos conforme necessário ou desejado, e as ofertas de cursos são continuamente avaliadas para atualizar o currículo de acordo com as necessidades da comunidade. Por exemplo, há um curso de informação sobre saúde comunitária realizada na Biblioteca Pública de Chapel Hill. Consistia em duas partes: uma análise da avaliação da informação online sobre saúde e um debate sobre fontes de informação online confiáveis em saúde. Estes cursos foram ministrados em colaboração com a Biblioteca de Ciências da Saúde da UNC. Um módulo sobre notícias e mídia e um outro sobre segurança e privacidade online foram adicionados em resposta ao crescente discurso em torno das “notícias falsas”. Porém, este artigo não forneceu maiores informações sobre esses cursos. Essa última inclusão aponta para sua visão, de modo geral, do letramento digital sendo algo que extrapola o ensino de habilidades técnicas, para incorporar análises críticas dos usos das TDIC.

O estudo relatado no texto de **Heidi Julien, David Gerstle, Brian Detlor, Tara La Rose e Alexander Serenko** (2021) foi movido pela seguinte questão de pesquisa: “Como é que as bibliotecas públicas e outras organizações comunitárias podem avaliar as iniciativas de letramento digital que oferecem às comunidades que servem?”(p.440) sendo que para efeitos da pesquisa, as organizações comunitárias são instituições sem fins lucrativos com bases locais que têm por objetivo melhorar o bem-estar das suas comunidades. Também fizeram a questão “Quais fatores organizacionais (por exemplo, fatores administrativos) promovem ou desafiam as iniciativas de formação em letramento digital oferecidas às comunidades locais?” A pesquisa foi realizada com base em entrevistas com administradores de bibliotecas públicas e organizações comunitárias que oferecem iniciativas em letramento digital e com os treinadores e clientes dessas ações de formação. Como resultados, apresentam seções que abordam o tipo de treinamento oferecido nos programas, desenho

dos programas, os públicos pretendidos para os programas, as motivações das organizações para ofertar os programas, os desafios na oferta.

Em termos do tipo de treinamento (termo usado pelos autores) em letramento digital oferecido, as competências digitais mais comuns ensinadas incluíram codificação, segurança informática, IA e robótica, gravação de áudio e vídeo, e competências informáticas básicas (digitação, utilização do *mouse*). Em todas as instituições (bibliotecas públicas e centros comunitários), os organizadores procuram ofertar para programas a vários níveis de competência, incluindo formação avançada (por exemplo, IA, realidade virtual, impressão 3D) e programas “intermédios” e básicos (por exemplo, Microsoft Suite, Adobe, correio eletrónico e redes sociais). As bibliotecas públicas focam principalmente no treinamento em habilidades básicas: compreensão e uso de hardware de computador (por exemplo, mouse e teclado), mídias sociais, e-mail, mecanismos de busca, software dos Microsoft Office, e iPads e tablets, se bem que existem também oportunidades de treinamento mais avançadas, como a criação de videogames e a digitalização de memórias. Uma das bibliotecas de médio porte também oferece um programa de letramento digital que instrui os usuários sobre codificação HTML/XML e design de websites. Os autores concluem que a forma com que os administradores concebem o letramento digital é restrita à formação no uso das TIC centrada especialmente no hardware e no software como foco nas competências desse uso. O uso ético da informação, as atitudes o *mindsets* em relação à cultura digital, foram assuntos muito pouco abordados. Tampouco há menção explícita nesse artigo sobre o tema de segurança online e privacidade. Indubitavelmente, o propósito desses programas promovidos pelo Canadá é extremamente louvável, sendo que todas as organizações estudadas manifestaram que a missão primordial com esses treinamentos é a inclusão na sociedade da informação e cultura digital dos grupos marginalizados como pessoas indígenas, mulheres, idosos e estudantes e alunos de grupos minoritários que sofrem com a exclusão social. Mas é também relevante notar que os entrevistados também mencionaram que são justamente esses grupos que tendem a ser os mais afetados pelos extremos climáticos daquele país, dependendo de transporte coletivo etc., o que compromete, muitas vezes, a sua possibilidade de frequentar os treinamentos com consistência contínua.

## 6. Considerações finais

A competência digital é essencial para navegar no mundo digital atual e requer estratégias educacionais dedicadas para garantir que as pessoas estejam equipadas com os conhecimentos, habilidades e atitudes necessários para maximizar seus benefícios e, ao mesmo tempo, mitigar os possíveis riscos de perda de privacidade e segurança inerentes à vida online – a *onlife* como referido pelo Floridi. Parte íntegra às iniciativas em prol da competência digital deveria ser sensibilização e conhecimentos quanto à necessidade de avaliação da informação – o reconhecimento do conteúdo como potencial risco à segurança e privacidade online.

Ao abordar a questão de privacidade e segurança online, a tendência é de assumir que os efeitos danosos resultando do enfraquecimento ou perda da privacidade e segurança afetam principalmente grupos vulneráveis como crianças e idosos. Porém, o fenômeno também observado pelo Floridi e discutido acima, de que hoje no mundo digitalizados, nos somos o equivalente a nossa informação e a nossos dados, implica todos nós corremos o risco de ter nossas identidades roubadas. O fato preocupante é que na “infoesfera” (termo também cunhado pelo Floridi), somente podemos falar em “minha informação” e “meus dados” no sentido que, nesse novo espaço ontológico, somos *constituídos* por esses dados e informações. Porém, como já mencionado neste texto, muitos de nossos dados e nossas informações – no sentido de dados e informações sobre nós – são pertencentes às grandes empresas *Big Tech* para as quais nós os cedemos ao se inscrever nos serviços “*onlife*” ofertados. É um pacto em que a maioria das pessoas entram para poder compartilhar livre e gratuitamente (e frequentemente, de forma intensiva) para receber em retorno, o sentimento de comunidade, família e conexão que a afiliação e participação nas redes sociais pode proporcionar. E para os *influencers*, uma renda financeira.

Esse *modus operandi* dos sites das redes sociais, pelo qual a participação dos seus usuários somente acontece por meio da compartilha dos seus dados pessoais suscita o que é conhecido na literatura como o “paradoxo de privacidade” (outro assunto abordado acima). Nisso, os usuários das redes e outras plataformas manifestam (em pesquisas de opinião e *surveys*) uma preocupação genuína com sua privacidade e segurança online, mas ao mesmo tempo, cedem livremente seus dados pessoais às empresas. Evidentemente, como no consumo online de bens e produtos, a conveniência e os percebidos ganhos superam os possíveis riscos. É notável que os usuários das redes sociais são eles mesmos responsáveis

para proteger seus dados e informações pessoais da coleta de dados por terceiros, opções essas passadas para os usuários por meio da prática desajeitada (por ser ou muito detalhada ou não detalhada o suficiente) de “aviso e escolha” – hoje usualmente contida na apresentação de *cookies* aos usuários para que selecionem os mais apropriados. A análise do fenômeno do paradoxo de privacidade é pertinente para que em futuras pesquisas de natureza possivelmente mais empírica, a pesquisadora pode estar atenta a como as pessoas expressam preocupações com a sua privacidade, e, inclusive, expressar isto com uma autoavaliação da sua competência digital nessa esfera, mas não adotam comportamentos coerentes com essas preocupações. Como Nissenbaum, pesquisadora citada neste relatório, nos lembra: a privacidade é contextual.

No que diz respeito ao alcance dos objetivos propostos no início desta pesquisa – englobados pelo objetivo geral de “realizar uma revisão da literatura científica e cinzenta acerca dos temas que se interseccionam: competência digital e segurança e privacidade online”, acreditamos que este foi atendido na revisão agregada numa síntese qualitativa da literatura estudada. Porém, os objetivos foram alcançados, mas não sem limitações perceptíveis.

Por exemplo, o uso da base de dados Dimensions levou à recuperação de artigos em outras línguas, apesar de ter empregado um filtro de idioma em todas as pesquisas nas bases. Foram recuperados e contemplados em fases iniciais das pesquisas nas bases porque os resumos (*abstracts*), títulos, palavras-chaves estiveram em inglês, o que é esperado. Por causa da inteligibilidade desses metadados, dois desses artigos em línguas estrangeiras continuaram a ser contemplados como parte do *corpus* potencial a ser analisado, até que o arquivo dos respectivos artigos foram abertos e o idioma deles foi constatado. O filtro de idioma para o texto completo não parece ter funcionado adequadamente nesta base de dados.

Outro artigo recuperado que não parece ter atendido à conjugação (com o operador booleano AND) dos termos da expressão de busca, foi o de Konstantina Martzoukou (2021), recuperado pela base de dados LISA. Pois embora esse artigo tenha abordado o tema de competência digital de crianças em idade escolar, ele não menciona a privacidade e segurança em relação à competência digital. De fato, sabemos que essa autora já

desenvolveu pesquisas sobre o tema de privacidade digital para crianças<sup>10</sup>, fato que levou à leitura cuidadosa do artigo, na esperança de encontrar essa temática abordada nele. De modo semelhante, o artigo por Igbo (2020), também recuperado pela base de dados LISA, embora muito interessante e relevante por tratar da competência digital de universitários nigerianos, tampouco mencionou a temática de privacidade e segurança digitais.

A experiência no uso do software Iramuteq não foi muito satisfatória. Este foi o primeiro contato com o software, e a intenção tinha sido usá-lo para auxiliar na filtragem da quantidade grande (106) de artigos recuperados inicialmente – filtragem por meio dos descritores (palavras-chave) dos artigos – para reduzir este corpus a um tamanho factível para uma única pesquisadora revisar. O software não é muito intuitivo manusear, sendo necessário esta pesquisadora acompanhar uma oficina online para realizar ações básicas com o software. A interpretação dos dados usando o Iramuteq necessita muito mais experiência e ensinamento com o software. Como trabalha com dados quantitativos, contagem de descritores, foram incluídos nos resultados finais, artigos de qualidade questionável. Cabe mencionar aqui que, nos estudos de revisões sistemáticas, com equipes de pesquisadores, utiliza-se ferramentas de avaliação da qualidade dos artigos recuperados, tal como a *Crowe Critical Appraisal Tool (CCAT)*<sup>11</sup> e a *Joanna Briggs Institute (JBI) critical appraisal tools for qualitative research*<sup>12</sup>.

A ausência de artigos recuperados na língua portuguesa e do Brasil aponta que há muito mais a ser pesquisado, inclusive com estudos empíricos, neste tema que conjuga competência digital com privacidade e segurança online. Esta pesquisa mostrou a relevância da temática. Esses esforços em estudos e pesquisas futuros – esforços teóricos e aplicados – trarão contribuições valiosas para o âmbito da Ciência da Informação, não apenas por trazer reflexões sobre aspectos fundamentais da área e seu *locus* tão central na infoesfera, mas também sobre as atribuições dos profissionais (bibliotecários, docentes, professores) necessários para futuros iniciativas, programas, políticas e pesquisas sobre esta temática nesses âmbitos profissionais. Por fim, será importante reconhecermos que, em nível mais básico, o que une os entendimentos e conceitualizações diversos da competência digital é o pressuposto de que certos entendimentos, competências e recursos permitem às pessoas

---

<sup>10</sup> Por exemplo: Martzoukou, K. Maddie is online: co-creating with young people for safer and resilient online connectivity. Projeto desenvolvido por essa pesquisadora desde 2022.

<sup>11</sup> Disponível em: <https://conchra.com.au/wp-content/uploads/2015/12/CCAT-user-guide-v1.4.pdf>

<sup>12</sup> Disponível em: <https://jbi.global/critical-appraisal-tools>

envolverem-se proficiente e criticamente com dados, informação, plataformas e as mídias digitais, e que hoje, todas estas configurações digitais estão envolvidas na organização da relação de um indivíduo com a sociedade, relação esta permeada por entendimentos da privacidade que terão que ser continuamente reavaliados por cidadãos ativos e engajados.

## 7. Referências

BARAD, K. Posthumanist performativity: Toward an understanding of how matter comes to matter. **Signs: Journal of women in culture and society**, v. 28, n. 3, p. 801-831, 2003.

BARRETT-MAITLAND, N; LYNCH, J. Social media, ethics and the privacy paradox. In: KALLONIATIS, C.; TRAVIESO-GONZALEZ, C.M. (Eds.) **Security and privacy from a legal, ethical, and technical perspective**. Doi 10.5772/intechopen.78747: IntechOpen, 2020. p. 1-15.

BAWDEN, D. (2008) Origins and Concepts of Digital Literacy. In: LANKSHEAR, C.; KNOBEL, M. (Eds.) **Digital Literacies: concepts, policies, and practices**. Lausanne: Peter Lang, 2008. p. 17-32.

BUCKINGHAM, D. Defining digital literacy-What do young people need to know about digital media? **Nordic journal of digital literacy**, v. 10, n. Jubileumsnummer, p. 21-35, 2015.

CARRETERO, S.; VUORIKARI, R.; PUNIE, Y. **DigComp 2.1: The digital competence framework for citizens with eight proficiency levels and examples of use**. Luxembourg: Publications Office of the European Union, 2017.

CILIP. CILIP Definition of Information Literacy 2018. Disponível em: <https://infolit.org.uk/ILdefinitionCILIP2018.pdf>. Acesso em: 05 ago. 2024

CODINA, L. Revisões sistematizadas em Ciências Humanas y Sociales. 2: Búsqueda y evaluación. In: LOPEZOSA C.; DÍAZ-NOCI, J.; CODINA, L. (Eds.). **Metodos Anuario de Métodos de Investigación en Comunicación Social, 1**. Barcelona: Universitat Pompeu Fabra, 2020. p. 61-72.

CRESWELL, J.W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 2.ed. Porto Alegre: Artemed, 2007.

CRONIN, M. A.; GEORGE, E. The why and how of the integrative review. **Organizational Research Methods**, v. 26, n. 1, p. 168-192, 2023.

DEMO, Pedro. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2000.

DUFVA, M. **MEGATREND 4: Technology is becoming embedded in everything**, SITRA, 2020. Disponível em: [https://www.sitra.fi/en/archive/?search\\_term=Technology%20is%20becoming%20embedde d%20in%20everything](https://www.sitra.fi/en/archive/?search_term=Technology%20is%20becoming%20embedde d%20in%20everything). Acesso em: 09 jul. 2024.

FAZIL, A.W; HAKIMI, M.; SAJID, S.; QUCHI, M.M.; KHALIQYAR, K.Q. Enhancing internet safety and cybersecurity awareness among secondary and high school students in Afghanistan: a case study of Badakhshan Province. **American Journal of Education and Technology**, v. 2, n. 4, p. 50-61, 2023.

FEENBERG, A. A Critical Theory of Technology. In: FELT, U.; FOUCHÉ, R.; MILLER, C. A.; SMITH-DOERR, L. (Eds.). **The Handbook of Science and Technology Studies**. 4 ed. Cambridge: MIT Press, 2017, p. 635-663.

FERRARI, A., PUNIE, Y., Y BRECKO, B. **DIGCOMP**: A Framework for Developing and Understanding Digital Competence in Europe. Luxembourg: Publications Office of the European Union. 2013. Disponível em: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-framework-developing-and-understanding-digital-competence-europe>

FINK, A. **Conducting research literature reviews**: from the internet to paper. 4th edition, Delhi; London: Sage Publications, 2014.

FLORIDI, L. The ontological interpretation of informational privacy. **Ethics and information technology**, v. 7, p. 185-200, 2005.

FLORIDI, L. The Information Society and its Philosophy: Introduction to the Special Issue on 'the Philosophy of Information, its Nature, and Future Developments'. **The Information Society**, v.25, n.3, p.153-8, 2009.

FLORIDI, L. **The fourth revolution**: how the infosphere is reshaping human reality. Oxford: OUP, 2014.

FU, J. Complexity of ICT in education: a critical literature review and its implications. **International Journal of education and Development using ICT**. v.9, n.1, 2013, p. 112-125.

GASQUE, K. C. G. D. Competência em Informação: conceitos, características e desafios. **AtoZ: novas práticas em informação e conhecimento**, v. 2, n. 1, p. 5-9, 2013.

GILSTER, P. **Digital Literacy**. New York: Wiley, 1997.

GONZÁLEZ-IBÁÑEZ, R.; SHAH, C. Investigating positive and negative affects in collaborative information seeking: A pilot study report. **Proceedings of the American Society for Information Science and Technology**, v. 49, n. 1, p. 1-4, 2012.

GONZALEZ GOMEZ, N. A ética da informação de Luciano Floridi: nas Trilhas da Filosofia [preprint, c.2020]. Disponível em: <http://eprints.rclis.org/42284/1/A%20%C3%89tica%20da%20Informa%C3%A7%C3%A3o%20de%20Luciano%20Floridi%20nas%20Trilhas%20da%20Filosofia.pdf>. Acesso em: 14 set. 2024.

GRANT, M.J.; BOOTH, A. A typology of reviews: an analysis of 14 review types and associated methodologies. **Health information & libraries journal**, v. 26, n. 2, p. 91-108, 2009.

- HAIDER, J; SUNDIN, O. **Paradoxes of media and information literacy: The Crisis of information.** London/New York: Routledge/Taylor & Francis, 2022.
- HICKS, A. Moving Beyond the Descriptive: The Grounded Theory of Mitigating Risk and the Theorisation of Information Literacy. **Journal of Documentation**, v.76, n.1, p.126–44, 2019.
- HILBERT, M. Digital technology and social change: the digital transformation of society from a historical perspective. **Dialogues in Clinical Neuroscience**, v.22, n.2, p.189–94, 2022.
- HOLMSTRÖM OLSSON, H.; BOSCH, J. Going Digital: Disruption and Transformation in Software-intensive Embedded Systems Ecosystems. **Journal of Software, Evolution and Process**, v.32, n.6, e2249, 2020.
- ILOMÄKI, L.; PAAVOLA, S.; LAKKALA, M.; KANTOSALO, A. Digital competence—an emergent boundary concept for policy and educational research. **Education and information technologies**, v. 21, p. 655-679, 2016.
- JOHNSON, M.W.; LASHER, M. The community workshop series: A case study for community-engaged learning in LIS. **Library Trends**, v. 69, n. 4, p. 752-767, 2021.
- KALLINIKOS, J., AALTONEN, A.; MARTON, A. The ambivalent ontology of digital artifacts. **MIS Quarterly**, v.37, n.2, p.357–70, 2013.
- KNOFF, J.W. Doing a literature review. **PS: Political Science & Politics**, v. 39, n. 1, p. 127-132, 2006.
- LAURILLARD, D.; DERRICK, J.; DOEL, M. **Building Digital Skills in the FE Sector: future of skills and lifelong learning.** London: Government Office for Science, 2016.
- LEMOS, R. Carregando...a cultura digital entre as fronteiras da civilização. Rio de Janeiro: ITS-Rio. Agosto, 2024. Disponível em: <https://itsrio.org/pt/publicacoes/carregando-a-cultura-digital-entre-as-fronteiras-da-civilizacao>. Acesso em: 13 set. 2024.
- LLOYD, A. Framing information literacy as information practice: site ontology and practice theory. **Journal of Documentation**, v. 66, n.2 p. 245 – 258, 2010.
- LLOYD, A. Information literacy and literacies of information: a mid-range theory and model. **Journal of Information Literacy**, v. 11, n. 1, p. 91-105, 2017.
- MARTIN, A. (2006). Literacies for the digital age. In: MARTIN, A.; MADIGAN, D. (Eds.). **Digital literacies for learning**, London: Facet, 2006. p. 3–25.
- MARTIN, A; GRUDZIECKI, J. DigEuLit: Concepts and tools for digital literacy development. **Innovation in Teaching and Learning in Information and Computer Sciences**, v.5, n.4, p.249–267, 2006.
- MÅRD, M.; HALLIN, A. Digital Literacy in a Post-Digital Era: Rethinking ‘Literacy’ as Sociomaterial Practice. In: WIDEN, G.; TEIXEIRA, J. **Information Literacy and the Digitalisation of the Workplace.** London: Facet, 2024. p.15-28.

- MBANDJE, D. C.; LOUREIRO, M.J.; LUCAS, M. Digital competence and information literacy: clarifying concepts based on a literature review. **Educational Media International**, v. 60, n. 3-4, p. 306-316, 2023.
- NABHAN, S. Pre-service teachers' conceptions and competences on digital literacy in an EFL academic writing setting. **Indonesian Journal of Applied Linguistics**, v.11, n.1, 187-199, 2021.
- NISSENBAUM, H. A contextual approach to privacy online. **Dædalus, the Journal of the American Academy of Arts & Sciences**, v.140, n.4, Fall, p.32-48, 2011.
- NISSENBAUM, H. Respecting context to protect privacy: Why meaning matters. **Science and engineering ethics**, v. 24, n. 3, p. 831-852, 2015.
- NORBERG, P. A.; HORNE, D. R.; HORNE, D. A. The privacy paradox: personal information disclosure intentions versus behaviors. **Journal of Consumer Affairs**, v.41, n.1, p.100-126, 2007.
- OH, S. S.; KIM, K.-A; KIM, M.; OH, J.; CHU, S.H.; CHOI, J. Measurement of Digital Literacy Among Older Adults: Systematic Review. **Journal of medical Internet research**, v. 23, n. 2, p. e26145, 2021.
- ORLIKOWSKI, W. J.; SCOTT, S.V. The algorithm and the crowd. **Mis Quarterly**, v. 39, n. 1, p. 201-216, 2015.
- ONU. Declaração Universal dos Direitos Humanos. Paris: Organização das Nações Unidas, 1948. Disponível em: <https://brasil.un.org/sites/default/files/2020-09/por.pdf>. Acesso em: 16 set. 2024.
- PETERS, M.D.J.; MARNIE, C.; TRICCO, A.; POLLOCK, D.; MUNN, Z.; ALEXANDER, L.; MCINERNEY, P.; GODFREY, C.; KHALIL, H. Updated methodological guidance for the conduct of scoping reviews. **JBI Evidence Synthesis** v.18, n.10, p 2119-2126, 2020.
- PIETERS, W. The (Social) Construction of Information Security. **The Information Society**, v.27, n.5, p.326-335, 2011.
- PIETERS, W. Beyond individual-centric privacy: Information technology in social systems. **The Information Society**, v. 33, n. 5, p. 271-281, 2017.
- RADER, H. B. Information Literacy 1973-2002: A Selected Literature Review. **Library Trends**, v. 51, n. 2, p. 242-259, Fall 2002.
- RAY, A. Digital literacy. In: KHOSROW-POUR, M. (Ed.). **Encyclopedia of information science and technology**. 4<sup>th</sup> ed. Hershey, PA: IGI Global, 2018. p.2225-2234.
- REDDY, P; SHARMA, B; CHAUDHARY, K. Digital Literacy: A Review of Literature. **International Journal of Technoethics**, v.11, n.2, p.65-94, July-December 2020.

SAVIRIMUTHU, J. Do algorithms dream of 'data' without bodies?. **International Review of Law, Computers & Technology**, v. 31, n. 2, p. 243-262, 2017.

SHARMA, R.S.; MALONE, L.G.; GUAN, C.; DATTAKUMAR, A. A Maturity Model for Digital Literacies and Sustainable Development. In: KHOSROW-POUR, M. (Ed.). **Encyclopedia of information science and technology**. 4<sup>th</sup> ed. Hershey, PA: IGI Global, 2018. p.2280-2291.

SLOAN, R.; WARNER, R. **Unauthorized access: The crisis in online privacy and security**. Boca Raton/London/New York: Taylor & Francis, 2017.

SNYDER, Hannah. Literature review as a research methodology: An overview and guidelines. **Journal of business research**, v. 104, p. 333-339, 2019.

SUNDIN, O.; FRANCKE, H. In search of credibility: pupils' information practices in learning environments. **Information Research – An international electronic journal**, v.14, n.4, paper 418, 2009.

SUNDIN, O.; HAIDER, J.; ANDERSSON, C.; CARLSSON, H.; KJELLBERG, S. The search-ification of everyday life and the mundane-ification of search. **Journal of Documentation**, v.73, n.2, p.224-243, 2017.

SURI, H. Essential Features of Methodologically Inclusive Research Syntheses. In: **Annual Meeting of the American Educational Research Association**, New Orleans, LA, April 2002. p.1-12, 2002. Disponível em: <https://files.eric.ed.gov/fulltext/ED464923.pdf>. Acesso em: 09 jul. 2024.

TINMAZ, H.; LEE, Y. T.; FANEA-IVANOVICI, M.; BABER, H. A systematic review on digital literacy. **Smart Learning Environments**, v. 9, n. 1, p. 21, 2022.

TORONTO, C.; REMINGTON, R. (Eds.). **A step-by-step guide to conducting an integrative review**. Switzerland: Springer Nature, 2020.

VUORIKARI, R.; PUNIE, Y.; GOMEZ, S. C.; VAN DEN BRANDE, G. **DigComp 2.0: The digital competence framework for citizens. Update phase 1: The conceptual reference model**. Brussels: Joint Research Centre, 2016.

WEINBERGER, M.; BOUHNIK, D. Identifying trends in information security and privacy concern research. **IFLA journal**, v. 49, n. 3, p. 527-540, 2023.

WIDEN, G.; AHMAD, F.; HUVILA, I. Connecting information literacy and social capital to better utilise knowledge resources in the workplace. **Journal of Information Science**, v. 49, n. 6, p. 1481-1492, 2023.

# APÊNDICE A

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
1	WoS	Elrayah, Musaddag; Jamil, Saima	Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness	2023	INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY	17	2	166-187	10.5281/zenodo.4766711
2	WoS	Corcoran, Erin; Clement, Alex; Gabrielli, Joy	A measurement model of online privacy cognitions in a sample of US adolescents	2024	BEHAVIOUR & INFORMATION TECHNOLOGY				10.1080/0144929X.2024.2305286
3	WoS	Heidi Julien, David Gers-tle, Brian Detlor, Tara La Rose, Alexander Serenko	Digital Literacy Training for Canadians, Part 1:“It’s... Just Core Public Works”	2021	The Library Quarterly	91	4	437-456	10.1086/715918
4	WoS	Jang, Yujin; Ko, Bomin	Online Safety for Children and Youth under the 4Cs Framework-A Focus on Digital Policies in Australia, Canada, and the UK	2023	CHILDREN-BASEL	10	8		10.3390/children10081415
5	WoS	Tomczyk, Lukasz; Potyra-la, Katarzyna	Parents' knowledge and skills about the risks of the digital world	2021	SOUTH AFRICAN JOURNAL OF EDUCATION	41	1		10.15700/saje.v41n1a1833
6	WoS	Portes, Audrey; N'Goala, Gilles; Cases, Anne-Sophie	Digital transparency: Dimensions, antecedents and consequences on the quality of customer relationships	2020	RECHERCHE ET APPLI-CATIONS EN MARKET-ING-ENGLISH EDITION	35	4	72-98	10.1177/2051570720973548
7	WoS	Pacheco, Edgar	Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors	2024	Arxiv				ar-Xiv:2403.09208
8	WoS	LEE,, Hee Jung	A Study on the Children's Online Personal Data Protection	2021	National Public law Review	17	2	157-190	10.46751/nplak.2021.17.2.157
9	WoS	Dennen, Vanessa P.; Choi, Hajeen; Word, Kari	Social media, teenagers, and the school context: a scoping review of research in education and related fields	2020	ETR&D-EDUCATIONAL TECHNOLOGY RE-SEARCH AND DEVEL-	68	4	1653-1658	10.1007/s11423-020-09796-z

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
					OPMENT				
10	WoS	Kang, Eun Jin; Kim, Amie; Lee, Jiun	International Comparative Study on Digital Media Literacy Elements in National Early Childhood Curricula in Finland, Canada, Australia, and South Korea	2022	Korean Journal of Child Studies	43	4	525-537	10.5723/kjcs.2022.43.4.525
11	WoS	Mayo, Amanda L.; Fung, Vera; Hitzig, Sander L.; Gould, Sarah; Posa, Stephanie; deLuca, Leslie Summers; Kayssi, Ahmed	Exploring the psychosocial needs of persons with lower extremity amputation and feasibility of internet cognitive behavioural therapy: a qualitative study	2023	DISABILITY AND REHABILITATION	45	24	4025-4034	10.1080/09638288.2022.2144492
12	WoS	Gonzalez-Villa, Angela; Gewerc, Adriana	A systematic review of the tensions between the public and private in adolescents' social networks: New education challenges	2024	E-LEARNING AND DIGITAL MEDIA	21	2	141-159	10.1177/20427530231156283
13	WoS	Aslan, Ayse; Mold, Freda; van Marwijk, Harm; Armes, Jo	What are the determinants of older people adopting communicative e-health services: a meta-ethnography	2024	BMC HEALTH SERVICES RESEARCH	24	1		10.1186/s12913-023-10372-3
14	WoS	Sinyayskaya, Yadviga E.	Online Social Media Communication: the Effect of Having Privacy Violation Experience on Online Behavior	2022	SOCIAL PSYCHOLOGY AND SOCIETY	13	1	33-50	10.17759/sps.2022130103
15	WoS	Kim,, Jae Sun	Administrative Law Response in Regulating Disinformation - Focus on the UK's Regulatory Discussion -	2020		24	3	223-248	10.32632/ELJ.2020.24.3.223
16	WoS	Sander, Ina	Critical big data literacy tools-Engaging citizens and promoting empowered internet usage	2020	DATA & POLICY	2			10.1017/dap.2020.5
17	WoS	Moor, Lily; Anderson, Joel R.; Power, Jennifer; James, Alexandra; Waling, Andrea; Shackleton, Nicole	The risks and benefits of technologised sexual practice scale: a quantitative measure of technology facilitated sex and intimacy	2024	SEXUAL HEALTH	21	1		10.1071/SH23034

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
18	WoS	Sharma, Varun; Ghosh, Shreya; Mahara, Priti	Exploring the determinants of internet addiction among Peri-urban adolescents (aged 13-18) in Delhi-NCR, India: an ordered logit model analysis.	2024	International journal of adolescent medicine and health				10.1515/ijamh-2023-0148
19	LISA	Archambault, Susan G	Expanding on the Frames: Making a Case for Algorithmic Literacy	2023	Communications in Information Literacy	17	2	530-553	
20	LISA	Pavey, Sarah, MSc FCLIP FRSA	Robot Wars – The Unleashing of Information Literacy	2023	The School Librarian	71	2	41609	
21	LISA	Al-Khatib, Tahani	Netiquette rules in online learning through the lens of digital citizenship scale in the post-corona era	2023	Journal of Information, Communication & Ethics in Society	21	2	181-201	10.1108/JICES-08-2021-0089
22	LISA	Bragazzi, Nicola Luigi;Crapanzano, Andrea;Converti, Manlio;Zerbetto, Riccardo;Khamisy-Farah, Rola	The Impact of Generative Conversational Artificial Intelligence on the Lesbian, Gay, Bisexual, Transgender, and Queer Community: Scoping Review	2023	Journal of Medical Internet Research	25	1	e52091	10.2196/52091
23	LISA	Busch-Casler, Julia;Radic, Marija	Trust and Health Information Exchanges: Qualitative Analysis of the Intent to Share Personal Health Information	2023	Journal of Medical Internet Research	25	1	e41635	10.2196/41635
24	LISA	Arakpogun, Emmanuel Ogiemwonyi;Whalley, Jason;Wanjiru, Roseline;Elsahn, Ziad;Rama Krishna Reddy Kummitha	Bridging the digital divide in Africa via universal service funds: an institutional theory perspective	2023	Information Technology & People	36	8	126-154	10.1108/IPT-01-2023-0042
25	LISA	Wadee Alhalabi;Sharma, Gajanand;Upadhyay, Utsav;Kumar, Alok;Gupta, Brij;Arya, Varsha;Chui, Kwok	Cyberbullying in the Metaverse: A Prescriptive Perception on Global Information Systems for User Protection	2023	Journal of Global Information Management	31	1	45658	10.4018/JGIM.325793
26	LISA	Heinrich, Matthew;Gerhart, Natalie	Privacy Education Effectiveness: Does It Matter?	2023	Journal of Information Systems Education	34	1	49-69	

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
27	LISA	Preston, Alison;Mawhinney, Natalie	What are the most important information skills young people need today?	2022	The School Librarian	70	3	p.10-11	
28	LISA	Kumar, Priya C;Byrne, Virginia L	The 5Ds of privacy literacy: a framework for privacy education	2022	Information and Learning Science	123	7/8	445-461	10.1108/ILS-02-2022-0022
29	LISA	Caffrey, Carolyn;Lee, Hannah;Withorn, Tessa;Clarke, Maggie;Castañeda, Amalia;Macomber, Kendra;Jackson, Kimberly M;Eslami, Jillian;Haas, Aric;Philo, Thomas;Galoozis, Elizabeth;Vermeer, Wendolyn;Andora, Anthony;Katie Paris Kohn	Library instruction and information literacy 2021	2022	Reference Services Review	50	3/4	271-355	10.1108/RSR-09-2022-0035
30	LISA	Yang, Keng;Hu, Yekang;Qi, Hanying	Digital Health Literacy: Bibliometric Analysis	2022	Journal of Medical Internet Research			e35816	10.2196/35816
31	LISA	Polizzi Gianfranco;Harrison, Tom	Wisdom in the digital age: a conceptual and practical framework for understanding and cultivating cyber-wisdom	2022	Ethics and Information Technology	24	1		10.1007/s10676-022-09640-3
32	LISA	Zhao, Yuxiang Chris;Zhao, Mengyuan;Song, Shijie	Online Health Information Seeking Behaviors Among Older Adults: Systematic Scoping Review	2022	Journal of Medical Internet Research			e34790	10.2196/34790
33	LISA	Valle, María;Barroso, Carmen;Alcalá, Leopoldo	Perceptions and Attitudes of Spanish “Digital Seniors” Towards E-Government	2022	International Journal of Electronic Government Research	18	1	p.1-19	10.4018/IJEGR.297228
34	LISA	Chisholm, Alexandria;Hartman-Caverly, Sarah	Privacy Literacy: From Doomscrolling to Digital Wellness	2022	Portal : Libraries and the Academy	22	1	53-79	

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
35	LISA	Marcial, Dave E;Palama, Jan Cynth;Maypa, Aurielle Lisa;Launer, Markus A	Responsible Digital Citizenship: A Measurement Of Trust In The World Wide Web	2022	Webology	19	2	6852-6868	
36	LISA	Dunaway, Mary;Macharía, Mary	The Effect of Digital Citizenship on Negative Online Behaviors and Learning Outcomes in Higher Education	2021	Journal of Information Systems Education	32	4	294-307	
37	LISA	Cheng, Christina;Elsworth, Gerald;Osborne, Richard H	Validity Evidence Based on Relations to Other Variables of the eHealth Literacy Questionnaire (eHLQ): Bayesian Approach to Test for Known-Groups Validity	2021	Journal of Medical Internet Research			e30243	10.2196/30243
38	LISA	Annis, Catherine;Jinghui (Jove) Hou;Tang, Tian	Perceptions, motivators and barriers of using city management applications among citizens: a focus group approach	2021	Information Technology & People	34	4	1338-1356	10.1108/ITP-03-2020-0148
39	LISA	Kar, Arpan Kumar	What Affects Usage Satisfaction in Mobile Payments? Modelling User Generated Content to Develop the “Digital Service Usage Satisfaction Model”	2021	Information Systems Frontiers	23	5	1341-1361	10.1007/s10796-020-10045-0
40	LISA	Martzoukou, Konstantina	Academic libraries in COVID-19: a renewed mission for digital literacy	2021	Library Management	42	4/5	266-276	10.1108/LM-09-2020-0131
41	LISA	Matthew Weirick Johnson;Lasher, Meggie	The Community Workshop Series: A Case Study for Community-Engaged Learning in LIS	2021	Library Trends	69	4	752-767	
42	LISA	Marino, Bill	Privacy concerns and the prevalence of third-party tracking cookies on ARL library homepages	2021	Reference Services Review	49	2	115-131	10.1108/RSR-03-2021-0009
43	LISA	Oh, Sarah Soyeon;Kyoung-A, Kim;Kim, Minsu;Oh, Jaeuk;Sang Hui Chu;Choi, JiYeon	Measurement of Digital Literacy Among Older Adults: Systematic Review	2021	Journal of Medical Internet Research	23	2	e26145	10.2196/26145
44	LISA	Mehmet Ali AK-KAYA;POLAT, Özgür	Covid-19 Pandemic Process Experience of Izmir Kâtip Celebi University Library Through Key Statistics	2021	Journal of Balkan Libraries Union	8	1	1-13	10.16918/jblu.93709

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
45	LISA	Ankamah, Samuel;Gyesi, Kwesi;Anaman, Aba Amandzewaa	The Evaluation of Information Literacy among Medical Students at the College of Health Sciences, University of Ghana	2021	Library Philosophy and Practice			1-39	
46	LISA	Amit Lavie Dinur;Aharoni, Matan;Karniel, Yuval	Safe online ethical code for and by the “net generation”: themes emerging from school students’ wisdom of the crowd	2021	Journal of Information, Communication & Ethics in Society	19	1	129-145	10.1108/JICES-02-2020-0021
47	LISA	Fázik, Jakub;Steinerová, Jela	Technologies, knowledge and truth: the three dimensions of information literacy of university students in Slovakia	2021	Journal of Documentation	77	1	285-303	10.1108/JD-05-2020-0086
48	LISA	Withorn, Tessa;Joanna Messer Kimmitt;Carolyn Caffrey Gardner;Andora, Anthony;Springfield, Cristina;Ospina, Dana;Clarke, Maggie;Martinez, George;Castañeda, Amalia;Haas, Aric;Vermeer, Wendolyn	Library instruction and information literacy 2019	2020	Reference Services Review	48	4	601-682	10.1108/RSR-08-2020-0057
49	LISA	Igbo, Harriet Uche, PhD	Undergraduates' Digital Literacy and Access to Information in Nigerian University Libraries: Does Subject Background Make a Difference?	2020	Library Philosophy and Practice			1-25	
50	LISA	Band, Barbara	Ten... no Twelve! Twitter Digital Leaders and Innovators	2020	The School Librarian	68	2	86	
51	LISA	Jacobson, Jenna;Gruzd Anatoliy	Cybervetting job applicants on social media: the new normal?	2020	Ethics and Information Technology	22	2	175-195	10.1007/s10676-020-09526-2
52	LISA	Rivero, Erin	Chapter 3. Confronting Concerns	2020	Library Technology Reports	56	4	25-33	
53	LISA	Frings-Hessami, Viviane;Sarker, Anindita;Oliver, Gillian;Misita Anwar	Documentation in a community informatics project: The creation and sharing of information by women in Bangladesh	2020	Journal of Documentation	76	2	552-570	10.1108/JD-08-2019-0167

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
54	LISA	Rana, Nripendra P;Luthra, Sunil;Rao, H Raghav	Key challenges to digital financial services in emerging economies: the Indian context	2020	Information Technology & People	33	1	198-229	10.1108/ITP-05-2018-0243
55	LISA	Black, Shelly	The implications of digital collection takedown requests on archival appraisal	2020	Archival Science	20	1	91-101	10.1007/s10502-019-09322-y
56	LISA	Magee, Rachel M;Buck, Margaret H;Kitzmann, Juliana;Morris, Nathaniel;Petrimoulx, Dylan;Rich, Matthew;Sensiba, Joshua;Tiemann, Eyan;Wempe, Aidan	Teen Social Media Practices and Perceptions of Peers: Implications for Youth Services Providers and Researchers	2019	Journal of Research on Libraries and Young Adults	10	3	1-21	
57	LISA	Anderson, Amelia;Phillips, Abigail	"Getting Basic Information Isn't as Helpful as the Nuanced Advice We Can Give Each Other": Teens with Autism on Digital Citizenship Education	2019	Journal of Research on Libraries and Young Adults	10	3	1-27	
58	LISA	Lavranou, Rena;Tsohou, Aggeliki	Developing and validating a common body of knowledge for information privacy	2019	Information and Computer Security	27	5	668-686	10.1108/ICS-08-2018-0099
59	LISA	Anonymous	ARTICLE ALERTS	2019	Journal of Information Ethics	28	2	148-156	
60	LISA	Hossain, Zakir;Hashmi, Yasmine;Mezbah-ul-Islam, Muhammad	ICT Facilities and Literacy in Rural Non-Government Secondary School Libraries of Bangladesh	2019	School Libraries Worldwide	25	2	66-80	10.14265.25.2.005
61	LISA	Marden, William;Griffey, Jason;Berman, Erin;Houghton, Sarah;West, Jessamyn;Hellman, Eric;Lamanna, T J;Beckstrom, Matt	Choose Privacy Week 2018: Big Data is Watching You	2019	Journal of Intellectual Freedom and Privacy	4	1	3-13	10.5860/jifp.v4i1.6885
62	LISA	Maceli, Monica	Librarians' Mental Models and Use of Privacy-Protection Technologies	2019	Journal of Intellectual Freedom and Privacy	4	1	18-32	10.5860/jifp.v4i1.6907

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
63	LISA	Atiso, Kodjo;Kammer, Jenna	Online Safety and Academic Scholarship: Exploring Researchers' Concerns from Ghana	2019	Journal of Librarianship and Scholarly Communication	7		n/a	10.7710/2162-3309.2263
64	LISA	Matteson, Miriam L;Gersch, Beate	Unique or ubiquitous: information literacy instruction outside academia	2019	Reference Services Review	47	1	73-84	10.1108/RSR-12-2018-0075
65	LISA	Jan Michael Alexandre Cortez Bernadas;Soriano, Cheryl Ruth	Online privacy behavior among youth in the Global South: A closer look at diversity of connectivity and information literacy	2019	Journal of Information, Communication & Ethics in Society	17	1	17-30	10.1108/JICES-03-2018-0025
66	LISA	Crawford, Sharinne;Hokke, Stacey;Nicholson, Jan M;Zion, Lawrie;Lucke, Jayne;Keyzer, Patrick;Hackworth, Naomi	"It's not black and white": Public health researchers' and ethics committees' perceptions of engaging research participants online	2019	Internet Research	29	1	123-143	10.1108/IntR-07-2017-0278
67	SCOPUS	Tomczyk Ł.; Eger L.	Online safety as a new component of digital literacy for young people; [Онлайн-безопасность как новый компонент цифровой грамотности молодежи]	2020	Integration of Education	24	2	172-184	10.15507/1991-9468.099.024.202002.172-184
68	SCOPUS	Potyrała K.; Tomczyk Ł.	Teachers in the lifelong learning process: examples of digital literacy	2021	Journal of Education for Teaching	47	2	255-273	10.1080/02607476.2021.1876499
69	SCOPUS	Adigüzel S.; Eryilmaz S.	Empowering digital citizenship through distance education: A technology-driven education action plan	2023	Critical Roles of Digital Citizenship and Digital Ethics			49-60	10.4018/978-1-6684-8934-5.ch004

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
70	SCOPUS	Nabhan S.	Pre-service teachers' conceptions and competences on digital literacy in an EFL academic writing setting	2021	Indonesian Journal of Applied Linguistics	11	1	187-199	10.17509/ijal.v11i1.34628
71	SCOPUS	Sander I.	Critical big data literacy tools - Engaging citizens and promoting empowered internet usage	2020	Data and Policy	2	3		10.1017/dap.2020.5
72	SCOPUS	Huatay K.C.V.; Mendoza A.P.M.; Rodriguez J.C.F.; Ninaquispe J.C.M.	Digital Literacy in Basic Secondary School Students: A Gender Comparative Study	2023	Proceedings of the 2023 IEEE 3rd International Conference on Advanced Learning Technologies on Education and Research, ICALTER 2023				10.1109/ICALTE R61411.2023.10372931
73	SCOPUS	Saritepeci M.; Yildiz Durak H.; Özüdođru G.; Atman Uslu N.	The role of digital literacy and digital data security awareness in online privacy concerns: a multi-group analysis with gender	2024	Online Information Review				10.1108/OIR-03-2023-0122
74	SCOPUS	Tomczyk Ł.; Potyrała K.	Parents' knowledge and skills about the risks of the digital world	2021	South African Journal of Education	41	1		10.15700/saje.v41n1a1833
75	SCOPUS	Walsh K.; Pink E.; Ayling N.; Sondergeld A.; Dallaston E.; Tournas P.; Serry E.; Trotter S.; Spanos T.; Rogic N.	Best Practice Framework for Online Safety Education: Results from a rapid review of the international literature, expert review, and stakeholder consultation	2022	International Journal of Child-Computer Interaction	33			10.1016/j.ijcci.2022.100474
76	SCOPUS	González-Villa Á.; Gewerc A.	A systematic review of the tensions between the public and private in adolescents' social networks: New education challenges	2024	E-Learning and Digital Media	21	2	141-159	10.1177/20427530231156283

	Database	Authors	Title	Year	Source (journal/ book/ proceedings)	Vol	Issue	Pages	DOI
77	SCOPUS	Nguyen K.P.; Luke A.K.; Cheng Y.; John A.; Cham K.M.	THE LIMITED LEVEL OF DIGITAL SKILLS AND COMPETENCIES OF OPTOMETRY STUDENTS	2022	Journal of Information Technology Education: Research	21		97-114	10.28945/4929
78	Dimensions	Phippen, Andy	Digital Literacy	2024					
79	Dimensions	Buchan, M. Claire; Bhawra, Jasmin; Katapally, Tarun	Improving digital literacy in a digital world: Development of an evidence-based digital literacy program and assessment tool to evaluate youth digital literacy	2023	OSF Preprints				
80	Dimensions	Voicu, Simona-Nicoleta; Crăciun, Ioan	Preventive online safety education for teenagers	2023	International Journal of Legal and Social Order	3	1		
81	Dimensions	Fazil, Abdul Wajid; Haki-mi, Musawer; Sajid, Saiddamin; Quchi, Mohammad Mustafa; Khaliqyar, Khudai Qul	Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province	2023	American Journal of Education and Technology	2	4	61	
82	Dimensions	Triratnawati, Atik; Hidayah, Sita; Lazuardi, Elan	Menjadi Pelajar Cakap Digital': Proyek Bersama Webinar dan Sosialisasi Kecerdasan Digital di Madrasah Muallimat Muhammadiyah Yogyakarta	2022	Bakti Budaya	5	1	10-24	
83	Dimensions	Shahrokh Nikou, Mark De Reuver and Matin Mahboob Kanafi	Workplace literacy skills—how information and digital literacy affect adoption of digital technology	2022	Journal of Documentation	78	7	371-391	

# APÊNDICE B

## Corpus dos abstracts tratados para o Iramuteq

### \*\*\*\* \*Abstract\_01

This study investigates the impact of digital\_literacy, citizenship, curation practices, connectedness, and online\_privacy concerns on cybersecurity behaviour. It specifically examines the moderating role of cybersecurity awareness in these factors. The objective is to examine the relationship between these elements and individuals' cybersecurity behaviours, offering valuable insights to guide training programmes and interventions. Methodology A survey was conducted on a sample of 235 individuals living in different cities in Saudi Arabia to collect data. Confirmatory factor analysis was used to assess the measuring scales, while regression analysis was employed to analyse the relationships between the variables under investigation. Additionally, a moderation test was performed to evaluate the influence of cybersecurity awareness on the associations between predictor variables and cybersecurity behaviour. Findings The regression analysis reveals significant correlations between digital\_literacy specifically copyright, citizenship, curation, and connectedness, online\_privacy concerns, and cybersecurity behaviour. The understanding of cybersecurity significantly influenced the level and trajectory of these relationships. A deeper comprehension of cybersecurity enhances the positive effects of digital\_literacy, including copyright awareness, responsible citizenship, content curation, and connectedness, on cybersecurity behaviour. Implications This study highlights the importance of tailored educational efforts that consider individuals' levels of expertise and specific concerns. Organisations and governments can utilise these findings to create customised cybersecurity training programmes, improve digital\_literacy, and tackle issues related to online\_privacy. The report highlights the significance of integrating cybersecurity knowledge into wider digital\_literacy initiatives. To the best of the researcher's knowledge, previous studies have not examined the relationship between these variables. This study contributes to current knowledge by investigating the combined influence of digital\_literacy, citizenship, curation practices, connectedness, and online\_privacy concerns on cybersecurity behaviour. Furthermore, this study examines the potential moderating impact of cybersecurity awareness.

### \*\*\*\* \*Abstract\_02

Media and technology are omnipresent in adolescent lives, with implications for digital privacy. Extant literature has yet to quantitatively explore adolescent cognitions about digital privacy in interpersonal, commercial, and institutional settings, precluding a comprehensive understanding of their motivation to engage in certain online behaviours e.g. using privacy settings, sharing personal data. Compromised privacy may result in adverse outcomes e.g. identity theft, cyberbullying, sexual solicitation, stalking, thus, the present study aims to fill this gap through the development and validation of a theoretically grounded measurement model of adolescent privacy-related cognitions Adolescent Cognitions about Online\_Privacy; ACOP, utilising confirmatory factor analysis within a structural equation framework. Study participants n = 960, 10-14 years old completed a digital survey on technology use and attitudes, including items on digital privacy-related attitudes, subjective norms, and perceived behavioural control. A three-factor model of adolescent privacy-related cognitions demonstrated adequate model fit. Invariance was established between all groups tested and latent mean differences emerged based on gender, race, and online risk level. This study is an important first step in quantitative understanding of adolescent privacy-related cognitions based on strong theoretical rationale. Further validation of this model is needed to inform on digital\_literacy interventions or apply in predictive analyses.

### \*\*\*\* \*Abstract\_03

In the first of two articles, interviews with administrators of digital literacy programs in Canadian public libraries and other community organizations revealed a sector working to address the digital divide, focusing on marginalized people. Programs narrowly defined digital literacy as skillful use of a

range of basic and more advanced technologies. Funding from corporate or other external sources and community interest are key to establishing programs. Challenges arise from lack of resources, including staff time, and limited staff expertise, as well as competition for learners' time.

\*\*\*\* \*Abstract\_04

This study analyzes the previous literature on the online\_safety of children and youth under the 4Cs risk framework concerning contact, content, conduct, and contract risks. It then conducts a comparative study of Australia, Canada, and the UK, comparing their institutions, governance, and government-led programs. Relevant research in Childhood Education Studies is insufficient both in quantity and quality. To minimize the four major online risks for children and youth in cyberspace, it is necessary to maintain a regulatory approach to the online exposure of children under the age of 13. Moreover, the global society should respond together to these online risks with multi-level policymaking under a multi-stakeholder approach. At the international level, multilateral discussion within the OECD and under UN subsidiaries should continue to lead international cooperation. At the domestic level, a special agency in charge of online\_safety for children and youth should be established in each country, encompassing all relevant stakeholders, including educators and digital firms. At the school and family levels, both parents and teachers need to work together in facilitating digital\_literacy education, providing proper guidelines for the online activities of children and youth, and helping them to become more satisfied and productive users in the digital era.

\*\*\*\* \*Abstract\_05

In this article we present the level of knowledge and literacy held by the parents of primary school students regarding internet safety online\_safety, digital safety in the context of digital\_literacy in terms of both technical skills and knowledge. The study reported on here was conducted in Poland, and was commissioned by the Ministry of National Education. The research involved measuring the knowledge and skills regarding the prevention of electronic threats ethreats which are defined as problematic situations and behaviour mediated by digital media and the internet. E-threats are related to mental and physical health, social aspects and technical matters related to the use of information and communication technologies ICTs. In order to narrow down the research area, 6 components related to e-threats were selected, namely: the ergonomics of using digital media; the evaluation of the reliability of online information; the influence of advertising on consumers' choices; risky online relationships; understanding the mechanisms of secure logging-in; and protection against malware. The DL level was measured using a competence test. An analysis of 514 tests revealed that the most neglected areas were the protection of children against unwanted communication with other users, and secure loggingin. The strongest component was the ergonomics of using ICT. We also noted that more than one fifth of parents showed a satisfactory level of DL related to online\_safety. Another observation was that DL is a complex and heterogeneous concept. The DL components are related with one another to different extents. Some DL elements are determined by the level of education, place of living, subjective sense of own well-being or intuitive perception self-evaluation.

\*\*\*\* \*Abstract\_06

This research focuses on transparency in a digital environment, examines how it is perceived by customers through different evaluations perceived clarity, objectivity, and openness, and examines how each of these dimensions affects customer trust and engagement to the brand. It pointed out that judgements of transparency differ according to the relationship that consumers have personally developed with their digital environment literacy, consumer acumen, and concern for privacy. Based on an empirical study conducted in e-commerce N = 445, the results show that perceived clarity - unlike perceived objectivity - is accompanied by a decline in trust and has a direct impact on engagement. On the contrary, perceived openness encourages engagement but not trust. This research highlights how consumer literacy and consumer acumen promote the perception of transparency, while concern for privacy degrades it. Theoretical and practical implications are then drawn from this research.

\*\*\*\* \*Abstract\_07

Older adults' growing use of the internet and related technologies, further accelerated by the COVID\_19 pandemic, has prompted not only a critical examination of their behaviours and attitudes

about online threats but also a greater understanding of the roles of specific characteristics within this population group. Based on survey data and using descriptive and inferential statistics, this empirical study delves into this matter. The behaviours and attitudes of a group of older adults aged 60 years and older n=275 regarding different dimensions of online\_safety and cybersecurity are investigated. The results show that older adults report a discernible degree of concern about the security of their personal information. Despite the varied precautions taken, most of them do not know where to report online threats. What is more, regarding key demographics, the study found some significant differences in terms of gender and age group, but not disability status. This implies that older adults do not seem to constitute a homogeneous group when it comes to attitudes and behaviours regarding safety and security online. The study concludes that support systems should include older adults in the development of protective measures and acknowledge their diversity. The implications of the results are discussed and some directions for future research are proposed.

\*\*\*\* \*Abstract\_08

The pandemic of COVID\_19 has been accelerating the digital transformation in every area of political, economic and social area of life. The protection of informational privacy has been essential condition upon which the possibility of ongoing positive change depends. Under the amendment of statutes about personal data protection in Feb. 2020, which consolidates the statutes and government organizations related to data protection, the new organization is expected to develop more reasonable and effective legal systems. One of the tasks is to develop the specific approach to children's online\_privacy because they are most active and sophisticated user of new online services and at the same time they lack the ability to assess the potential risks of compromising informational privacy and seek remedies for breach. It is inevitable to make paternalistic approach by transferring children's power to consent to parents or legal agents. However, it is not enough to respond to various demands. To empower children themselves to navigate the digital communication environment and make good decisions for themselves, parents, teachers as well as service providers should cooperate to raise digital\_literacy of children. Since the Act on Promotion of Information and Communications Network Utilization and Information Protection, ETC had adopted the power to consent of legal representatives of a child in 2011, the Act on the Protection of Personal Information has adopted almost same approaches. In the amendment of the Act on Promotion of Information and Communications in 2018.12. it has been newly introduced the power to make public policies for the protection of children, the obligation of service providers to provide information in understandable way by children and to acquire the parents' consent in a verifiable way. For the future improvement, the issues such as proper range of children's age, more supports for the empowerment strategy should be subject to social discussions and policy-making.

\*\*\*\* \*Abstract\_09

This scoping review of research explores which disciplines have studied social media as it relates to education and, more broadly, use by students of high school and college age. The sample explores 10 years of research 2009 to 2018. A search of Web of Science yielded 580 relevant peer-reviewed articles published through the end of 2018, with 260 44.8% of these articles focused on education. Research in this area has been on a steady upward trajectory since 2009, the first year when relevant social media articles appeared. About half of this research was conducted in North American settings, and quantitative surveys were the most popular data collection method. Findings show that within education, the dominant themes of research on social media were use as a teaching and learning tool; adoption, use, and beliefs; digital\_literacy; effects of use; and identity. Outside of education, the dominant themes were negative behaviours, health issues, identity development and expression, digital citizenship, and social relationships. This review shows several areas where education researchers and practitioners would benefit from attending to research conducted outside of our discipline. Although the field of educational research sufficiently addresses issues like teacher professional development and pedagogical uses of social media, the larger issues that affect our students and, in turn, the school context are being explored in other disciplines.

\*\*\*\* \*Abstract\_10

Objectives Digital\_media\_literacy has been recognized internationally as an important competence.

The 2022 Revised Curriculum for elementary and secondary education reflects Digital\_media\_literacy as an essential competency for democratic citizenship. While the global trend suggests early childhood as the time for commencing Digital\_media\_literacy education, the related elements are not specifically contained in the Korean national early childhood curriculum Nuri Curriculum. The purpose of the current study is to propose a direction for revision of the Nuri Curriculum by comparatively analyzing the educational expectations, structures, and contents related to Digital\_media\_literacy in early childhood curricula in Finland, Canada Ontario, and Australia. Methods: Finland, Canada, and Australia implement lifetime media\_literacy education and systematically include media\_literacy in national level early childhood curricula. Educational expectations, structures, and contents related to digital\_literacy and media\_literacy were analyzed according to media\_literacy and related skills and elements. Results First, the educational expectations from international early childhood education curricula reflects Digital and media literacy competency. Second, the international curricula suggest active online\_safety in ways such as participating in a safe, media-friendly environment. Finally, the international curricula encourage active development of digital\_literacy by suggesting diverse ways of using media. Conclusion For digital\_media\_literacy development in early childhood, the elements of digital\_media\_literacy should be more specifically contained in the national level curriculum. Considering the change in the 2022 Revised Curriculum and global trend, it is necessary to reflect competencies in

digital\_media\_literacy comprehensively in the Nuri Curriculum.

\*\*\*\* \*Abstract\_11

Purpose Following major lower extremity amputation LEA, patients experience significant emotional distress and are at risk for anxiety and depression. There is a lack of mental health supports for this population, and internet-based cognitive behavioural therapy iCBT may be a useful resource to meet this need. The purpose of this study was to use a qualitative approach to explore the mental health needs of LEA patients and to gauge their attitudes of the use of iCBT to help them cope with their amputation. Methods Semi-structured qualitative interviews were conducted with inpatients and outpatients with LEA recruited from a major urban rehabilitation hospital. Data were analysed using inductive codebook thematic analysis TA. Results Ten interviews were completed with individuals with LEA. The main themes identified were: 1 Fixating on the past; 2 Worry about the future; 3 Unmet mental health needs; 4 Barriers to Mental Health Support; 5 Importance of peer support; and 6 Tailoring iCBT. Conclusions Our findings highlight that patients with LEA are open to learning more about iCBT to meet their mental health needs. Key iCBT implementation considerations include taking into account issues of stigma associated with mental health, timing of delivery, levels of digital\_literacy, online\_security, and interactive content.

\*\*\*\* \*Abstract\_12

Social networks are colonised by a culture of confession that turns teenager privacy into a commodity to achieve recognition and social acceptance. This display accelerates the porosity of the boundaries between the public and the private and feeds surveillance capitalism. The aim of this systematic review is to examine the empirical evidence on the public-private interaction of teenagers' contributions to social networks in the last 5 years in databases: Eric, Scopus and Web of Science. Based on the Prisma Statement, the initial search produced 1449 documents, of which 81 were included in the final analysis after the application of exclusion and inclusion criteria and the purging of duplicates. The results show a field of study developed with a decreasing trend in production in recent years, knowledge gaps and discordant findings. It is concluded the need to build solid knowledge and initiate new lines in the study of the issue in order to understand the exhibition of teenagers in social networks. It is points out the urgency of a training based on their own media practices and in digital\_literacy for a broad understanding of online\_privacy.

\*\*\*\* \*Abstract\_13

Gradually, society has shifted more services online, with COVID\_19 highlighting digital inequalities in access to services such as healthcare. Older adults can experience such digital inequalities, yet this group is also more likely to need medical appointments, compared to younger people. With the growing digitalisation of healthcare, it is increasingly important to understand how older people can

best use communicative e-health services to interact with healthcare services. This is especially if older adults are to access, and actively interact with health professionals/clinicians due to their general health decline. This review aims to synthesise older adults' experiences and perceptions of communicative e-health services and, in turn, identify barriers and facilitators to using communicative e-health services. **Methods** A meta-ethnography was conducted to qualitatively synthesise literature on older adults' experiences of using communicative e-health services. A systematic search, with terms relating to 'older adults', 'e-health', 'technology', and 'communication', was conducted on six international databases between January 2014 and May 2022. The search yielded a total of 10 empirical studies for synthesis. **Results** The synthesis resulted in 10 themes that may impact older adults' perceptions and/or experiences of using communicative e-health services. These were: 1 health barriers, 2 support networks, 3 application interface/design, 4 digital\_literacy, 5 lack of awareness, 6 online\_security, 7 access to digital devices and the internet, 8 relationship with healthcare providers, 9 in-person preference and 10 convenience. These themes interlink with each other. **Conclusion** The findings suggest older adults' experiences and perceptions of communicative e-health services are generally negative, with many reporting various barriers to engaging with online services. However, many of these negative experiences are related to limited support networks and low digital\_literacy, along with complicated application interfaces. This supports previous literature identifying barriers and facilitators in which older adults experience general technology adoption and suggests a greater emphasis is needed on providing support networks to increase the adoption and usage of communicative e-health services.

\*\*\*\* \*Abstract\_14

**Objective.** To analyze the effect of privacy violation experience on privacy-protective behaviors **Background.** In the era of rapid development of Internet technologies, privacy issues call for scientific reflection. Understanding the factors that regulate online user behaviour might assist in elaborating the adequate privacy policy. **Study design.** Regression analysis provides a parametric evaluation of the effect of privacy experience on usage of privacy settings. Various matching technics were applied for preliminary balancing of the control N=215 and treatment groups N=160 by a set of key covariates. **Participants.** Users of the largest Russian online social network VKontakte from the Russian city Vologda. The sample size is 375 respondents 55% female from 16 to 83 age Mean=32,5; Med. =31; SD=12,9. **Measurements.** Both survey data on privacy experience and observed behavioral data on privacy settings from users' online accounts were used. Additionally, the scale of P. Tetterdell & D. Holman on propensity to make social connection and M. Rosenberg's self-esteem scale were adopted in the study **Results.** The experience of privacy violation does not lead to the cautious behaviour online: the users tend to regulate only the access to the public posts on profile due to past bad experience. The privacy settings literacy turns significantly affect the usage of privacy settings. **Conclusions.** The findings support the privacy paradox hypothesis. As having specific online\_privacy management skills encourages more cautious behaviour online, digital\_literacy interventions can improve the safety of social networking sites.

\*\*\*\* \*Abstract\_15

In UK, regulatory discussions have been brought up by the Brexit referendum of 2016. The UK governments has approached diversely including i DCMS of the UK Council for Internet Safety as an administrative regulatory department; ii Ofcom as a broadcasting and telecommunication regulatory government; and 3 Electoral Commission as a regulatory system to prevent disseminating disinformation in the course of the election. The UK's regulatory methods includes i interpreting existing laws Defamation law, Communication Law, Data Protection Law, ii establishing new law Digital Signature law, Online\_Safety Law, iii establishing detailed guideline, iv strengthening ethical standard of the independent regulatory institute, v requiring more responsibility of the service providers. Moreover, indirect guidelines are discussed including RESIST Counter-Disinformation Toolkit, SHARE checklists. Currently, new direct regulatory methods including making new laws seems not be welcomed because these could interfere the freedom of the people in the cyberspace and these could not be so effective ways of preventing disinformation issues. Rather, indirect but strong regulatory alternatives are introducing such as self-regulatory methods of the service providers, strengthening digi-

tal\_literacy of the users. These indirect ways could include disclosing information flows in the cyberspace, methods of the data analysis, or online users' right access, revise, refuse to automatic decision etc, which would be good references in South Korea.

\*\*\*\* \*Abstract\_16

Datatified societies need informed public debate about the implications of data science technologies. At present, internet users are often unaware of the potential consequences of disclosing personal data online and few citizens have the knowledge to participate in such debates. This paper argues that critical big data literacy efforts are one way to address this lack of knowledge. It draws on findings from a small qualitative investigation and discusses the effectiveness of online critical big data literacy tools. Through pre and post use testing, the short- and longer-term influence of these tools on people's privacy attitudes and behaviour was investigated. The study's findings suggested that the tools tested had a predominantly positive initial effect, leading to improved critical big data literacy among most participants, which resulted in more privacy-sensitive attitudes and internet usage. When analyzing the tools' longer-term influence, results were more mixed, with evidence suggesting for some that literacy effects of the tools were short-lived, while for others they led to more persistent and growing literacy. The findings confirm previous research noting the complexity of privacy attitudes and also find that resignation toward privacy is multi-faceted. Overall, this study reaffirms the importance of critical big data literacy and produces new findings about the value of interactive data literacy tools. These tools have been under-researched to date. This research shows that these tools could provide a relevant means to work toward empowering Internet users, promoting a critical internet usage and, ideally, enabling more citizens to engage in public debates about changing data systems.

\*\*\*\* \*Abstract\_17

Technologies such as the Internet, smartphones, and sex toys have demonstrated the capacity to facilitate and enhance sexual and intimate practice by offering new ways to meet sexual partners, maintain and establish intimate connections, and providing access to sexual education and exposure to new ways of engaging in sex. They have also afforded novel risks to safety, privacy, and sexual autonomy. Understanding how people perceive and experience both the risks and benefits of using technology to facilitate sex and intimacy is important to understanding contemporary sexual practice, health, and pleasure. However, research in this space is currently hampered by a lack of quantitative measures to accurately and holistically assess both the risks and benefits in the context of technologised sexual practices. Methods To facilitate a nuanced quantitative exploration of these concepts, we present the psychometric properties of the newly developed Risks and Benefits of Technologised Sexual Practice Scale. Results Using an exploratory Study 1, n = 445 and confirmatory factor analysis Study 2, n = 500, this paper presents evidence for a 6-factor scale Benefits 3 'sexual gratification', 'connection', and 'access to information and culture'; Risks 3 'concerns', 'worries', and 'knowledge of rights and ownership'. Conclusion This scale may be used to contribute to research areas including sexual health, sexual behaviour, sexual education, online connection, online\_safety, and digital\_literacy with the aim to contribute to a sex- and technology-positive framework for understanding sexual health and pleasure. Technology has the potential to benefit relationships - it can facilitate and enhance sexual and intimate practices in a variety of ways. However, it also has the potential to be risky, with people reporting concerns about safety and privacy. This paper presents a new measure that is designed to accurately assess perceptions of the risks and benefits of sexualised technology use.

\*\*\*\* \*Abstract\_18

In recent years, there has been phenomenal growth in internet usage worldwide, with a substantial proportion of children and adolescents actively engaging with online platforms. While the internet presents numerous opportunities for children and adolescents, the lack of digital\_literacy and adequate online\_safety measures exposes them to various cybercrimes, including cyberbullying, cyberstalking, identity theft, and sexual predation. Moreover, there is growing concern regarding internet addiction among this population. METHODS To investigate the determinants of internet addiction among adolescents, we conducted a cross-sectional study in peri-urban Delhi-NCR, India. We used a

self-administered questionnaire to gather information on internet usage, and 630 adolescents aged 13-18 participated in the study, also completing an Internet Addiction Test. RESULTS The findings indicate that 415 adolescents 65.9 % exhibited no signs of internet addiction, suggesting a healthy relationship with the internet. However, 215 adolescents 33.1 % displayed symptoms of internet addiction. Among those exhibiting internet addictions, 159 74.0 % were classified as mild internet addicts, indicating moderate levels of internet usage. Furthermore, 56 26.0 % adolescents were classified as moderate internet addicts, reflecting a higher level of internet addiction. CONCLUSIONS Our study highlights the significant influence of various factors, including family dynamics, environmental factors, and personal experiences, on internet addiction among adolescents. Based on these findings, we propose implementing measures at different levels to foster responsible internet use among adolescents, thereby substantially reducing internet addiction.

\*\*\*\* \*Abstract\_19

Traditional information\_literacy skills e.g., effectively finding and evaluating information need to be updated due to the rapidly changing information ecosystem and the growing dominance of online platforms that use algorithms to control and shape information. This article proposes additions to the current ACRL Framework for Information Literacy for Higher Education that relate to algorithmic literacy. The "Authority is Constructed and Contextual" frame can be applied to recognizing the need to question algorithmic authority including algorithmic bias, the Information Has Value" frame can be used to acknowledge online platforms' use of proprietary algorithms allowing third parties to access personal data, and the "Searching as Strategic Exploration" frame can draw attention to search results in online platforms are mediated through algorithms. Classroom activities to teach the new knowledge practices and dispositions are also included.

\*\*\*\* \*Abstract\_20

Pavey discusses the impact of artificial intelligence AI on education and the need for information\_literacy specialists to adapt. She reflects on the rapid advancements in AI technology, such as ChatGPT, and the potential implications for teaching and assessment. While some educational organizations, like the International Baccalaureate Organisation, have embraced AI, others are skeptical and may choose to ban it. Pavey argues that instead of fearing AI, educators should focus on developing critical information, media, and digital\_literacy skills in students. She suggests that AI can alleviate the tedium of routine writing tasks, allowing students to engage in more creative and critical thinking. However, she acknowledges the concerns about cheating and the need for effective regulation. She urges educators to adapt their teaching methods and embrace the opportunities presented by AI in education.

\*\*\*\* \*Abstract\_21

This study aims to investigate the trending term Netiquette as an important element in the effective digital citizenship. The research suggests a systematic framework of netiquette rules in the field of online education based on the classical core rules of netiquette and according to the digital citizenship scale DCS. The research also studies the corresponding responsibilities of both educators and students to raise awareness towards using technology in a balanced, safe, smart and ethical way as the shift towards the digital activities increased significantly in the post-corona time. Design/methodology/approach The research used the qualitative data that were based on the everyday observation and analysis of the online education experience at the university of Jordan in the academic year 2020/2021; the online group discussions of students and teachers; and investigating the guidelines of the online learning netiquette rules in various academic institutes. Comparative analysis was conducted to merge and eliminate redundant rules and to add sub rules, and then to cluster them into groups. The suggested clustered groups were distributed into the classical core rules outline of netiquette. In each core rule, the sub rules were reclassified and recategorized according to the DCS by studying the complexity levels and their corresponding factors. The suggested framework updates and adds DCS levels and factors considering the exceptional experience of online education through the pandemic. Findings The research finds that "Netiquette" had been neglected in cyber ethics literature, and so it has to be rediscovered through the lens of digital citizenship that becomes very noticeable issue in the post COVID era. So, the research presents a systematic framework that

outlines more than 150 netiquette sub rules in the field of online education, and that were clustered according to DCS and the classical core rules of netiquette. It also adds a new factor to the bottom level of DCS which is the primarily skills and traits, and also updates the internet and political activism factor by adding the social perspective. Originality/value A novel classification of the classical core rules of netiquette was proposed in the field of online education to serve as a spectrum of identifying the complexity of digital citizenship levels and factors. This research can be a starting point of more works on netiquette research in online education and on other fields such as online business meetings, social media networking and online gaming.

\*\*\*\* \*Abstract\_22

Despite recent significant strides toward acceptance, inclusion, and equality, members of the lesbian, gay, bisexual, transgender, and queer LGBTQ community still face alarming mental health disparities, being almost 3 times more likely to experience depression, anxiety, and suicidal thoughts than their heterosexual counterparts. These unique psychological challenges are due to discrimination, stigmatization, and identity-related struggles and can potentially benefit from generative conversational artificial intelligence AI. As the latest advancement in AI, conversational agents and chatbots can imitate human conversation and support mental health, fostering diversity and inclusivity, combating stigma, and countering discrimination. In contrast, if not properly designed, they can perpetuate exclusion and inequities. Objective: This study aims to examine the impact of generative conversational AI on the LGBTQ community. Methods: This study was designed as a scoping review. Four electronic scholarly databases Scopus, Embase, Web of Science, and MEDLINE via PubMed and gray literature Google Scholar were consulted from inception without any language restrictions. Original studies focusing on the LGBTQ community or counselors working with this community exposed to chatbots and AI-enhanced internet-based platforms and exploring the feasibility, acceptance, or effectiveness of AI-enhanced tools were deemed eligible. The findings were reported in accordance with the PRISMA-ScR Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews. Results: Seven applications HIVST-Chatbot, TelePrEP Navigator, Amanda Selfie, Crisis Contact Simulator, REALbot, Tough Talks, and Queer AI were included and reviewed. The chatbots and internet-based assistants identified served various purposes: 1 to identify LGBTQ individuals at risk of suicide or contracting HIV or other sexually transmitted infections, 2 to provide resources to LGBTQ youth from underserved areas, 3 facilitate HIV status disclosure to sex partners, and 4 develop training role-play personas encompassing the diverse experiences and intersecting identities of LGBTQ youth to educate counselors. The use of generative conversational AI for the LGBTQ community is still in its early stages. Initial studies have found that deploying chatbots is feasible and well received, with high ratings for usability and user satisfaction. However, there is room for improvement in terms of the content provided and making conversations more engaging and interactive. Many of these studies used small sample sizes and short-term interventions measuring limited outcomes. Conclusions: Generative conversational AI holds promise, but further development and formal evaluation are needed, including studies with larger samples, longer interventions, and randomized trials to compare different content, delivery methods, and dissemination platforms. In addition, a focus on engagement with behavioral objectives is essential to advance this field. The findings have broad practical implications, highlighting that AI's impact spans various aspects of people's lives. Assessing AI's impact on diverse communities and adopting diversity-aware and intersectional approaches can help shape AI's positive impact on society as a whole.

\*\*\*\* \*Abstract\_23

Digital health has the potential to improve the quality of care, reduce health care costs, and increase patient satisfaction. Patient acceptance and consent are a prerequisite for effective sharing of personal health information PHI through health information exchanges HIEs. Patients need to form and retain trust in the systems they use to leverage the full potential of digital health. Germany is at the forefront of approving digital treatment options with cost coverage through statutory health insurance. However, the German population has a high level of technology skepticism and a low level of trust, providing a good basis to illuminate various facets of eHealth trust formation. Objective: In a German setting, we aimed to answer the question, How does an individual form a behavioral intent

to share PHI with an HIE platform? We discussed trust and informed consent through 1 synthesizing the main influence factor models into a complex model of trust in HIE, 2 providing initial validation of influence factors based on a qualitative study with patient interviews, and 3 developing a model of trust formation for digital health apps. Methods: We developed a complex model of the formation of trust and the intent to share PHI. We provided initial validation of the influence factors through 20 qualitative, semistructured interviews in the German health care setting and used a deductive coding approach to analyze the data. Results: We found that German patients show a positive intent to share their PHI with HIEs under certain conditions. These include perceived information security and a noncommercial organization as the recipient of the PHI. Technology experience, age, policy and regulation, and a disposition to trust play an important role in an individual's privacy concern, which, combined with social influence, affects trust formation on a cognitive and emotional level. We found a high level of cognitive trust in health care and noncommercial research institutions but distrust in commercial entities. We further found that in-person interactions with physicians increase trust in digital health apps and PHI sharing. Patients' emotional trust depends on disposition and social influences. To form their intent to share, patients undergo a privacy calculus. Hereby, the individual's benefit eg, convenience, benefits for the individual's own health, and the benefits for public welfare often outweigh the perceived risks of sharing PHI. Conclusions: With the higher demand for timely PHI, HIE providers will need to clearly communicate the benefits of their solutions and their information security measures to health care providers physicians, nursing and administrative staff and patients and include them as key partners to increase trust. Offering easy access and educational measures as well as the option for specific consent may increase patients' trust and their intention to share PHI.

\*\*\*\* \*Abstract\_24

The purpose of this paper is to provide evidence-based policy recommendations for improving the implementation of universal service funds USF with a view to closing the digital divide in Africa. Design/methodology/approach The paper adopts a qualitative approach that draws examples from various African countries supported by 25 interviews from key stakeholders with hands-on experience and roles that shape telecommunications policy in Africa and other developing countries. Findings The study's findings point out that institutional voids which characterize several African countries inhibit the effectiveness of USF in African countries. The authors identify several institutional and organisational factors and explain how they negatively affect the performance of USF. The authors find that in order to overcome these obstacles, there is a need for a clear redefinition of Universal Access and Service UAS policies, restructuring the governance of USF, encouraging cross-sectoral collaborations, and bottom-up initiatives to bridge the digital divide in African countries. Originality/value The paper contributes to the underexplored USF literature by shedding light on the role of institutional factors in determining the success of USF. The paper thus complements and provides a different perspective on promoting digital inclusion in Africa from the viewpoint of institutional voids, bringing new insights into the existing literature on how to deal with an intractable area of UAS policy and the wider digital divide debate in developing countries.

\*\*\*\* \*Abstract\_25

The emergence of the metaverse, a virtual reality space, has ushered in a new era of digital experiences and interactions in global information systems. With its unique social norms and behaviours, this new world presents exciting opportunities for users to connect, socialize, and explore. However, as people spend more time in the metaverse, it has become increasingly apparent that the issue of cyberbullying needs to be addressed. Cyberbullying is a serious problem that can harm victims psychologically and physically. It involves using technology to harass, intimidate, or humiliate individuals or groups in global information systems. The risk of cyberbullying is high in the metaverse, where users are often anonymous. Therefore, it is crucial to establish a safer and more respectful culture within the metaverse to detect and prevent such incidents from happening.

\*\*\*\* \*Abstract\_26

Mobile devices are a constantly used item in a college student's life. Students depend on them for entertainment, academics, and socializing with their friends. While they continually use them, they

perhaps do not understand the impact of their use on their privacy or that the devices can be used to track them and collect their personal information. This study utilizes the Antecedent, Privacy Concern, Outcome APCO model, combined with the Fogg behaviour Model FBM to determine 1 the factors that comprise privacy concerns on a mobile device; 2 whether individuals use privacy-protective behaviours, and 3 whether education on privacy issues regarding mobile devices will increase their use of privacy-enhancing technology PET. A longitudinal study was conducted to test whether privacy protection education increases the use of PET. While students express concern for their privacy when using mobile devices and express an intent to use additional PET, their behaviour using mobile device protections does not change, even after an educational intervention. Perceived privacy control does not change their privacy concern and habit and trust outweigh the impact of privacy concern. Theoretical and practical implications are provided.

\*\*\*\* \*Abstract\_27

In 2022, information skills have never been more important for young people. The pandemic has brought about a step-change in the use of, and reliance upon, digital media. Events in the past two years have focused a new spotlight on the issues of misinformation and disinformation, and upcoming online\_safety legislation highlights the importance of finding ways to mitigate online harms. Here, Preston and Mawhinney share insights into what information skills young people need to navigate the digital world today.

\*\*\*\* \*Abstract\_28

Existing privacy-related educational materials are not situated in privacy theory, making it hard to understand what specifically children learn about privacy. This article aims to offer learning objectives and guidance grounded in theories of privacy and learning to serve as a foundation for privacy\_literacy efforts. Design methodology approach This article reviews theories of privacy and literacy as social practices and uses these insights to contribute a set of learning objectives for privacy education called the 5Ds of privacy\_literacy. Findings This article connects the 5Ds of privacy\_literacy with existing curricular standards and offers guidance for using the 5Ds to create educational efforts for preteens grounded in theories of sociocultural learning. Practical implications Learning scientists, instructional designers and privacy educators can use the 5Ds of privacy\_literacy to develop educational programs that help children hone their ability to enact appropriate information flows. Social implications Current approaches to privacy education treat privacy as something people need to protect from the incursions of technology, but the authors believe the 5Ds of privacy\_literacy can redefine privacy – for children and adults alike – as something people experience with the help of technology. Originality/value This study uniquely integrates theories of privacy and learning into an educational framework to guide privacy\_literacy pedagogy.

\*\*\*\* \*Abstract\_29

This paper presents recently published resources on library instruction and information\_literacy. It provides an introductory overview and a selected annotated bibliography of publications covering various library types, study populations and research contexts. The selected bibliography is useful to efficiently keep up with trends in library instruction for busy practitioners, library science students and those wishing to learn about information\_literacy in other contexts. Design/methodology/approach &gt; This article annotates 424 English-language periodical articles, monographs, dissertations, theses and reports on library instruction and information\_literacy published in 2021. The sources were selected from the EBSCO platform for Library, Information Science, and Technology Abstracts LISTA, Education Resources Information Center ERIC, Scopus, ProQuest Dissertations and Theses, and WorldCat, published in 2021 that included the terms information\_literacy, library instruction, or information fluency in the title, abstract or keywords. The sources were organized in Zotero. Annotations summarize the source, focusing on the findings or implications. Each source was categorized into one of seven pre-determined categories: K-12 Education, Children and Adolescents; Academic and Professional Programs; Everyday Life, Community, and the Workplace; Libraries and Health Information\_Literacy; Multiple Library Types; and Other Information\_Literacy Research and Theory. Findings &gt; The paper provides a brief description of 424 sources and highlights sources that contain unique or significant scholarly contributions. Originali-

ty/value &gt; The information may be used by librarians, researchers and anyone interested as a quick and comprehensive reference to literature on library instruction and information\_literacy within 2021.

\*\*\*\* \*Abstract\_30

Digital health is growing at a rapid pace, and digital health literacy has attracted increasing attention from the academic community. Objective The purposes of this study are to conduct a systematic bibliometric analysis on the field of digital health literacy and to understand the research context and trends in this field. Methods Methods A total of 1955 scientific publications were collected from the Web of Science core collection. Institutional co-operation, journal co-citation, theme bursting, keyword co-occurrence, author co-operation, author co-citation, literature co-citation, and references in the field of digital health literacy were analyzed using the VOSviewer and CiteSpace knowledge mapping tools. Results The results demonstrate that the United States has the highest number of publications and citations in this field. The University of California System was first in terms of institutional contributions. The Journal of Medical Internet Research led in the number of publications, citations, and co-citations. Research areas of highly cited articles in the field of digital health literacy mainly include the definition and scale of health literacy, health literacy and health outcomes, health literacy and the digital divide, and the influencing factors of health literacy. Conclusions: We summarized research progress in the field of digital health literacy and reveal the context, trends, and trending topics of digital health literacy research through statistical analysis and network visualization. We found that digital health literacy has a significant potential to improve health outcomes, bridge the digital divide, and reduce health inequalities. Our work can serve as a fundamental reference and directional guide for future research in this field.

\*\*\*\* \*Abstract\_31

The internet presents not just opportunities but also risks that range, to name a few, from online abuse and misinformation to the polarisation of public debate. Given the increasingly digital nature of our societies, these risks make it essential for users to learn how to wisely use digital technologies as part of a more holistic approach to promoting human flourishing. However, insofar as they are exacerbated by both the affordances and the political economy of the internet, this article argues that a new understanding of wisdom that is germane to the digital age is needed. As a result, we propose a framework for conceptualising what we call cyber-wisdom, and how this can be cultivated via formal education, in ways that are grounded in neo-Aristotelian virtue ethics and that build on three prominent existing models of wisdom. The framework, according to which cyber-wisdom is crucial to navigating online risks and opportunities through the deployment of character virtues necessary for flourishing online, suggests that cyber-wisdom consists of four components: cyber-wisdom literacy, cyber-wisdom reasoning, cyber-wisdom self-reflection, cyber-wisdom motivation. Unlike the models on which it builds, the framework accounts for the specificity of the digital age and is both conceptual and practical. On the one hand, each component has conceptual implications for what it means to be wise in the digital age. On the other hand, informed by character education literature and practice, it has practical implications for how to cultivate cyber wisdom in the classroom through teaching methods that match its different components.

\*\*\*\* \*Abstract\_32

With the world's population aging, more health-conscious older adults are seeking health information to make better-informed health decisions. The rapid growth of the internet has empowered older adults to access web-based health information sources. However, research explicitly exploring older adults' online health information seeking OHIS behaviour is still underway. Objective: This systematic scoping review aims to understand older adults' OHIS and answer four research questions: 1 What types of health information do older adults seek and where do they seek health information on the internet? 2 What are the factors that influence older adults' OHIS? 3 What are the barriers to older adults' OHIS? 4 How can we intervene and support older adults' OHIS? Methods: A comprehensive literature search was performed in November 2020, involving the following academic databases: Web of Science; Cochrane Library database; PubMed; MEDLINE; CINAHL Plus; APA PsycINFO; Library and Information Science Source; Library, Information Science and Technology Abstracts; Psychology

and Behavioral Sciences Collection; Communication & Mass Media Complete; ABI/INFORM; and ACM Digital Library. The initial search identified 8047 publications through database search strategies. After the removal of duplicates, a data set consisting of 5949 publications was obtained for screening. Among these, 75 articles met the inclusion criteria. Qualitative content analysis was performed to identify themes related to the research questions. Results: The results suggest that older adults seek 10 types of health information from 6 types of internet-based information sources and that 2 main categories of influencing factors, individual-related and source-related, impact older adults' OHIS. Moreover, the results reveal that in their OHIS, older adults confront 3 types of barriers, namely individual, social, and those related to information and communication technologies. Some intervention programs based on educational training workshops have been created to intervene and support older adults' OHIS. Conclusions: Although OHIS has become increasingly common among older adults, the review reveals that older adults' OHIS behaviour is not adequately investigated. The findings suggest that more studies are needed to understand older adults' OHIS behaviours and better support their medical and health decisions in OHIS. Based on the results, the review proposes multiple objectives for future studies, including 1 more investigations on the OHIS behaviour of older adults above 85 years; 2 conducting more longitudinal, action research, and mixed methods studies; 3 elaboration of the mobile context and cross-platform scenario of older adults' OHIS; 4 facilitating older adults' OHIS by explicating technology affordance; and 5 promoting and measuring the performance of OHIS interventions for older adults.

\*\*\*\* \*Abstract\_33

A typology of user was explored as to behaviour and perception of e-Government through a telephone survey involving 405 Internet users between 60 and 79 years of age. Ten different groups were identified by means of dimensionality reduction techniques followed by a cluster analysis. The main conclusion is that there is no consistent pattern, although among the groups which do use e-Government, they have less concerns than the rest and see less need for modifications to be applied to adapt the websites to the needs of seniors. Within this older age group, two types are clearly identified. Those who feel uncomfortable, which explains their avoidance of eGovernment, and to a lesser degree, those whose lack of contact with public administration may be due to a lack of interest for such services. It appears that a senior-friendly offering together with learning opportunities would increase interest for this channel.

\*\*\*\* \*Abstract\_34

Personal technology use can significantly impact wellness. The transition to widespread remote learning, working, and socializing during the COVID\_19 pandemic exacerbated society's reliance on technology. This article presents a case study of how the authors applied their privacy scholarship to offer a responsive learning experience for students concerning the social implications of the pandemic. The article also explores the authors' unique approach to digital wellness, which seeks to align wellness goals and habits regarding technology while placing a special emphasis on privacy, particularly information asymmetries, attention engineering, and the hidden harms of invasive data collection.

\*\*\*\* \*Abstract\_35

The Internet is a powerful platform in the workplace. However, when abused, it is a place that destroys everyone. This paper presents how society is practicing netizenship responsibility. Specifically, it measures trust towards the Internet and social media as perceived by the employees. It also describes predictors that affect confidence level on the Internet and social media trust. A total of 5146 were analyzed from 36 countries. An online survey questionnaire was used utilizing the Marcial Launer Digital Trust in the Workplace Questionnaire. Results show that the overall mean of the agreement level on Internet trust is moderate  $x$  equals 2.59. It also shows that age, gender, continent, innovation index, income level, social technologic ladder, internet satisfaction, job position, company form, company role, and company size were significant predictors of Internet trust. It is concluded that citizens have reasonable confidence that society is doing responsible citizenship. There is a need to establish an ecosystem that can be digitally trusted.

\*\*\*\* \*Abstract\_36

With the increase in Internet use, there has been an upsurge in negative online behaviours such as cyberbullying and online harassment among college students. As a result of the negative online behaviours, many students may experience anxiety, depression, feelings of loneliness, and alienation, which ultimately can impact their well-being and interfere with their ability to learn. It is envisaged that extending digital citizenship behaviour to educational settings will arrest, or at the very least help mitigate, the impact of these negative behaviours on student learning outcomes. Using data collected from 184 university students, results show that perceived learning outcomes indirectly impact the relationship between digital citizenship and cyberbullying behaviours.

\*\*\*\* \*Abstract\_37

Background: As health resources and services are increasingly delivered through digital platforms, eHealth literacy is becoming a set of essential capabilities to improve consumer health in the digital era. To understand eHealth literacy needs, a meaningful measure is required. Strong initial evidence for the reliability and construct validity of inferences drawn from the eHealth Literacy Questionnaire eHLQ was obtained during its development in Denmark, but validity testing for varying purposes is an ongoing and cumulative process. Objective: This study aims to examine validity evidence based on relations to other variables—using data collected with the known-groups approach—to further explore if the eHLQ is a robust tool to understand eHealth literacy needs in different contexts. A priori hypotheses are set for the expected score differences among age, sex, education, and information and communication technology ICT use for each of the 7 eHealth literacy constructs represented by the 7 eHLQ scales. Methods: A Bayesian mediated multiple indicators multiple causes model approach was used to simultaneously identify group differences and test measurement invariance through differential item functioning across the groups, with ICT use as a mediator. A sample size of 500 participants was estimated. Data were collected at 3 diverse health sites in Australia. Results: Responses from 525 participants were included for analysis. Being older was significantly related to lower scores in 4 eHLQ scales, with 3. Ability to actively engage with digital services having the strongest effect total effect  $-0.37$ ;  $P < .001$ , followed by 1. Using technology to process health information total effect  $-0.32$ ;  $P < .001$ , 5. Motivated to engage with digital services total effect  $-0.21$ ;  $P = .01$ , and 7. Digital services that suit individual needs total effect  $-0.21$ ;  $P = .02$ . However, the effects were only partially mediated by ICT use. Higher education was associated with higher scores in 1. Using technology to process health information total effect  $0.22$ ;  $P = .01$  and 3. Ability to actively engage with digital services total effect  $0.25$ ;  $P < .001$ , with the effects mostly mediated by ICT use. Higher ICT use was related to higher scores in all scales except 2. Understanding health concepts and language and 4. Feel safe and in control. Either no or ignorable cases of differential item functioning were found across the 4 groups. Conclusions: By using a Bayesian mediated multiple indicators multiple causes model, this study provides supportive validity evidence for the eHLQ based on relations to other variables as well as established evidence regarding internal structure related to measurement invariance across the groups for the 7 scales in the Australian community health context. This study also demonstrates that the eHLQ can be used to gain valuable insights into people's eHealth literacy needs to help optimize access and use of digital health and promote health equity.

\*\*\*\* \*Abstract\_38

The purpose of this paper is to understand citizens' perceptions of smartphone-based city management apps and to identify facilitators and barriers that influence app adoption and use. An aim is to identify how current technology adoption theories might be expanded and enriched for studying citizen adoption of city apps in the US. Design/methodology/approach This paper presents a qualitative exploratory case study of citizen perceptions of city management apps in Tallahassee, a top-ranked digital city in the southeastern United States. The authors derive empirical data from focus group discussions with citizens using thematic analysis. Findings Overall, the findings suggest that city management apps are primarily perceived and used by citizens as handy and efficient tools for the provision of information and public services. The findings suggest that current technology adoption and use models applied to citizen adoption of m-government may benefit by being expanded for the US context. Originality/value This paper highlights what factors of m-government technology are effective, useful or inhibiting in citizens' lives from the perspective of a group of citizens in the south-

eastern US. Implications that might be learned for researchers and practitioners are discussed.

\*\*\*\* \*Abstract\_39

Mobile payment services have become increasingly important in daily lives in India due to multiple planned and unplanned events. The objective of this study is to identify the determinants of usage satisfaction of mobile payments which could enhance service adoption. The “Digital Service Usage Satisfaction Model” has been proposed and validated by combining technology adoption and service science literature. First the data was extracted from Twitter based on hashtags and keywords. Then using sentiment mining and topic modelling the large volumes of text were analysed. Then network science was also used for identifying clusters among associated topics. Then, using content analysis methodology, a theoretical model was developed based on literature. Finally using multiple regression analysis, we validated the proposed model. The study establishes that cost, usefulness, trust, social influence, credibility, information privacy and responsiveness factors are more important to increase the usage satisfaction of mobile payments services. Also methodologically, this is an endeavour to validate a new approach which uses social media data for developing a inferential theoretical model.

\*\*\*\* \*Abstract\_40

The COVID\_19 pandemic has placed online learning, blended or hybrid provision as the “new normal” in Higher Education. For most universities and their academic libraries, especially those with a less strong online presence, the pandemic has caused numerous challenges. However, it has also been a catalyst for change and resifting of priorities. For academic librarians involved in the delivery of information skills literacy training, a renewed mission is emerging, addressing access and connectivity to resources, designing for online education and fostering the development of digital\_literacy of students. Design methodology approach This is a conceptual paper based on the author's personal experiences and subjective opinion as a Library and Information Science educator with considerable expertise in online distance learning in the UK. Reflecting critically on the impact of the pandemic from an educational point of view and on key changes experienced, the paper centres on the argument that academic librarians could emerge as strategic partners in Higher Education, towards the direction of enhancing students' digital competences development. Findings The complete and involuntary shift to online learning due to COVID\_19 restrictions has opened the door to multiple challenges in Higher Education, which are complex and ongoing: the implementation of remote tools and practices en masse in online teaching and learning in a way that ensures accessibility and equity for all, issues connecting to online pedagogy and how to prepare students with the information and digital\_literacy competences required for the new online learning normal. As academic libraries move forward, they have a renewed mission to help learners in the online space to become both information rich and digitally competent. There is an opportunity to act as the connecting link that will help to move a step forward a strategic vision that places design for equity at the centre of education. Originality/value The impact of COVID\_19 within Higher Education and academic libraries more specifically, is a theme that has not been yet sufficiently discussed, researched or critically debated as the world is still currently going through the pandemic crisis. This paper aims to initiate some early thoughts and conversation, as well as put forward the author's personal critical positioning on the issues, challenges and potential opportunities, emerging in the current educational climate for academic librarians, and to highlight areas of importance for the design and direction of information and library science curricula.

\*\*\*\* \*Abstract\_41

For over a decade, the University of North Carolina at Chapel Hill has offered some variation of the Community Workshop Series, a partnership to provide digital\_literacy and computer technology classes to community members at local public libraries. Both authors have served as coordinators of the program as library science graduate students at the University of North Carolina School of Information and Library Science. We situate this program within existing literature on digital\_literacy and information\_literacy, community engagement, and the graduate student experience to show the utility of this program and similar programs for training graduate students, enhancing the graduate student experience, supporting the needs of community members, and bolstering the capacities of

public libraries. The authors provide an overview of the program and encourage others to start similar programs. To this end, the authors present a case study of the Community Workshop Series, including discussion of creating the program and keeping things going, and provide a how-to guide for creating your own. The authors identify four recommendations for creating a similar program to clearly delineate takeaways that might inform readers' attempts to create similar programs, and they provide additional materials and documentation in appendices to support the creation of new community-engaged programs in LIS.

\*\*\*\* \*Abstract\_42

The integration of third-party resources on library websites may be inadvertently contributing to surveillance technologies without user knowledge. This study set out to determine the prevalence of third-party tracking cookies on ARL member homepages, the entities that are tracking users and for what purpose and what control users have over their cookie preferences. Design/methodology/approach Homepages from the 124 ARL member libraries were visited. Evidence of a privacy or cookie statement was collected and cookie logs were captured. This data were compared against the Disconnect list of known trackers and analyzed to determine the extent to which third-party tracking cookies were used across ARL sites, who was setting the cookies and for what purpose, and whether this use differed with regards to a library's identifying features. Findings It was determined that many ARL libraries do contribute to the ability to track a user's activity across the web, with one-third containing third-party tracking cookies. A user's contact with tracking cookies is influenced by various traits defining the institution. Users are given very little control over the cookies logged on their machines. Originality/value This study explores library efforts to protect user privacy, adopting an introspective approach that focuses on library websites. It will provide discussion points for librarians to question not only what third-party tracking cookies are present on their sites and why, but also how to educate their users about privacy issues.

\*\*\*\* \*Abstract\_43

Background Numerous instruments are designed to measure digital literacy among the general population. However, few studies have assessed the use and appropriateness of these measurements for older populations. Objective: This systematic review aims to identify and critically appraise studies assessing digital literacy among older adults and to evaluate how digital literacy instruments used in existing studies address the elements of age appropriate digital literacy using the European Commission's Digital Competence DigComp Framework. Methods: Electronic databases were searched for studies using validated instruments to assess digital literacy among older adults. The quality of all included studies was evaluated using the Crowe Critical Appraisal Tool CCAT. Instruments were assessed according to their ability to incorporate the competence areas of digital literacy as defined by the DigComp Framework 1 information and data literacy, 2 communication and collaboration, 3 digital content creation, 4 safety, and 5 problem-solving ability, or attitudes toward information and communication technology use. Results: Searches yielded 1561 studies, of which 27 studies 17 cross-sectional, 2 before and after, 2 randomized controlled trials, 1 longitudinal, and 1 mixed methods were included in the final analysis. Studies were conducted in the United States 18/27, Germany 3/27, China 1/27, Italy 1/27, Sweden 1/27, Canada 1/27, Iran 1/27, and Bangladesh 1/27. Studies mostly defined older adults as aged  $\geq 50$  years 10/27 or  $\geq 60$  years 8/27. Overall, the eHealth Literacy Scale eHEALS was the most frequently used instrument measuring digital literacy among older adults 16/27, 59%. Scores on the CCAT ranged from 34 34/40, 85% to 40 40/40, 100%. Most instruments measured 1 or 2 of the DigComp Framework's elements, but the Mobile Device Proficiency Questionnaire MDPQ measured all 5 elements, including "digital content creation" and "safety." Conclusions The current digital literacy assessment instruments targeting older adults have both strengths and weaknesses, relative to their study design, administration method, and ease of use. Certain instrument modalities like the MDPQ are more generalizable and inclusive and thus, favorable for measuring the digital literacy of older adults. More studies focusing on the suitability of such instruments for older populations are warranted, especially for areas like digital content creation and safety that currently lack assessment. Evidence based discussions regarding the implications of digitalization for the treatment of older adults and how health care professionals may benefit from this phe-

nomenon are encouraged.

\*\*\*\* \*Abstract\_44

Information centers aim at meeting the information requirements of the society they serve, while they become active parts of all kinds of experiences within the society in this process. However, it is more important for information centers which can become social institutions of culture in that way to show their adaptation skills in extraordinary times. Thus, they contribute to the normalization of life within the identity of a public institution. In their quality as active and integral contributors of formal education provided in our country, the university libraries are among the most important information centers that are expected to turn this responsibility into a priority reflex. The outbreak of the COVID\_19 pandemic that continues to cause severe trauma and chaos globally has introduced an atmosphere in which university libraries are expected to show such a reaction. The present study aims to show how the university libraries in our country have been affected by the pandemic and the new conditions, and to what extent their services will adapt to the new normal, as will be exemplified by the case study of Izmir Katip Celebi University IKCU Library. To that effect, a comparison has been made between 2019 the former "normal" for the libraries and 2020 when the pandemic broke out in March also in Turkey. As a result, an analysis based on specific

\*\*\*\* \*Abstract\_45

The purpose of this study was to assess the information\_literacy of medical students at the University of Ghana. The convenience sampling technique was used to choose 206 respondents for the study, which yielded a response rate of 93.7 per cent. The study found that the majority of respondents needed information to acquire new knowledge in a subject area and to write assignments or project work. Moreover, most respondents rely on books, electronic books, and journals as their primary sources of knowledge. Furthermore, most respondents stated that they obtain their information via the internet. Additionally, most responders use the databases PubMed, ScienceDirect, and Google Scholar. Again, the majority of respondents are aware of the concept of plagiarism and will acknowledge the author of a book if they use a piece of it in their work or study. Last but not least, respondents major concerns about information access were low internet speed, high cost of books and other information materials, and information overload. Thus, it is strongly recommended among others that the CHS administration especially the CHS Library should manage and develop their collections in that required and relevant information sources will be available for students to use in their assignments and project works.

\*\*\*\* \*Abstract\_46

Children are becoming heavy users of communication and information technologies from an early age. These technologies carry risks to which children may be exposed. In collaboration with the Israel Ministry of Education IME, the authors launched a week-long safe online awareness program for school children in 257 elementary and middle schools in Israel. Each class independently composed a safe and ethical code of online behaviour following two classroom debate sessions. The purpose of this study was to analyze these codes and learn how school children perceive and understand the proper use of the network using thematic analysis. Design methodology approach A total of 8,181 students between the ages of 8 and 14 years in 303 classes from 257 schools participated in the program. These classes composed 303 ethical codes, which were decomposed into 2,201 elements phrases, sentences, or paragraphs. Using mixed-methods research combining quantitative and qualitative methodologies, the elements of the ethical codes were analyzed, interpreted, and classified to identify the dominant themes and discourses used by the students when addressing issues related to safe online use. Findings Findings indicate that Israeli students are aware of the dangers and risks of the internet, and these concerns are reflected in their own ethical codes. The students discouraged online self-exposure and encouraged precautions and wariness towards members of out-groups. The themes included sentences which asked for responsible, appropriate, and lawful use, expressed concern about privacy issues, and stated the need for adult involvement. Most of them reflected an us against them strangers perspective. Originality value The current study presents an innovative "bottom-up" program based on wisdom of the crowd approach, that can be implemented in schools internationally in order to encourage reflexivity and teach children the necessary skills for safe online

experiences. In addition, this study analyses the school children's own views of the dangers of social media and learn about their perspective and understanding of internet use.

\*\*\*\* \*Abstract\_47

The purpose of this paper is to inform on results of the study based on the dissertation project – the study of newcoming university students and their information\_literacy experience. It describes the three categories of information\_literacy experience as perceived by these students. Design/methodology/approach The document is based on a qualitative phenomenographic study of 40 first year undergraduate students of teacher education programs from five faculties of Comenius University in Bratislava. Data were collected from each participant in two stages by three methods: written statements, drawings and interviews. Findings The phenomenographic analysis results in three categories of information\_literacy: 1 the conception of digital technologies, 2 the conception of knowledge and 3 the conception of truth. The outcome space presented by two alternative models points to a strong interrelation of all three categories. The resulting conceptions point to the diversity of the concept of information\_literacy in relation to other types of literacies, especially digital\_literacy, reading and media literacy, as well as to intersections with other scientific disciplines such as psychology, cognitive science or philosophy. Research limitations/implications The most important limits of this qualitative research are the low numbers of participants and the high degree of subjectivity in data evaluation. For this reason, a verification study was carried out one-year later. Originality value Although phenomenographic studies of information\_literacy in the educational context are quite common, the third category of this study brings a new contribution to the information\_literacy theory – the dimension of truth or truthfulness of information.

\*\*\*\* \*Abstract\_48

This paper aims to present recently published resources on library instruction and information\_literacy, providing an introductory overview and a selected annotated bibliography of publications covering various library types, study populations and research contexts. Design/methodology/approach This paper introduces and annotates English-language periodical articles, monographs, dissertations, reports and other materials on library instruction and information\_literacy published in 2019. Findings The paper provides a brief description of all 370 sources and highlights sources that contain unique or significant scholarly contributions. Originality/value The information may be used by librarians, researchers and anyone interested as a quick and comprehensive reference to literature on library instruction and information\_literacy.

\*\*\*\* \*Abstract\_49

The study attempted to find out whether undergraduates subject background has influence on their application of digital\_literacy skills in accessing digital information for educational problem solving. The design of the Ex- Post Facto survey was used for the study. A37- item Questionnaire was used to collect data from a sample of 1506, which represented 5% of 30,121 undergraduates of seven federal universities in southern Nigeria, which were purposely selected for the study. The major finding of the study showed that subject background had strong influence and makes the difference in undergraduates ability to use digital\_literacy skills in accessing information. The direction of the difference is that those in science-related disciplines demonstrated greater skills than those in Arts-related fields in the application of digital\_literacy skills for information access. The major challenge was lack of adequate education and training for developing digital\_literacy skills among undergraduates. It was recommended among others, that the National Universities Commission NUC should formulate policies that would enforce university-wide training of undergraduates, especially those in Arts Humanities for digital\_literacy skills development.

\*\*\*\* \*Abstract\_50

Band features 12 Twitter digital leaders and innovators. These include the DigitalPrimaryTeacher, Edufuturists, and Edtech UK.

\*\*\*\* \*Abstract\_51

With the introduction of new information communication technologies, employers are increasingly engaging in social media screening, also known as cybervetting, as part of their hiring process. Our research, using an online survey with 482 participants, investigates young people's concerns with

their publicly available social media data being used in the context of job hiring. Grounded in stakeholder theory, we analyze the relationship between young people's concerns with social media screening and their gender, job seeking status, privacy concerns, and social media use. We find that young people are generally not comfortable with social media screening. A key finding of this research is that concern for privacy for public information on social media cannot be fully explained by some "traditional" variables in privacy research. The research extends stakeholder theory to identify how social media data ethics should be inextricably linked to organizational practices. The findings have theoretical implications for a rich conceptualization of stakeholders in an age of social media and practical implications for organizations engaging in cybervetting.

\*\*\*\* \*Abstract\_52

Today's library and information professionals are confronting gendered voice assistant personas, bias in misunderstood speech, data privacy and security concerns, and inherited inequalities informing algorithms and misinformation. In chapter 3 of Library Technology Reports vol. 56, no. 4 Virtual Voice Assistants, we address the ways library and information professionals can collaborate to create meaningful change to disrupt bias and inequality in digital assistant technology while safeguarding against privacy and security concerns and moving toward a more ethical and inclusive AI ecosystem.

\*\*\*\* \*Abstract\_53

The purpose of this paper is to discuss the creation and sharing of information by Bangladeshi women participants in a community informatics project and to assess to what extent the information provided to them meets their short and longer-term needs. Design/methodology/approach The analysis is based on data collected during a workshop with village women in Dhaka and focus group discussions in rural Bangladesh in March and April 2019. The information continuum model is used as a framework to analyse the data. Findings The study shows that the women document their learning and share it with their families and communities and that they are very conscious of the importance of keeping analogue back-ups of the information provided to them in digital format. They use notebooks to write down information that they find useful and they copy information provided to them on brown paper sheets hung in the village community houses. Practical implications This paper raises questions about how information is communicated to village women, organised and integrated in a community informatics project, and more generally about the suitability and sustainability of providing information in digital formats in a developing country. Originality/value The paper shows how village women participants in a community informatics project in Bangladesh took the initiative to create and preserve the information that was useful to them in analogue formats to remedy the limitations of the digital formats and to keep the information accessible in the longer term.

\*\*\*\* \*Abstract\_54

Digital financial services DFS have substantial prospect to offer a number of reasonable, appropriate and secure banking services to the underprivileged in developing countries through pioneering technologies such as mobile phone based solutions, digital platforms and electronic money models. DFS allow unbanked people to obtain access to financial services through digital technologies. However, DFS face tough challenges of adoption. Realising this, the purpose of this paper is to identify such challenges and develop a framework. Design methodology approach The authors developed a framework of challenges by utilising interpretive structural modelling ISM and fuzzy MICMAC approach. The authors explored 18 such unique set of challenges culled from the literature and further gathered data from two sets of expert professionals. In the first phase, the authors gathered data from 29 professionals followed by 18 professionals in the second phase. All were pursuing Executive MBA programme from a metropolitan city in South India. The implementation of ISM and fuzzy MICMAC provided a precise set of driving, linkage and dependent variables that were used to derive a framework. Findings ISM model is split in eight different levels. The bottom level consists of a key driving challenge V11 i.e. high cost and low return related problem, whereas the topmost level consists of two highly dependent challenges namely V1 i.e. risk of using digital services and V14 i.e. lack of trust. The prescribed ISM model shows the involvement of "high cost and low return related problem V11", which triggers further challenges of DFS. Originality value None of the existing research has explored key challenges to DFS in detail nor formulated a framework for such challenges. To the best

of the authors' knowledge, this is the first paper on DFS that attempts to collate its challenges and incorporate them in a hierarchical model using ISM and further divide them into four categories of factors using fuzzy MICMAC analysis.

\*\*\*\* \*Abstract\_55

As data privacy legislation and protections are implemented and advocated for internationally, archivists must consider how these developments impact their work, particularly appraisal. Online digital collections make records more easily accessible to researchers and the general public. However, private and sensitive information may be disseminated through these collections inadvertently. In 2018, the European Union EU passed the General Data Protection Regulation, which includes right to be forgotten RTBF legislation. This enables EU citizens to request the redaction of their personal information online. In the wake of EU court rulings which demonstrate how the RTBF impacts what archives make accessible, and increasing public concerns regarding online\_privacy, archivists should be aware of the possibility of receiving increased digital collection takedown requests and what their legal liabilities may be. This article explores how takedown requests, as well as RTBF advocacy and criticism, are positioned with respect to appraisal theory. It also addresses how takedown requests affect appraisal praxis and how archivists can be better prepared to manage them.

\*\*\*\* \*Abstract\_56

This paper presents the results of an empirical study examining teen social media practices, which was collaboratively developed, carried out, analyzed, and presented by a team of researchers that included seven teens. This co-designed study characterizes the social media use of thirteen teens through a survey, highlighting their complex relationships to technology and their prioritization of learning when online. Further, the results highlight that some teens' assessment of information shared through social media is socially informed, while others rely on preexisting perceptions and beliefs when deciding what to believe on social media. Through the analysis of these findings, the teen researchers who participated in the project had access to opportunities for metacognition and literacy skills development. By connecting the co-designed study and the experiences of the teen researchers, this paper contributes an argument that teens have complex perceptions of their relationships with social media and that collaborative research with teens is achievable and valuable, with direct implications discussed for youth services providers in libraries as well as researchers.

\*\*\*\* \*Abstract\_57

In this exploratory study, the researchers examine the intersection of teens with autism as public library users, their perceptions of and experiences with cyberbullying, and the potential role of public librarians in providing relevant digital citizenship programming. Results from this study indicate that teens on the autism spectrum live rich digital lives and have experience with both sides of cyberbullying, or digital drama. This study suggests that teens are willing to answer questions about their digital lives and demonstrate a desire to learn more about best practices in navigating the online environment, especially when learning alongside peers. Practical implications based in inclusion are given for public librarians seeking to implement digital citizenship education for the communities they serve.

\*\*\*\* \*Abstract\_58

This paper aims to present a common body of knowledge CBK for the field of information privacy, titled InfoPrivacy CBK. The purpose of the proposed CBK is to guide internet users to better understand the concept of information privacy and associate information privacy-related concepts. The InfoPrivacy CBK was created with an educational orientation to provide the basis for designing privacy awareness and training programs and organizing relevant educational material. Design methodology approach The proposed CBK for information privacy was developed conceptually and includes five domains and four levels of analysis. It is illustrated with conceptual maps. The authors identified a variety of concepts related to information privacy and created a set of categories to categorize the concepts. They used, as inclusion criteria, both theoretical and practical information privacy aspects, so that the developed CBK can address the challenges of modern technologies for preserving information privacy. Findings To validate and refine the conceptually developed CBK, the authors conducted an empirical research, in which seven information privacy experts participated. The experts commented largely positively for the structure and content of InfoPrivacy CBK, as well as for the ex-

tent to which it achieves the intended educational goals. Research limitations/implications The proposed InfoPrivacy CBK was validated by a limited number of information privacy experts, mainly due to the lengthy and in-depth participation that was required. Practical implications The InfoPrivacy CBK can be used primarily by privacy awareness and training programs developers, such as organizations, data protection officers, the state, educational policy makers and teachers. Social implications Internet users will benefit from InfoPrivacy CBK by acquiring knowledge and skills from theoretically grounded training programs, which can enhance their awareness and critical thinking on issues related to the protection of their information privacy. This will lead to more privacy-aware online societies, communities, networks, etc. Originality/value This work intends to bridge the existing gap in the literature through the creation of a novel CBK for information privacy; information privacy is a field for which no such research effort has been recorded. This paper offers important knowledge in the field of information privacy, which could be useful to both technological education designers and learners students, employees, etc.

\*\*\*\* \*Abstract\_59

Apparently, there is no end to the falsifying reporter compounded now by the president's deceptive statements as well as fake news. "E.U. Fines Mastercard \$650 Million Over Fees" Amie Tsang, The New York Times January 23, 2019, p. B3 Mastercard, like other enormous companies see above, has displeased the European Commissioners "by raising payment-processing fees artificially." B1, B4 French authorities fined Google \$57 million for failing to fully inform users of its search engine, Google Maps, and YouTube concerning data collection for targeted advertising. The New York Times March 6, 2019, p. A23 Wu begins with a list of the percentage of Americans who want positive things: 75 percent of us would like the very rich to be taxed at a higher rate; 83 percent desire net neutrality; 60 percent want more potent privacy legislation; and 92 percent would like Medicare to attempt to get drug costs lowered. According to Dargis, one of the Times' primary cinema critics, J.T. LeRoy is a superior film.

\*\*\*\* \*Abstract\_60

The study explored the ICT facilities and services at rural Non-Government Secondary NGS school libraries in Bangladesh. It identified the ICT literacy of NGS school library professionals known as assistant librarians. An exploratory method was used to ensure the best possible outcomes. Based on the interview and literature review in the qualitative phase, a questionnaire was developed for the quantitative phase and collected 86 responses using an online survey. Findings showed, most of the rural NGS school libraries do not have the ICT facilities and of those that do, they are insufficient in number to provide efficient services to library users. There was a lack of ICT skills among assistant librarians and most agreed that ICT literacy would increase the efficiency of their work and regarded it as an essential tool for school libraries. The study provides an analysis of the prevailing situation that helps in planning for policy makers and further in-depth research.

\*\*\*\* \*Abstract\_61

Five months ago, when the members of ALA's Privacy Subcommittee met to decide on this year's [2018] "Choose Privacy Week" CPW theme, it's a fair bet to say that only a tiny percentage of the general public had ever heard of Cambridge Analytica, Aleksandr Kogan, the SCL Group, or of a fairly obscure app called thisisyourdigitallife. And yet, there were warnings about Cambridge Analytica's program as early as December 2015, when the London Guardian first reported on this data-collection program and its integration with Facebook as part of Ted Cruz's 2016 bid for the US presidency. Michael Zimmer, a University of Wisconsin-Milwaukee associate professor and a member of ALA's Privacy Subcommittee, was quoted by the Guardian about why the use of such data was highly problematic. "It's one thing for a marketer to try to predict if people like Coke or Pepsi," said Zimmer, "but it's another thing for them to predict things that are much more central to our identity, and what's more personal in how I interact with the world in terms of social and cultural issues?" In the wake of Mark Zuckerberg's Congressional testimony last week [in April 2018] and the related explosion of public interest in how online personal data is collected, stored, shared, used, and sometimes misused, this year's CPW theme—"Big Data is Watching You"—could not be more perfectly timed.

\*\*\*\* \*Abstract\_62

Libraries of all kinds are uniquely positioned to educate and advocate for the use of privacy-protection technologies PPT by our patrons and in our communities; this naturally extends our decades-long mission to protect our patrons' privacy in both digital and physical library environments. In pursuit of building an understanding of the challenges to expanding such work, this research study assesses librarians' existing technical knowledge of the internet's function, and their current use and understanding of a series of popular PPT. This research study begins to close the gap in research by building our knowledge of practicing librarians' underlying assumptions about the function of the internet and how these internal models are employed in their understanding and use of PPT. Research study participants were asked to draw and explain their perception of the functioning of the internet, to use several PPT, and to explain the protections afforded by each technology. The findings indicate that participants maintained inaccurate mental models of the internet and PPT, leading to difficulties in understanding function, and that they struggled with organizational and technical barriers to integrating such technologies into their daily lives.

\*\*\*\* \*Abstract\_63

This paper investigates factors, including fears of cybercrime, that may affect researchers' willingness to share research in institutional repositories in Ghana. METHODS Qualitative research was conducted to understand more about the experiences of Ghanaian researchers when sharing research in institutional repositories. Interviews were conducted with 25 participants, documents related to policy and infrastructure in Ghana were examined, and observations were held in meetings of information technology committees. FINDINGS The findings indicate that researchers are specifically concerned about three areas when sharing research online: fraud, plagiarism, and identity theft. DISCUSSION This paper adds to research that examines barriers toward using institutional repositories, and highlights the lack of basic preventative strategies in Ghana—such as training, security, and infrastructure that are commonplace in developed countries. CONCLUSION This study draws on findings from Bossaller and Atiso 2015 that identified fears of cybercrime as one of the major barriers to sharing research online for Ghanaian researchers. While several other studies have found that fear of identity theft or plagiarism are barriers toward sharing work in the institutional repository, this is the first study that looks specifically at the experiences researchers have had with cybercrime to understand this barrier more fully.

\*\*\*\* \*Abstract\_64

The purpose of this paper is to investigate how US public libraries offer information\_literacy IL instruction to their patrons. Design methodology approach The study is a content analysis of eight library websites to determine passive IL instruction and active literacy instruction. Findings Library web guides offer passive IL instruction by highlighting resources patrons may wish to access to resolve information inquiries. Further, the authors found that a little less than 50 per cent of library programming offers some IL instruction, the majority of which relates to helping patrons learn to use tools to create information products. Originality/value IL is the ability to recognize the need for information, to effectively find information to meet that need and to use information for some purpose or goal. Academic, school and public libraries believe that understanding and using information critically and effectively bring gains to an individual and to society. However, they diverge in how and why they engage in IL instruction. The authors' findings suggest that less than half of the libraries surveyed are providing active IL instruction, despite the recognition of the benefits IL provides.

\*\*\*\* \*Abstract\_65

The purpose of this paper is twofold. First, it explores the extent to which diversity of connectivity or the connection through multiple internet access points may facilitate online\_privacy behaviour. Second, it explains the diversity of connectivityonline\_privacy behaviour link in terms of information\_literacy. Design methodology approach Situated in the context of urban poor youth in the Philippines n = 300, this paper used a quantitative approach, specifically an interview-administered survey technique. Respondents were from three cities in Metro Manila. To test for indirect relationship, survey data were analyzed using bootstrapping technique via SPSS macro PROCESS Hayes, 2013. Findings Urban poor youth with diversified connection to the internet engaged in online\_privacy behaviour. The more the youth are connected to the internet through diverse modalities, the more

this fosters cautious online\_privacy behaviour. In addition, information\_literacy explained how diversity of connectivity facilitated online\_privacy behaviour. It suggests that differences in online\_privacy behaviour may result from the extent of basic knowhow of navigating online information. In the context of the urban poor in the Global South, the youth are constantly negotiating ways to not only connect to the internet but also acquire digital skills necessary for protective online behaviours. Originality/value To date, this is one of the few papers to contribute to conversations about online\_privacy among youth in the Global South. It broadens the literature on social determinants of online\_privacy behaviour that is crucial for designing policy interventions for those in the margins.

\*\*\*\* \*Abstract\_66

The internet offers an opportunity for researchers to engage participants in research in a cost-effective and timely manner. Yet the use of the internet as a research tool internet research comes with a range of ethical concerns, and the rapidly changing online environment poses challenges for both researchers and ethics committees. The purpose of this paper is to highlight the key ethical issues of using the internet to recruit, retain and trace participants in public health research, from the perspectives of researchers and human research ethics committee HREC members. Design methodology approach This study employed a qualitative design using semi-structured interviews with eight public health researchers and seven HREC members in Australia to explore the key ethical issues of using the internet to engage research participants. Findings The study identified commonalities between researchers and HREC members regarding the utility and ethical complexity of using the internet to recruit, retain and trace research participants. The need for guidance and support regarding internet research, for both groups, was highlighted, as well as the need for flexibility and responsiveness in formal ethical processes. Originality/value This research contributes to the understanding of how the internet is used to engage participants in public health research and the ethical context in which that occurs. Supporting the ethical conduct of internet research will benefit those involved in research, including researchers, HRECs, organisations and research participants.

\*\*\*\* \*Abstract\_67

Digital\_literacy refers to the skills required to achieve digital competence, the confident and critical use of information and communication technology for learning, leisure, communication and future work of young people. Digital competence has a dual nature. First of all, it is the technical ability to operate programs, pages, equipment. Secondly, it is also the ability to use digital media safely. Both perspectives are important in the educational perspective, i.e. media education and socialisation. Materials and Methods. The paper presents the attempts to measure digital\_literacy in the area of threats resulting from using the new media in the group of upper-secondary school students fourth educational cycle. The study was carried out using a diagnostic test with 18 questions. The research was conducted in the group of 1693 youths aged 15–21. The research was designed based on traditional methods of testing knowledge and skills. Results. The findings showed that the weakest digital\_literacy component was the copyright-related knowledge and the strongest area was online shopping and financial operations. All digital\_literacy components are interrelated. The improvement in one area leads to the development of other digital\_literacy elements. Despite this correlation, digital\_literacy is a heterogeneous concept. There are also differences regarding certain digital\_literacy components, determined by gender – girls obtained higher test results in terms of the soft competencies whereas boys were better with the technical aspects of digital\_literacy. Based on the cluster analysis, we noticed that 41.41% of the students obtained good and very good results from the competence test. More than half of the students require further education in most of the analysed areas. Discussion and Conclusion. For educational decision-makers, the findings highlight the importance of designing training programs aimed at developing students' digital literacies, with a special focus on new topics as sexting, piracy and cyberbullying. © Tomczyk Ł., Eger L., 2020.

\*\*\*\* \*Abstract\_68

The text aims at measuring digital\_literacy among teachers of the third stage of education in Poland lower secondary schools. The study was commissioned by the Ministry of National Education and was conducted in 2018 in Poland, and involved a group of 484 teachers. The goal of the research was

to present the teachers' knowledge and skills related to digital threats in the areas of the assessment of the reliability of information, sexting, cyberbullying, intellectual property rights, the protection of online images, and protection against malware. Digital\_literacy DL was measured using a knowledge and competence test and a diagnostic survey. The ability to enter the LLL process thanks to the ongoing advancement of ICT increases the online\_safety of all of the school-related stakeholders. A detailed analysis of the results also revealed that the teachers obtained good results in the test in terms of their knowledge about sexting and image protection but scored poorly regarding copyright and the assessment of the reliability of online information; male teachers know more about the technical aspects of digital safety than female teachers; trainees need particular support in the form of informal and non-formal education. © 2021 International Review of Finance Ltd.

\*\*\*\* \*Abstract\_69

The European Union Digital Education Action Plan addresses the imperative of digital citizenship in the landscape of post-pandemic education. This abstract highlights the plan's focus on equipping learners with the skills to navigate the digital sphere responsibly. Emphasizing digital\_literacy, online\_safety, and ethical behaviour also the plan aims to foster critical engagement with safer technology by promoting inclusivity and equitable access, it seeks to empower individuals to thrive as responsible digital citizens in an interconnected world.

\*\*\*\* \*Abstract\_70

This case study seeks to examine pre-service teachers' digital\_literacy conceptions in an EFL academic writing context and aims to identify pre-service teachers' competences concerning the predominant dimensions of digital\_literacy encompassing critical thinking, online\_safety skills, digital culture, collaboration and creativity, finding information, communication, and functional skills. This case study involved both quantitative and qualitative data taken from 107 preservice teachers' online questionnaires and one 5-member focus group discussion delivered to pre-service teachers taking academic writing subjects in English Language Education Department in an urban university in Indonesia. In general, the result of the study revealed that the pre-service teachers' conceptions of digital\_literacy were principally associated with the narrow proficiency of utilizing online tools and technological devices and set aside a critical mindset. Further, in spite of the fact that most participating students were found to have lack of understanding of critical thinking and digital culture towards digital\_literacy, they appeared to possess the competencies of finding information, communication, and functional skills. Additionally, quantitative result of the pre-service teachers' competences demonstrated that communication dimension was the highest of all with the mean value of 3.95, followed by online\_safety skills 3.87, finding information 3.79, critical thinking 3.77, functional skills 3.75, as well as collaboration and creativity 3.43. The lowest mean 3.40 belonged to digital culture dimension. The findings have important implications for developing digital\_literacy framework in an EFL academic writing.

\*\*\*\* \*Abstract\_71

Datified societies need informed public debate about the implications of data science technologies. At present, internet users are often unaware of the potential consequences of disclosing personal data online and few citizens have the knowledge to participate in such debates. This paper argues that critical big data literacy efforts are one way to address this lack of knowledge. It draws on findings from a small qualitative investigation and discusses the effectiveness of online critical big data literacy tools. Through pre and post use testing, the short- and longer-term influence of these tools on people's privacy attitudes and behaviour was investigated. The study's findings suggested that the tools tested had a predominantly positive initial effect, leading to improved critical big data literacy among most participants, which resulted in more privacy-sensitive attitudes and internet usage. When analyzing the tools' longer-term influence, results were more mixed, with evidence suggesting for some that literacy effects of the tools were short-lived, while for others they led to more persistent and growing literacy. The findings confirm previous research noting the complexity of privacy attitudes and also find that resignation toward privacy is multi-faceted. Overall, this study reaffirms the importance of critical big data literacy and produces new findings about the value of interactive data literacy tools. These tools have been under-researched to date. This research shows that these

tools could provide a relevant means to work toward empowering internet users, promoting a critical internet usage and, ideally, enabling more citizens to engage in public debates about changing data systems.

\*\*\*\* \*Abstract\_72

This study aimed to compare the self-perception of digital skills across genders among secondary school students in Peru, to identify potential disparities and advocate for equity-promoting strategies. A structured survey was administered to evaluate operational and formality skills, as well as those related to digital content, among a representative sample of students from both genders using a convenience non-probabilistic sampling method. Females reported higher competence in most digital skills, notably in areas such as online\_safety and technical problem solving, whereas males demonstrated similar or superior competence in basic navigation and educational technology skills. The implementation of inclusive technological literacy workshops, integration of collaborative research projects and information sharing, and encouragement of male engagement in digital content creation are recommended. These should be supported by equitable access to technological resources, to enhance the confidence and digital competence of both genders in Peruvian classrooms.

\*\*\*\* \*Abstract\_73

Online\_privacy pertains to an individual's capacity to regulate and oversee the gathering and distribution of online information. Conversely, online\_privacy concern OPC pertains to the protection of personal information, along with the worries or convictions concerning potential risks and unfavorable outcomes associated with its collection, utilization and distribution. With a holistic approach to these relationships, this study aims to model the relationships between digital\_literacy DL, digital data security awareness DDSA and OPC and how these relationships vary by gender. Design methodology approach: The participants of this study are 2,835 university students. Data collection tools in the study consist of personal information form and three different scales. Partial least squares PLS, structural equation modeling SEM and multi-group analysis MGA were used to test the framework determined in the context of the research purpose and to validate the proposed hypotheses. Findings: DL has a direct and positive effect on digital data security awareness DDSA, and DDSA has a positive effect on OPC. According to the MGA results, the hypothesis put forward in both male and female sub-samples was supported. The effect of DDSA on OPC is higher for males. Originality value This study highlights the positive role of DL and perception of data security on OPC. In addition, MGA findings by gender reveal some differences between men and women.

\*\*\*\* \*Abstract\_74

In this article we present the level of knowledge and literacy held by the parents of primary school students regarding internet safety online\_safety, digital safety in the context of digital\_literacy DL in terms of both technical skills and knowledge. The study reported on here was conducted in Poland, and was commissioned by the Ministry of National Education. The research involved measuring the knowledge and skills regarding the prevention of electronic threats ethreats which are defined as problematic situations and behaviour mediated by digital media and the internet. Ethreats are related to mental and physical health, social aspects and technical matters related to the use of information and communication technologies ICTs. In order to narrow down the research area, 6 components related to ethreats were selected, namely the ergonomics of using digital media; the evaluation of the reliability of online information; the influence of advertising on consumers' choices; risky online relationships; understanding the mechanisms of secure logging-in; and protection against malware. The DL level was measured using a competence test. An analysis of 514 tests revealed that the most neglected areas were the protection of children against unwanted communication with other users, and secure logging in. The strongest component was the ergonomics of using ICT. We also noted that more than one fifth of parents showed a satisfactory level of DL related to online\_safety. Another observation was that DL is a complex and heterogeneous concept. The DL components are related with one another to different extents. Some DL elements are determined by the level of education, place of living, subjective sense of own wellbeing or intuitive perception self evaluation.

\*\*\*\* \*Abstract\_75

Children spend increasing amounts of time online prompting parents and carers, educators, school systems, and governments to raise concerns about their online\_safety. In a world first, Australia's eSafety Commissioner eSafety was charged with developing a national framework for online\_safety education. The Framework was developed in a two-stage sequential mixed-methods study involving collaboration between researchers, eSafety, experts and stakeholders. Stage 1, a rapid review of eight evidence sources provided the foundation for a multi-component Framework addressing key elements and effective practices for online\_safety education. Stage 2, tested and refined the Framework via individual interviews with online\_safety experts, and focus groups with stakeholders representing school-sector organisations and children's advocacy groups. The final Framework comprises 5 elements and 22 effective practices. The Framework will support schools in teaching online\_safety, assessing the quality of programs and approaches, and guiding best practice.

\*\*\*\* \*Abstract\_76

Social networks are colonised by a culture of confession that turns teenager privacy into a commodity to achieve recognition and social acceptance. This display accelerates the porosity of the boundaries between the public and the private and feeds surveillance capitalism. The aim of this systematic review is to examine the empirical evidence on the public-private interaction of teenagers' contributions to social networks in the last 5 years in databases: Eric, Scopus and Web of Science. Based on the Prisma Statement, the initial search produced 1449 documents, of which 81 were included in the final analysis after the application of exclusion and inclusion criteria and the purging of duplicates. The results show a field of study developed with a decreasing trend in production in recent years, knowledge gaps and discordant findings. It is concluded the need to build solid knowledge and initiate new lines in the study of the issue in order to understand the exhibition of teenagers in social networks. It is points out the urgency of a training based on their own media practices and in digital\_literacy for a broad understanding of online\_privacy.

\*\*\*\* \*Abstract\_77

Digital health is increasingly being utilized in clinical practice given its ease of accessibility, but it lacks emphasis from universities and accreditation bodies. This study attempted to better understand the digital capabilities of optometry students. Background With technological advancements transforming the Australian workforce and healthcare, there is a growing demand for digitally competent graduates. This study investigated digital perceptions and preferences of optometry students relating to their studies and readiness for work in healthcare. Methodology Current optometry students participated in an anonymous online survey. Questions were designed to evaluate their understanding and awareness of digital skills and competencies for learning whilst at university, and for use in the health sector workforce. Results were analyzed to underscore key trends and answers to open-ended questions underwent inductive thematic analysis to generate themes for discussion. Contribution Optometry educators can bridge the gap in digital practices between students and the workplace by obtaining a baseline of their capabilities and incorporating specific activities within the curriculum to increase student awareness and support their understanding and development in this aspect. Findings Most students were confident in using daily technologies for learning. Reference management software was perceived to be most important and useful skill to attain. While students were less confident in creating applications, they were keen to learn even though it seemed peripheral to their career and professional development. 70% of the students knew how to manage their online\_privacy and online\_security. Of the students, 92% highlighted that attaining competency in digital skills would enhance their career and professional development, but only 54% believed they possessed the relevant skills for entering the workforce. Only 19% of the students reported having sufficient university support. Recommendations Digital capabilities of learners do need to be taught explicitly and should for Practitioners not be assumed. To improve student learning outcomes, digital skills and competencies need to be embedded throughout the curriculum and addressed through learning objectives. Recommendations More work needs to be done in implementing digital training and services at for Researchers a subject, course, and institutional level. Some international benchmarking of optometry curricula and optometry research would clarify the need for digital education, to educators and students alike. Impact on Society Currently, there is a lack of recognition of digital health

by accrediting bodies, thus preventing digital competency from being a priority in the curriculum of schools. There is a further need to establish dialogue between universities, employers, and accrediting bodies to set consistent and realistic expectations of digital skills and competencies. Future Research Future studies should consider having larger sample sizes to observe similarities and differences in digital capabilities between year levels. Student focus groups and interviews can be performed to better understand the rationale behind the desire and interest to learn digital technologies that seemed irrelevant to optometry.

\*\*\*\* \*Abstract\_78

Digital\_literacy is a crucial skill set in the contemporary era, encompassing technical proficiency, information\_literacy and media literacy, data literacy, and more. There are further disciplines that are incorporated into the broad concept of digital\_literacy, including cybersecurity, online\_safety, and responsible communication. The importance of critical thinking in digital contexts and the emerging field of digital wellbeing are addressed. There are challenges in achieving digital\_literacy including the lack of common frameworks and diverse barriers such as access to technology, affordability, and cultural differences. Ultimately digital\_literacy is something that requires the input of various stakeholders, including educators, governments, technology providers, and community organisations. There is a clear need for a collaborative, multi-pronged approach to address these challenges and the need for common agreement on what digital\_literacy is.

\*\*\*\* \*Abstract\_79

The rapid expansion of digital connectivity has provided youth with near universal access to digital platforms for communication, entertainment, and education. This unprecedented access to digital devices continues to raise concerns about online\_safety, data\_privacy, and cybersecurity. The critical factor influencing the ability of youth to navigate digital platforms responsibly is digital\_literacy. While some regions across the world have implemented digital\_literacy programs, inequities and disparities remain in not only overall digital\_literacy levels, but also evaluation of digital\_literacy. To address these challenges, an environmental scan was conducted to identify existing digital\_literacy programs in Canada developed specifically for youth, as well as digital\_literacy assessment tools. The literature search encompassed peer-reviewed articles, organizational curricula, and assessment measures indexed in various databases. Data was synthesized from identified programs and assessment tools to inform the development of a new digital\_literacy program, and an assessment tool tailored for youth. The environmental scan identified 15 digital\_literacy programs targeting various components such as data safety, cyberbullying, and digital media. Based on the findings, a new program was developed focusing on four key components: 1 digital fluency, 2 digital privacy and safety, 3 ethics and empathy, and 4 consumer awareness. Additionally, 12 assessment tools were identified for digital\_literacy focusing on evaluating several aspects, including searching and processing digital information and digital safety, which informed the development of an assessment tool to complement the new program. Tailored digital\_literacy programs and assessments are crucial for understanding and addressing digital\_literacy among youth globally. This program's adaptability allows for customization to various target audiences, including culturally diverse and geographically remote communities, to enhance digital\_literacy across settings. Implementing digital\_literacy programs can better prepare youth for an increasingly digital world, while minimizing potential risks associated with technology use.

\*\*\*\* \*Abstract\_80

The rapid evolution of digital technology has brought both opportunities and risks, particularly for adolescents navigating the online world. This paper delves into the significance of preventive online\_safety education tailored for teenagers. It explores the current landscape of online threats, encompassing cyberbullying, privacy breaches, and exposure to inappropriate content, among others. Additionally, it evaluates existing educational approaches, emphasizing the need for a proactive, multifaceted strategy to equip teenagers with the necessary skills and knowledge to safely navigate the digital sphere. The proposed preventive education model integrates elements of digital\_literacy, critical thinking, and responsible online behaviour. Furthermore, it discusses potential challenges in implementing such programs and suggests collaborative efforts among educators, parents, and poli-

cymakers to ensure comprehensive online\_safety education for teenagers, fostering a safer and more secure digital environment for the next generation.

\*\*\*\* \*Abstract\_81

In the contemporary digital era, the pervasive influence of the internet underscores the imperative to equip the youth with skills for secure online navigation. While the internet presents vast opportunities, it simultaneously exposes young learners to potential risks, encompassing cyberbullying, privacy breaches, and security threats. This research meticulously examines the impact of cybersecurity education on the digital\_literacy and online\_safety of students, emphasizing the youth in Badakhshan Province, Afghanistan. It advocates for the cultivation of digital\_literacy and online\_safety principles across diverse age groups and fields of study. Furthermore, the study underscores the paramount importance of instilling awareness regarding responsible digital practices related to privacy, security, and copyright, with a compelling call for active parental involvement. To execute this research, a robust stratified random sampling technique was deployed, meticulously selecting 170 male and female students from various grade levels in both public and private schools within Badakhshan province, Afghanistan. Data collection was facilitated through a comprehensive survey questionnaire featuring 16 Likert scale-based questions. Subsequently, the gathered data underwent rigorous statistical analysis, encompassing descriptive and inferential statistics, regression analysis, and qualitative content analysis. This research yields invaluable insights into the internet behaviour and cybersecurity awareness of the youth in Badakhshan Province, Afghanistan. It makes essential contributions to comprehending their online activities and digital\_literacy. The overarching goal is to empower students to navigate the digital landscape with confidence and ethical discernment by integrating cybersecurity education into school curricula. This approach not only safeguards their privacy and security but also optimizes the internet's full potential. The study significantly contributes to fostering a safer, more responsible, and knowledge-driven society.

\*\*\*\* \*Abstract\_82

Nowadays, digital\_literacy is often considered as a compulsory competence for young people. The advancement in information technology has impacted societal lives in positive ways. However, this technology falls under suspicion for exerting negative influences in child development. In order to navigate the internet safely, young people need a particular skill. This community service program focused on assisting students to develop their digital\_literacy skills. The program took place between June to October 2021 in Muallimat Muhammadiyah Yogyakarta, that provides secondary education for female students. The program was conducted in three 3 stages, i.e. focus group discussion with students and teachers, webinar for students, and a collaborative project which resulted in three 3 different posters addressing internet-related problems. Before COVID\_19, this school is considered relatively unique because students live in dormitory. In addition, the school also imposes ban of personal mobile phone. Since the pandemic hit, students returned to their home and school activities were conducted online. Such changes pose a number of challenges for students, particularly in terms of time management, cyberbullying, and online\_privacy. Through this program, students were able to work together to reflect on their internet use and develop a safer way to navigate the internet.

\*\*\*\* \*Abstract\_83

Digital Empowerment Foundation DEF has been making use of many innovative methods and technologies to democratize innovation, upskill, build resilience and foster lifelong learning in rural India with a special focus on marginalized communities. We would like to showcase some of our innovations here. START A digital learning and Media & Information Literacy MIL toolkit, designed exclusively for first-generation technology users to promote digital inclusion and fight information poverty. It is a 45-hour digital learning curriculum that covers 30 topics ranging from basics of computers, use of applications, MIL and online\_security and online\_safety, among others. The pedagogy for START focuses on hands-on training and workshops in rural and tribal communities through activities and gamification of topics. GOAL Going Online as Leaders A program to connect urban volunteers with rural women online to provide them guidance and support in digital skills to bridge the information gap. This technology-enabled mentorship program was adopted by the Ministry of Tribal Affairs, Government of India and is now being replicated in several states. The data comparing baseline and

endline show that beneficiaries of GOAL show higher interest in pursuing higher education, greater self-confidence, improved communication skills and aspiration to become changemakers. // Digital Sarthak: This program demonstrates how digital\_literacy through the community network model can be an important strategy to achieve a replicable model of local economic development. 100 rural women were trained to further train 500 women-led Community Development Organizations CDOs and 10000 rural women entrepreneurs in the first stage. The program placed women in active roles in the information ecosystem that further improved their confidence and capacity. SkillBot: A self-learning chatbot built on the free and open-source Telegram platform. Telegram provides free backend technical support and chatbot feature. SkillBot was developed by DEF and Commonwealth of Learning to teach digital\_literacy, financial literacy, citizen services and data management to rural youth and artisans. SkillBot is multilingual and employs tutorial lessons, audio graphics, infographics, flashcards, interactive quizzes and activities for teaching. Skill Bot thus provides an accessible, easy to understand platform for skilling. Maker's Space is an initiative where physical centres equipped with STEM learning and digital skilling tools are created in DEF's community information centres at the remotest locations. Maker's Space facilitates an unstructured learning space supported by digital/STEM tools that allow children and youth, especially persons with disabilities, to take ownership of their learning and create innovative solutions for their communities.

# ANEXO A



University of  
Sheffield

Human  
Resources

## **STRICTLY PERSONAL**

Dr Ariadne Chloe Mary Furnival  
Information School

21 March 2024

Enquiries: Rosie Wainwright  
Personnel number: 10088839  
Faculty of Social Sciences

Director of Human Resources  
Ian Wright, FCIPD

Human Resources  
University of Sheffield  
The Arts Tower  
Western Bank  
Sheffield S10 2TN

**Telephone:** +44 (0) 114 222 1613

**Email:** [hrhub@sheffield.ac.uk](mailto:hrhub@sheffield.ac.uk)

Dear Dr Furnival,

I am delighted to inform you that the title of Visiting Researcher has been conferred on you from 21 March 2024 to 31 July 2024, linked to the Information School at the University of Sheffield.

You are invited to use their facilities to conduct your own personal research and to meet with other academics to exchange ideas and research findings. This visit does not carry any remuneration from this University.

Should you have any queries arising from this letter please do not hesitate to contact me at the email address above.

I do hope that your association with the University will prove enjoyable and mutually beneficial.

Yours sincerely,

A handwritten signature in black ink that reads 'R. Wainwright'.

pp. Lorraine Sweeney  
Faculty HR Manager



# ANEXO B



MINISTÉRIO DA EDUCAÇÃO  
UNIVERSIDADE FEDERAL DE SÃO CARLOS  
SECRETARIA GERAL DE EDUCAÇÃO A DISTÂNCIA

## CERTIFICADO

Certificamos que **Ariadne Chloe Mary Furnival** concluiu o curso **Revisão Bibliográfica Sistemática**, oferecido pela Secretaria Geral de Educação a Distância da Universidade Federal de São Carlos, num total de 12 horas, no período de 11 de julho de 2023 a 23 de outubro de 2023.

São Carlos, 23 de outubro de 2023

**Profª Drª Cleonice Maria Tomazzetti**  
Secretária Geral de Educação a Distância  
SEaD-UFSCar



UNIVERSIDADE FEDERAL DE SÃO CARLOS  
SECRETARIA GERAL DE EDUCAÇÃO A DISTÂNCIA

**Curso: Revisão Bibliográfica Sistemática**

**Ariadne Chloe Mary Furnival**

**Nota: 10,00**

- Unidade 1. Metanálise
- Unidade 2. Questões de pesquisa
- Unidade 3. Bases de dados
- Unidade 4. Acesso às bases de dados
- Unidade 5. Strings de busca
- Unidade 6. Critérios de inclusão e exclusão
- Unidade 7. Exportação de metadados
- Unidade 8. Introdução ao StArt
- Unidade 9. Importação de metadados
- Unidade 10. Selecionando os artigos
- Unidade 11. Extração e apresentação dos dados
- Unidade 12. Redação de artigo (RBS)
- Unidade 13. Introdução à Bibliometria
- Unidade 14. VOSviewer



6536e0de-d74c-4908-a336-42b4ac1e01c5



Portal de Cursos Abertos da UFSCar - PoCA  
Processo: 23112.002203/2018-14

