
Privacy literacy: uma análise da literatura científica em Ciência da Informação no período pré-COVID-19

Alfabetización en privacidad: un análisis de la literatura científica en ciencias de la información en el periodo pre-COVID-19

Privacy literacy: an analysis of the scientific literature in Information Science in the pre-COVID-19 period

José Augusto BAGATINI, José Augusto Chaves GUIMARÃES

Universidade Estadual Paulista - UNESP, Depto de Ciência da Informação, Av. Higino Muzzi Filho, 737, Marília, SP, 17525-900, Brasil; jose.bagatini@unesp.br, chaves.guimaraes@marilia.unesp.br

Resumen

Como resultado de su inclusión en la economía digital, los individuos se ven incentivados a utilizar soluciones informáticas conectadas a Internet para realizar actividades cotidianas, lo que resulta en la creación de un extenso y detallado rastro de datos sobre sí mismos. Para hacer frente a este problema, la alfabetización en privacidad se destaca como una herramienta que debe ponerse a disposición de la sociedad para promover el desarrollo de habilidades que puedan subsidiar acciones individuales y colectivas para preservar derechos como la privacidad, la protección de datos, el derecho a ser olvidado y la autodeterminación informativa. De esta forma, analizamos cómo el tema de la alfabetización en privacidad ha sido abordado en la literatura internacional de ciencias de la información, a través de la exploración de publicaciones indexadas en las bases de datos Scopus, Web of Science y LISA, resultando en un corpus de 23 artículos diferentes. Metodológicamente, se aplicó el análisis de dominio en los enfoques epistemológico y bibliométrico. De esta manera, fue posible ofrecer una visión histórico-conceptual del fenómeno de la alfabetización en privacidad y su configuración como mecanismo de resistencia. En cuanto a la configuración de la literatura analizada, se observó una dispersión de autores, países e instituciones, lo que indica que se trata de un tema nuevo que aún se encuentra en proceso de consolidación científica. Desde el punto de vista temático, se destaca la preocupación de los estudios con los grupos supuestamente más vulnerables, destacando el papel social de la alfabetización en la privacidad.

Palabras clave: Privacidad. Alfabetización en privacidad. Protección de datos. Datos personales.

1. Introdução

A presente pesquisa, integra-se em um projeto maior denominado “O Letramento em privacidade na literatura da Ciência da Informação e a pandemia da covid-19: antes, durante e depois”, que parte do pressuposto que o advento da pandemia de Covid-19 trouxe significativos impactos

Abstract

As a result of their inclusion in the digital economy, individuals are encouraged to use computerized solutions connected to the Internet to carry out everyday activities, resulting in the creation of an extensive and detailed data trail about themselves. To address this problem, privacy literacy stands out as a tool to be made available to society to promote the development of skills that can subsidize individual and collective actions to preserve rights such as privacy, data protection, the right to be forgotten, and informational self-determination. In this way, we analysed how the topic of privacy literacy has been addressed in the international information science literature by examining publications indexed in the Scopus, Web of Science, and LISA databases, resulting in a corpus of 23 different articles. Methodologically, domain analysis was applied in epistemological and bibliometric approaches. In this way, it was possible to provide a historical-conceptual overview of the phenomenon of privacy literacy and its configuration as a resistance mechanism. As far as the configuration of the literature analysed is concerned, there was a dispersion of authors, countries and institutions, which indicates that this is a new topic that is still in the process of scientific consolidation. From a thematic point of view, the concern of the studies with supposedly more vulnerable groups stands out, highlighting the social role of literacy in privacy.

Keywords: Privacy. Privacy literacy. Data protection. Personal data.

em como a população global, por encontrar-se então em grande parte reclusa, passou a interagir de maneira mais efetiva com as tecnologias da informação (TIC). A isso se alia o fato de a pandemia de Covid-19 ter sido o primeiro grande advento global dessa categoria a ocorrer em um contexto de hiperconectividade, o que

possibilitou o emprego de uma série de técnicas e tecnologias de vigilância digital nos esforços globais de rastrear o comportamento do vírus (Poetranto & Ruan, 2021). Isso acarretou uma intensificação das preocupações com a proteção dos direitos relacionados à privacidade durante o referido período.

Dessa forma, este trabalho apresenta resultados da primeira etapa da pesquisa relativa ao comportamento da literatura internacional de Ciência da Informação na temática do letramento em privacidade no período pré-covid para, na segunda etapa, ora em desenvolvimento, comparar os resultados com o período da covid e, na terceira etapa, o período pós-covid.

Cabe, portanto, destacar a rápida disseminação da internet, sua ascensão a posto de tecnologia global e os impactos decorrentes no campo da privacidade.

Atualmente, a internet ocupa posto de ferramenta indispensável no desenvolvimento de atividades em todas as áreas humanas e seu crescimento tem sido contínuo desde os anos de 1990. Em 1996 já contava com mais de vinte milhões de usuários; no ano 2000, já eram mais de trezentos milhões (Castells, 2009); em 2019, cerca de 57 % da população global possuía acesso à internet, o que representava quatro bilhões e quatrocentos milhões de pessoas (Hootsuite & We Are Social, 2019).

A pandemia de COVID-19, que teve seu início decretado em 2020 e fim em 2023 (Naciones Unidas, 2023; Organización Panamericana de Salud, 2020), foi responsável por acelerar mais ainda a digitalização de economias e sociedades evidenciando, assim, questões de conectividade e serviços digitais, principalmente em um contexto de grande assimetria de acesso à Internet e serviços digitais entre nações (World Economic Forum, 2021). Em busca de amenizar tal disparidade, em 2021, durante o Fórum Econômico Mundial, foi lançada a proposta da The EDISON Alliance, que tem como visão: toda pessoa pode participar da economia digital de maneira acessível, sendo sua missão mobilizar um movimento global e intersetorial para o desenvolvimento de ações que buscam resultados sociais e econômicos por meio da conectividade e aperfeiçoamento de investimentos digitais; e sua abordagem sendo a de construir uma “rede de redes” para identificar e escalar relacionamentos intersetoriais para impulsionar mudanças e gerar impacto (World Economic Forum, 2021). Em suma, segundo seu próprio manifesto, a Aliança EDISON tem por objetivo, através da participação de diversos setores da economia, acelerar a expansão da infraestrutura digital e a implantação da

banda larga visando a recuperação da economia e redução das desigualdades (World Economic Forum, 2021).

A iniciativa proposta pela Aliança EDISON alinhava-se em objetivos, no momento de sua proposição, com diversas outras iniciativas que já se encontravam em curso, demonstrando assim, que a segunda década do século XXI foi marcado por uma acirrada disputa pelo controle do mercado de acesso à internet, resultando em uma verdadeira corrida para definir quem controlaria o acesso de bilhões de novos participantes da economia digital.

Destaca-se entre as propostas que se encontravam em curso o Projeto Aquila, lançado em 2014 pelo Facebook, atualmente META (Meta, 2021), que financiou o desenvolvimento de drones que levariam internet às áreas remotas do planeta, entretanto, por motivos técnicos foi encerrado em 2018. No mesmo ano, a empresa anunciou que lançaria satélites com o mesmo objetivo, o projeto foi denominado Athena, já não se encontra em vigor; a divisão responsável pelo projeto foi vendida para a Amazon (Dent, 2021). No ano de 2020, o Facebook anunciou e disponibilizou o aplicativo para smartphones Discover, que fornece conexão gratuita em parceria com empresas de telefonia locais (Meta, 2021). Todos os projetos descritos são vinculados a iniciativa *Free Basics*, promovida pelo Facebook com objetivo de oferecer acesso a serviços básicos online sem custo (Meta, 2024).

Cumprir destacar também que, ao longo dos últimos anos, a iniciativa com maior sucesso comercial se deu pelas mãos da companhia Starlink que, valendo-se de satélites, busca alcançar a “conectividade global completa”. Em 2021 a empresa já contava com 1.369 satélites. Segundo a empresa, seu objetivo seria alcançado com cerca de 1.700 satélites ativos, atualmente sua rede é composta por mais de 5.000 satélites (Correia, 2023).

A vista do exposto, nota-se que a expansão da internet continuará sendo acelerada e com o objetivo final de integrar totalmente a humanidade na economia digital.

O avanço em direção à uma realidade de hiperconectividade, sem levar em conta a educação e a distribuição de ferramentas que previnam contra os prejuízos à privacidade, a proteção de dados e de ser esquecido dos usuários da internet pode acarretar o aprofundamento das desigualdades já impostas, além de trazer consigo novas maneiras de discriminação, sobretudo a grupos sociais já marginalizados.

A falta de preparo do usuário para lidar com essas novas problemáticas é demonstrada no documento National Privacy Test Report produzido pela empresa NordVPN, pesquisa essa que tem por objetivo mostrar como as pessoas em diferentes países entendem e seguem as diretrizes de segurança cibernética, avaliando os hábitos digitais, a consciência sobre privacidade digital e sua tolerância à riscos (NordVPN, 2021).

Com sua inserção na economia digital, um grupo ou indivíduo é estimulado a adotar soluções informatizadas e conectadas à internet para a execução de atividades cotidianas, resultando assim, na produção de um rastro de dados extenso e detalhado, o qual não é devidamente gerenciado porque esse grupo ou indivíduo não dispõe de ferramentas e habilidades que promovam a proteção de sua privacidade e dados (1).

Nesse contexto, os dados pessoais assumem um potencial danoso elevado, já que podem ser utilizados de diversas maneiras para influenciar as mais diversas áreas da vida da população uma vez que, nessa dinâmica, são acumulados indiscriminadamente, ou seja, conjuntos enormes se formam, uma vez que não é respeitado o conceito de temporalidade, promovendo assim, uma distorção no ciclo de vida que deveria ser imposta a esse tipo de dados (Bagatini & Guimarães, 2021). Por si só, a coleta, uso e armazenamento de dados pessoais já se mostra como um problema a ser combatido, todavia, soma-se a isso, o fato de que esses dados podem vir a ser publicizados por meio de ações não previstas.

Ao analisar 39 vazamentos de dados ocorridos entre os anos de 2009 e 2017, Bagatini (2019) identificou que 48% da amostragem ocorreu a partir de ataques maliciosos com intenção criminosa, 25% a partir de falhas de sistema e 27% dos vazamentos foram resultados de erro humano, mais de um quarto do total. Nos vazamentos analisados, nota-se que os principais dados vazados são endereço de e-mail, senhas, telefones, nomes, endereços, identificador social (CPF, N.I.E etc.), número de cartões de crédito e débito e fotografias. Conforme os conjuntos de dados pessoais de empresas e governos crescem, maiores são os números de afetados quando ocorrem vazamentos de dados. Segundo a base de dados *World's Biggest Data Breaches & Hacks*, organizada e publicada pela fundação Information is Beautiful (2021), os vazamentos de dados evoluíram como mostra a Figura 1.

A partir do gráfico apresentado, é possível notar que existe uma tendência de crescimento das ocorrências de vazamentos de dados, assim como o volume de dados nessas ocorrências. Embora não haja umnexo causal efetivo entre

ambas as situações, há de se considerar que o fato de os vazamentos estarem se tornando cada vez maiores em volume traz consequências. Já no que diz respeito a acentuada queda demonstrada no ano de 2020, pode decorrer do fato de que, recorrentemente, vazamentos de dados não são identificados imediatamente, podendo levar anos para se tornar de conhecimento público.

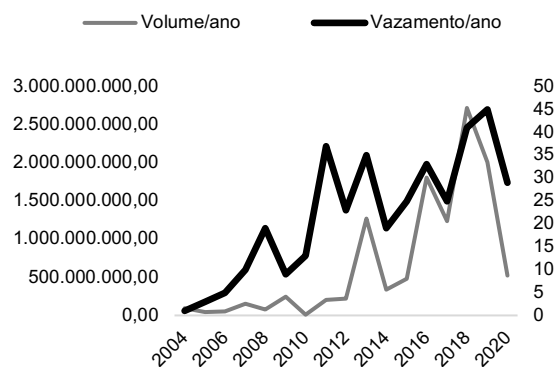


Figura 1. Casos e volume de dados vazados até 2020

Os conjuntos de dados pessoais de vítimas de vazamentos podem ser utilizados para diversos fins de natureza criminosa ou fraudulenta, tais como extorsão e fraude eletrônica (Bagatini, 2019).

A preocupação da sociedade civil enquanto a proteção de dados, transparece na quantidade de novas leis sobre a temática que vem sendo desenvolvidas e implementadas ao longo dos últimos anos acerca do tema. Dos 194 países listados pela *United Nations Conference on Trade and Development* (UNCTAD), em 2020, 66% já contavam com legislações que contemplam a proteção de dados pessoais, 10% se encontravam em processo de desenvolvimento de frameworks jurídicos acerca do tema, 19% dos países não possuíam legislação e nenhum projeto em trâmite, e por fim, 5% dos 194 países, não possuíam dados disponíveis sobre o tema (UNCTAD, 2020).

Das legislações que abordam o tema de proteção de dados, a General Data Protection Regulation (GDPR) é a mais proeminente. Aprovada em maio de 2016 e entrando em vigor em maio de 2018, revogou a Diretiva de Proteção de Dados pessoais de 1995 da União Europeia. A GDPR versa sobre privacidade e proteção de dados pessoais e aplica-se a todos os indivíduos na União Europeia (EU) e no Espaço Econômico Europeu (EEE), além de regulamentar também a exportação de dados para fora da EU e do EEE. Por suas características modernas, tornou-se um modelo a ser seguido por outros países. A GDPR

(European Union, 2016) define os dados pessoais como sendo:

[...] informação relativa a uma pessoa singular identificada ou identificável. [...] É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, um nome, um número de identificação, dados de localização [...] ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Entretanto, mesmo com leis que buscam regulamentar o processamento de dados pessoais, incidentes continuam a ocorrer e causam danos, sobretudo à população. Isso decorre do fato de que a dinâmica baseada em uso de dados pessoais é por si só danosa e deve ser combatida em favor da preservação da privacidade. Desse modo, o letramento em privacidade constitui uma ferramenta altamente relevante – e necessária – a ser disponibilizada à sociedade promovendo, assim, o desenvolvimento de habilidades que possam subsidiar ações individuais e coletivas que buscam a preservação de direitos fundamentais, caracterizando-se como um mecanismo de resistência.

A crescente noção de que existe a necessidade de promover o letramento em privacidade traduz-se, especialmente, na versão 2.2 do documento *The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes* (DigComp 2.2), que trata a temática da proteção de dados pessoais e privacidade, oferecendo orientações que visam o desenvolvimento de competências. A versão já citada do referido documento apresenta em seu conteúdo uma atualização dos “exemplos de conhecimentos, capacidades e atitudes aplicáveis a cada competência” (Dimensão 4). Estes novos exemplos ilustram áreas relevantes, com o objetivo de apoiar os cidadãos a usarem tecnologias digitais comumente utilizadas no dia a dia de forma confiante, crítica e segura, mas também tecnologias novas e emergentes (Vuorikari et al., 2022).

Destaca-se em seu conteúdo, as sugestões de conhecimento, capacidades e atitudes relativas à proteção de dados pessoais e privacidade que, segundo o DigComp 2.2, podem ser adquiridas (Tabela I). O letramento digital insere-se no amplo espectro do letramento informacional ou *information literacy*, termo cunhado por Zurkowski (1974, p.61) para representar a habilidade de uma pessoa solucionar seus problemas informacionais por meio da utilização de fontes relevantes de informação. Isso envolve um processo que compreende o reconhecimento de uma necessidade informacional e a busca, localização,

avaliação e uso de uma informação com vistas à geração de conhecimento. Desse modo, localiza-se uma informação e interage-se criticamente com ela para que seja possível transformá-la, comunicá-la e aplicá-la.

Conhecimento

Ciente de que a identificação eletrônica protegida é uma característica chave concebida para permitir uma partilha mais segura de dados pessoais com terceiros ao realizar transações do sector público e privado;

Sabe que a “política de privacidade” de uma aplicação ou serviço deve explicar quais os dados pessoais que recolhe (por exemplo, nome, marca do dispositivo, geolocalização do utilizador) e se os dados são partilhados com terceiros.

Sabe que o processamento de dados pessoais está sujeito a regulamentos locais, tais como o regulamento General Data Protection (GDPR) da União Europeia (EU) (por exemplo, as interações de voz com um assistente virtual são dados pessoais em termos da GDPR e podem expor os utilizadores a determinados riscos de proteção de dados, privacidade e segurança.

Capacidades

Sabe identificar mensagens de e-mail suspeitas que tentam obter informações sensíveis (por exemplo, dados pessoais, identificação bancária) ou que podem conter malware. Sabe que estas mensagens de correio eletrónico são frequentemente concebidas para enganar pessoas que não conferem com atenção e que são assim mais suscetíveis à fraude, ao conterem erros deliberados que impedem as pessoas mais atentas de clicar nelas.

Sabe como aplicar medidas básicas de segurança nos pagamentos online (por exemplo, nunca enviar uma digitalização de cartões de crédito ou dar o código PIN de um cartão de débito ou de crédito).

Sabe como utilizar a identificação eletrónica para serviços prestados pelas autoridades públicas ou serviços públicos (por exemplo, preencher o seu formulário fiscal, requerer benefícios sociais, solicitar certificados) e pelo setor empresarial, tais como bancos e serviços de transporte.

Sabe como utilizar certificados digitais fornecidos por autoridades certificadoras (por exemplo, certificados digitais para autenticação e assinatura digital armazenados em cartões de identidade nacionais).

Atitudes

Pondera os benefícios e riscos antes de permitir que terceiros processem dados pessoais (por exemplo, reconhece que um assistente de voz num smartphone, que é utilizado para dar comandos a um aspirador robô, poderia dar a terceiros - empresas, governos, cybercriminosos - acesso a dados). (IA)

Confiante na realização de transações online após tomar as medidas de segurança e proteção adequadas.

Tabela I. Conhecimentos, capacidades e atitudes

Nesse âmbito inserem-se, como destaca Marzal (2020), a *Media literacy*, a *Digital literacy*, a *Cyberliteracy*, a *Visual literacy*, a *Mobile literacy*, a *Critical information literacy*, a *academic literacy* e a *digital literacy*, ou letramento digital, que consiste na capacidade de utilizar-se da tecnologia

digital de modo proficiente, aspecto que inclui habilidades de leitura, de construção de conhecimento de forma hipertextual, de avaliar a qualidade da informação e de compreender as regras inerentes ao ciberespaço (Eshet-Alkalai & Amichai-Hamburger, 2004).

A isso se alia o letramento em privacidade que, embora caminhando lado-a-lado com o letramento digital em diversas situações, não pode ser com aquele confundido uma vez que ambos possuem características bem definidas. Christina Wissinger (2017, p. 379) afirma que, de acordo com a *American Library Association's Digital Literacy Task Force*, o letramento digital é:

“[...] a capacidade de usar tecnologias de informação e comunicação para encontrar, avaliar, criar e comunicar informações, exigindo habilidades cognitivas e técnicas.

Em contrapartida, a autora afirma que as definições para letramento em privacidade possuem enfoque na compreensão das responsabilidades e riscos associados ao compartilhamento de informações online (Wissinger, 2017). Langenderfer e Miyazaki (2009) propõem seguinte definição para letramento em privacidade sendo a compreensão que os consumidores têm do cenário de informações com o qual interagem e de suas responsabilidades dentro desse cenário. Givens (2015) apresenta também uma definição, para *privacy literacy*: nível de compreensão e consciência de como as informações são rastreadas e usadas em ambientes online e como essas informações podem reter ou perder sua natureza privada”.

Já na visão de Bartsch e Dienlin (2016), mesmo o letramento em privacidade sendo um conceito relativamente novo, já se consolida como o:

[...] conhecimento dos usuários sobre aspectos técnicos da proteção de dados online e sobre leis e diretrizes, bem como práticas institucionais e também sobre a capacidade dos usuários de aplicar estratégias para a regulamentação da privacidade individual e proteção de dados.

É a partir do letramento em privacidade que um indivíduo adquire a capacidade de usar as informações sobre como seus dados pessoais serão armazenados, usados ou distribuídos; combinando isso com sua filosofia pessoal sobre quais informações devem ser públicas e privadas, para tomar decisões conscientes acerca do tema (Wissinger, 2017).

Já no que diz respeito a estrutura do letramento em privacidade, Rotman (2009) afirma que deve abordar cinco áreas principais: a compreensão, que abrange como as informações pessoais são usadas online, o reconhecimento distingue os vários lugares em que as informações pessoais

podem ser compartilhadas online, a percepção se concentra nas consequências do compartilhamento de informações pessoais online, a avaliação aborda os riscos e benefícios do compartilhamento de informações; e por último, a decisão se concentra em quando compartilhar essas informações online.

Atualmente as pessoas podem estar mais vulneráveis do que deveriam, por não possuírem os conhecimentos preconizados por Rotman (2009), ou seja, não apresentam comportamentos de privacidade suficientes porque podem não serem capazes de colocá-los em prática, ficando assim, à mercê da vigilância mercadológica e governamental (Bartsch & Dienlin, 2016).

Entretanto, o conhecimento técnico não é suficiente para motivar mudanças sociais, havendo assim, a necessidade de que as pessoas sejam capazes de refletir e questionar sua cultura e condições sociais a fim de se motivarem a impulsionar reformas sociais, nesse sentido, o letramento em privacidade assume um papel importante na democracia, mais ainda em sociedades autoritárias, nas quais as pessoas podem ter uma necessidade maior de se proteger contra identificação (Masur, 2020).

Como se pode observar, o letramento digital em privacidade constitui temática atual e altamente relevante ao contexto da Ciência da Informação, razão pela qual torna-se necessário analisar em que medida essa temática vem sendo objeto de reprodução científica na área, em âmbito internacional, especialmente em um momento em que a população global está sendo direcionada a uma adoção acrítica de tecnologias que representam, além dos avanços, perigo e possíveis prejuízos a direitos fundamentais no desempenhar da vida social.

2. Metodologia

Buscando investigar a temática do letramento em privacidade no campo da Ciência da Informação, realizou-se uma pesquisa de natureza exploratória, pautada em fontes documentais e valendo-se de uma metodologia de análise de domínio (Hjørland, 2002, 2017), em uma abordagem bibliométrica valendo-se de matriz quali-quantitativa (por utilizar-se de elementos métricos e de conteúdo), a partir de busca nas bases de dados Web of Science (WoS), Scopus e Library and Information Science Abstracts (LISA), a partir do termo “privacy literacy”.

Na Web of Science foram utilizados os seguintes elementos na estratégia de pesquisa: “categoria: information science library science” e “tipos de documento: article”, tendo sido recuperados sete

itens, todos disponíveis para download. Já na pesquisa realizada na base de dados Scopus, os refinamentos utilizados foram: "subject area: social science", "document type: article" e "publication stage: final". Dezoito itens foram recuperados, todos disponíveis para download. Por fim, a busca realizada na base de dados LISA ocorreu a partir do termo "privacy literacy", com os limitadores "em: qualquer lugar, exceto texto completo – NOFT", "tipo de fonte: periódicos acadêmicos", "tipo de documento: artigo" e "opções de resultados: excluir documentos duplicados", resultando na recuperação de 10 itens, todos disponíveis para download.

Chegou-se, desse modo, a um corpus preliminar de 35 artigos, o que, excluídas as indexações em mais de uma base, levou a um corpus final de 23 artigos, cujos dados geraram fichas de registro contendo o(s) nome(s) do(s) autor(es), país(es) e instituição(ões) de origem, nome da revista, data de publicação e palavras-chave. A partir das fichas de registro, os resultados foram reunidos em tabelas e gráficos, a seguir apresentados e analisados.

3. Resultados

No que tange aos autores, foi possível identificar um conjunto de 50 pesquisadores, com 55 incidências nos 23 itens analisados. A partir da representação da Figura 2, nota-se que 61% do corpus teve o envolvimento de um ou dois autores, demonstrando proximidade com o modo de produção de artigos científicos no campo das ciências humanas. Em relação aos artigos que possuem três ou mais autores envolvidos, destacam-se Kumar et al. (2020) com cinco autores e Kezer et al. (2016) e Liu et al. (2017) com quatro autores cada, nestes exemplos nota-se que, mesmo menor, uma parcela significativa da produção difere da prática comum na área de ciências humanas, na qual os artigos são produzidos preferencialmente por um ou dois autores.

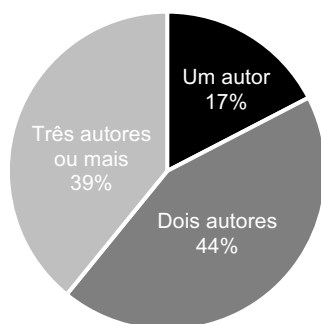


Figura 2. Autores por artigo

Verificou-se ainda a quantidade de artigos publicados por autor. Dos 50 pesquisadores, apenas cinco figuram como autores em dois artigos cada, a saber: Dan Bouhnik, Lemi Baruh, Maayan Zhitomirsky-Geffet, Maor Weinberger e Zeynep Cemalcilar. Os outros 45 publicaram somente um artigo. Isso revela que o tema vem sendo tratado ainda de forma incipiente, na medida em que os autores não têm demonstrado uma produção reiterada a respeito do tema, o que dificulta o aprofundamento das pesquisas. Tal resultado reitera a novidade do tema no campo da Ciência da Informação, pois ainda não foi possível sedimentar núcleos de pesquisadores mais produtivos a respeito.

Pela produção ser demasiadamente pulverizada entre autores, houve a necessidade de identificar a proveniência dessa produção, tanto geográfica, quanto institucional. A partir da análise de filiação institucional dos autores, foi possível identificar um conjunto de 30 instituições distribuídas em 14 países.

Países	Autor(es) vinculados
Estados Unidos	16
Alemanha	7
Israel	7
Turquia	6
Bélgica	4
Australia	3
Canadá	2
Hong Kong	2
Inglaterra	2
Irlanda	2
Bangladesh	1
Emirados Árabes Unidos	1
Holanda	1
Noruega	1
Total	55

Tabela II. Autores por países das instituições

Como pode observar na tabela II, há uma predominância de autores vinculados a instituições norte-americanas - Estados Unidos e Canadá – (33%), seguida de autores europeus (31%) que, juntos concentram 64% dos autores que publicaram sobre a temática no período analisado. Os demais autores provêm da Ásia (31%) e da Oceania (5%). Não se verificou nenhuma publicação da América Latina nem da África, aspectos que causam certa preocupação uma vez que tais regiões geográficas são permeadas por situações

econômicas que evidenciam mais fortes desigualdades no que se refere à cultural digital.

Verificou-se também a colaboração entre autores de diferentes instituições e países. No artigo de Lutz et al. (2020) há a colaboração entre autores de três universidades de três países diferentes (BI Norwegian Business School - Noruega, University of Leipzig - Alemanha, Vrije Universiteit Amsterdam - Holanda); em Epstein e Quinn (2020) 2 autores de 2 países: The Hebrew University of Jerusalem (Israel) e The University of Illinois – EUA; Liu et al. (2017)- dois autores são da City University of Hong Kong (Japão) e dois da University of Illinois (EUA); Weinberger e Zhitomirsky-Geffet da Bar-Ilan University (Israel) e Bouhnik da Jerusalem College of Technology – Israel; Miah et al. (2017) da Victoria University (Australia), Gammack da Zayed University (Emirados Árabes Unidos) e Hasan da MRC Bangladesh Ltd (Bangladesh). Os demais artigos em coautoria são de autores da mesma instituição ou de instituições diferentes no mesmo país, como Desimpelaere, Hudders e Sompel (2020), sendo os dois primeiros da Ghent University e Faculty of Economics and Business Administration (Bélgica).

Periódicos	Artigos
Media and Communication	3
Surveillance & Society	2
American Behavioral Scientist	1
ASIS&T	1
Chinese Journal of Communication	1
Communications in Information Literacy	1
IFLA Journal	1
Information Research	1
Information Systems	1
Information Systems Journal	1
Journal of Documentation	1
Journal of Information Ethics	1
Journal of psychosocial research on cyberspace	1
Meta-analysis	1
New Media & Society	1
Online Information Review	1
Social Media + Society	1
The Journal of Consumer Affairs	1
The DATA BASE for Advances in Information Systems	1
Total	22

Tabela III. Periódicos identificados e artigos

A produção acerca do tema também é pulverizada em relação às revistas em que foram publicados, conforme Tabela III, nota-se que os artigos foram publicados em 18 (2) periódicos diferentes e que apenas dois deles possuem dois ou mais artigos.

Destacam-se, nesse contexto, os periódicos ASIS&T, Communications in Information Literacy, IFLA Journal, Information Research, Journal of Documentation, Journal of Information Ethics e Online Information Review, a partir dos quais se demonstra que esta é uma temática contemplada no escopo dos periódicos da Ciência da Informação em geral e não se restringe a apenas algumas revistas.

Já em relação à cronologia das publicações (Figura 3), nota-se que a temática passou a receber atenção mais constante a partir de 2016, não havendo mais interrupção de artigos publicados. Os picos de publicações podem ser verificados em 2017 (ano anterior à efetivação da implementação da GDPR, o que pode evidenciar uma tendência da comunidade científica) e em 2020, demonstrando assim, que o tema tem relevância em relação ao cenário de discussão e adequação às novas leis de proteção de dados.

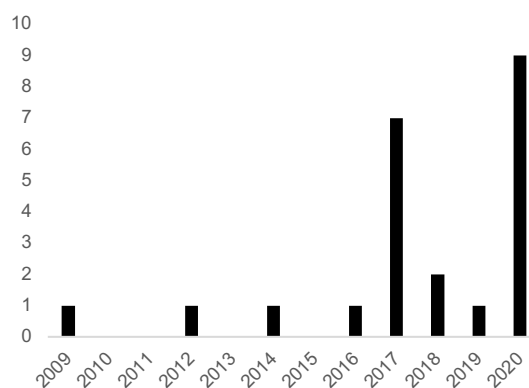


Figura 3. Cronologia dos artigos publicados

Passando-se a uma análise da forma como os artigos foram representados tematicamente por seus autores, identificou-se um conjunto de 113 (cento e doze) palavras-chave, o que significa uma média de 4,91 por artigo. Desse universo, foram preliminarmente excluídas as representações vagas ou metafóricas visto não atingirem a especificidade temática dos artigos recuperados, tais como: cinismo da privacidade, paradoxo da privacidade, paradoxo, algoritmos, capitalismo em plataformas e princípios de Biblioteconomia e Ciência da Informação. Em seguida, realizou-se uma análise de conteúdo (Bardin, 2013) das

palavras-chave significativas, categorizando-as como se descreve a seguir.

Uma primeira categoria refere-se ao processo que norteia a temática do presente trabalho: o letramento. Nesse sentido, observou-se uma forte incidência dessa temática, abrangendo palavras-chave relativas ao assunto, seja em âmbito geral, seja a aspectos específicos como o letramento digital, o letramento informacional, o letramento nos meios de comunicação e, mais fortemente, o letramento em privacidade. Esse letramento, por sua vez, teve por Objeto precípua a Informação pessoal.

Em seguida, buscou-se identificar o âmbito temático dos Contextos abordados, obtendo-se incidências relativas a Bibliotecas, Educação (nível superior, planos de ensino/currículo, jogos educativos e aprendizagem), Internet, Mídias e redes sociais, Saúde e à Sociedade da Informação, em que se vale de Meios notadamente digitais (Comunicação mediada por Tecnologia digital, Tecnologia da informação, Novas mídias e Dispositivos móveis, para atingir Sujeitos como Crianças, Idosos e Pais.

Para tanto, os artigos valem-se de Aportes teórico-metodológicos variados, fazendo uso de Análise de Conteúdo, Teorias críticas, Pesquisa participativa, Pesquisa social, Surveys, Princípios de transmissão, Design de sistemas de informação, Data collection, Teoria da motivação para proteção, e ainda de Métodos híbridos, evidenciando Interdisciplinaridades com a Comunicação, o Design e a Ética.

Emergiram, ainda, temáticas que evidenciam Valores (ou objetivos) relativos à Privacidade, Proteção de dados, Inclusão, Integridade contextual; Compartilhamento de informações e Autodeterminação informacional, entre outros. Em contrapartida, alguns Problemas (ou consequências) foram destacados como elementos temáticos de abordagem, relativos à Segregação digital, Plágio, Monitoramento, Individualismo, Anonimidade online, Datificação e a identificação das Fronteiras da privacidade.

4. Conclusão e perspectiva de continuidade da pesquisa

Considerando o letramento em privacidade como uma ferramenta a ser disponibilizada à sociedade para promover o desenvolvimento de habilidades que possam subsidiar ações individuais e coletivas para preservação de direitos como a privacidade, proteção de dados e ao esquecimento, o presente trabalho buscou verificar e analisar como o tema vem sendo tratado no meio

científico da Ciência da Informação a partir de bases de dados internacionais.

Os resultados evidenciam pulverização de autores, de instituições e de países e não permitem identificar, ainda, uma comunidade epistêmica sobre essa temática, mas esta parece estar em vias de constituição, uma vez que foi possível identificar um grupo de autores dedicados ao tema, mas ainda com uma produção dispersa. Tal aspecto se explica pelo fato de ser um tema ainda recente, cujos impactos vão sendo notados ao longo do tempo. Em que pese o fato de haver ainda uma produção científica pequena sobre o tema – o que poderia, de uma primeira leitura, sinalizar para um certo grau de invisibilidade – tem-se que o crescimento gradual dessa literatura revela uma relevância científica que desponta, em muito decorrente de sua indiscutível relevância social, haja vista que o tema vem se fazendo cada vez mais presente na mídia em geral, bem como em documentos normativos. Por outro lado, tal pulverização sinaliza para o fato de o tema revelar uma preocupação de natureza global e que apresenta perspectivas de crescimento e verticalização dados seus impactos na área.

Um aspecto positivo a ressaltar reside no fato de haver efetiva incidência de estudos colaborativos, com pesquisadores de instituições e países distintos, o que reforça a ideia de que a comunidade investigativa sobre o tema se encontra em fase de consolidação de tal modo que nos próximos anos poder-se-á identificar núcleos de pesquisa sobre esse tema, com a formação de colégios invisíveis (3).

Aspecto relevante a destacar, na literatura analisada, reside em uma preocupação dos estudos com grupos supostamente mais vulneráveis como crianças e idosos que precisam ser instruídos para que não se exponham a riscos ao expor seus dados na internet.

Por fim, e à vista dos dados relativos à segunda etapa da pesquisa, ora em desenvolvimento, percebe-se que essa natureza incipiente e emergente da literatura de Ciência da Informação, verificada no período pré-covid-19 se altera substancialmente a partir de 2021, seja no que tange à quantidade e à diversidade de autores, de instituições e de países e se torna mais complexa relativamente às temáticas envolvidas. Exemplo disso, ainda como dado preliminar, é a verificação de um crescimento da ordem de 620% das publicações nessa temática, indexadas apenas na base LISA (4).

Notas

- (1) Esse conjunto de dados se convencionou chamar por “dados pessoais” e são objetos de preocupação atualmente, por conta de, ao longo das últimas décadas, terem assumido característica de bem de consumo, o qual empresas e governos fazem de insumo para gerar insights e assim orientar suas atividades. Essa dinâmica, ainda pouco explorada, vem sendo tratada por estudiosos por meio de denominações como “economia de dados”, “capitalismo de dados”, “capitalismo de vigilância”, “economia de vigilância”, entre outras.
- (2) Um dos artigos que compõe o corpus analisado foi publicado em livro, não figurando assim, na análise de periódicos.
- (3) Um colégio invisível constitui uma comunidade de especialistas, independentemente de inserções geográficas ou institucionais, que atua de forma dinâmica, interativa e cooperativa, evidenciando muitas vezes coautorias e citações, e contribuindo para resultados de pesquisas mais robustos e cientificamente visíveis, com maior reconhecimento de seus pares (Crane, 1972; Hayashi et al., 2021; Merton, 1988; Price & Beaver, 1966).
- (4) Busca realizada no dia 29/02/2024 às 10:52h utilizando o termo “*privacy literacy*”, recuperando 72 itens.

Agradecimentos

Os autores consignam seu agradecimento à Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, pelo apoio financeiro à pesquisa, bem como ao Prof. Dr. Daniel Martínez-Ávila pelo suporte na recuperação dos dados na base LISA.

Referencias

- Bagatini, José Augusto (2019). A vulnerabilidade dos dados pessoais: Uma análise a partir de suas formas de divulgação indevida. Universidade Estadual Paulista - UNESP. Dissertação de mestrado.
- Bagatini, José Augusto; Guimarães, José Augusto C. (2021). Quando a memória encontra a internet: Reflexões acerca da vulnerabilidade da memória digital. // *Ibersid: revista de sistemas de información y documentación*. 15:2. <https://doi.org/10.54886/ibersid.v15i2.4773>
- Bardin, Laurence (2013). *L'analyse de contenu* (2ª ed.). Quadrige.
- Bartsch, Miriam; Dienlin, Tobias (2016). Control your Facebook: An analysis of online privacy literacy. // *Computers in Human Behavior*. 56, 147–154. <https://doi.org/10.1016/j.chb.2015.11.022>
- Castells, Manuel (2009). *The Rise of the Network Society* (2ª ed.). Wiley-blackwell.
- Correia, Flavia (2023). SpaceX passa de 5 mil satélites Starlink implantados em órbita. // *Olhar Digital*. <https://olhardigital.com.br/2023/08/27/ciencia-e-espaco/spacex-passa-de-5-mil-satelites-starlink-implantados-em-orbita/>
- Crane, Diana (1972). *Invisible Colleges: Diffusion of Knowledge in Scientific Communities*. University of Chicago Press.
- Dent, Steve (2021). Amazon has acquired Facebook's satellite internet team. // *Engadget*. <https://www.engadget.com/amazon-has-acquired-facebooks-satellite-internet-group-115312282.html>
- Desimpelaere, Laurien; Hudders, Liselot; Sompel, Dienneke Van de (2020). Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study. // *Media and Communication*. 8:4, Article 4. <https://doi.org/10.17645/mac.v8i4.3232>
- Epstein, Dmitry; Quinn, Kelly (2020). Markers of Online Privacy Marginalization: Empirical Examination of Socioeconomic Disparities in Social Media Privacy Attitudes, Literacy, and Behavior. // *Social Media + Society*. 6:2. <https://doi.org/10.1177/2056305120916853>
- Eshet-Alkalai, Yoram; Amichai-Hamburger, Yair (2004). Experiments in Digital Literacy. // *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*. 7, 421–429. <https://doi.org/10.1089/cpb.2004.7.421>
- European Union (2016). Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). <http://data.europa.eu/eli/reg/2016/679/2016-05-04>
- Givens, Cherie L. (2015). *Information Privacy Fundamentals for Librarians and Information Professionals*. Rowman & Littlefield Publishers. <https://rowman.com/isbn/9781442228818>
- Hayashi, Maria Cristina P. I.; Maroldi, Alexandre Masson; Hayashi, Carlos Roberto M. (2021). In vitam et post-mortem: Expressões de gratidão a Derek de Solla Price em agradecimentos e obituários acadêmicos. // *Palabra Clave (La Plata)*. 11:1, Article 1. <https://doi.org/10.24215/18539912e143>
- Hjørland, Birger (2002). Domain analysis in information science. Eleven approaches—Traditional as well as innovative. // *Journal of Documentation*. 58:4, 422–462. <https://doi.org/10.1108/00220410210431136>
- Hjørland, Birger (2017). Domain analysis. // *Knowledge Organization*. 44:6, 436–464. <https://doi.org/10.5771/0943-7444-2017-6-436>
- Hootsuite; We Are Social. (2019). *Digital 2019: Global Digital Overview*. <https://datareportal.com/reports/digital-2019-global-digital-overview>
- Information is Beautiful. (2021). *World's Biggest Data Breaches & Hacks*. // *Information Is Beautiful*. <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- Kezer, Murat [et al.] (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. // *Cyberpsychology*. 10. <https://doi.org/10.5817/CP2016-1-2>
- Kumar, Priya C. [et al.] (2020). Strengthening Children's Privacy Literacy through Contextual Integrity. // *Media and Communication*. 8:4, Article 4. <https://doi.org/10.17645/mac.v8i4.3236>
- Langenderfer, Jeff; Miyazaki, Anthony D. (2009). Privacy in the Information Economy. // *The Journal of Consumer Affairs*. 43:3, 380–388. <https://doi.org/10.1111/j.1745-6606.2009.01152.x>
- Liu, Qian [et al.] (2017). Predicting users' privacy boundary management strategies on Facebook. // *Chinese Journal of Communication*. 10:3, 295–311. <https://doi.org/10.1080/17544750.2017.1279675>
- Lutz, Christoph; Hoffmann, Christian Pieter; Ranzini, Giulia (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. // *New Media & Society*. 22:7, 1168–1187. <https://doi.org/10.1177/1461444820912544>
- Marzal, Miguel-Ángel (2020). A taxonomic proposal for multi-literacies and their competences. // *Profesional de La Información*. 29:4. <https://doi.org/10.3145/epi.2020.jul.35>
- Masur, Philipp K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of

- information. // *Media and Communication*. 8:2, 258–269. <https://doi.org/10.17645/mac.v8i2.2855>
- Merton, Robert K. (1988). The Matthew Effect in Science, II: Cumulative Advantage and the Symbolism of Intellectual Property. // *Isis*. 79:4, 606–623. <https://doi.org/10.1086/354848>
- Meta (2021, October 28). The Facebook Company Is Now Meta. // Meta. <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/>
- Meta (2024). Meta Connectivity. // Meta. <https://www.facebook.com/connectivity/solutions/discover>
- Miah, Shah J.; Gammack, John; Hasan, Najmul (2017). Extending the framework for mobile health information systems Research: A content analysis. // *Information Systems*. 69, 1-24. <https://doi.org/10.1016/j.is.2017.04.001>
- Naciones Unidas (2023). Se acaba la emergencia por la pandemia, pero el COVID continua. // Noticias ONU. <https://news.un.org/es/story/2023/05/1520732>
- NordVPN (2021). National Privacy Test. <https://nationalprivacytest.org>
- Organización Panamericana de Salud (2020). La OMS caracteriza a COVID-19 como una pandemia. // Organización Panamericana de la Salud. <https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia>
- Poetranto, Irene; Ruan, Lotus (2021). Intrusive Surveillance After the Coronavirus Pandemic: Issues on the Frontlines of Technology and Politics. // Carnegie Endowment for International Peace. <https://carnegieendowment.org/2021/10/19/intrusive-surveillance-after-coronavirus-pandemic-pub-85509>

Enviado: 2024-04-01. Segunda versión: 2024-05-29.
Aceptado: 2024-06-10.
