Competências digitais e a proteção de dados pessoais e privacidade

José Augusto Bagatini Lopes Pinto
Helen de Castro Silva Casarin

Como citar: PINTO, José Augusto Bagatini Lopes; CASARIN, Helen de Castro Silva. Competências digitais e a proteção de dados pessoais e privacidade. *In*: MOREIRA, Fábio Mosso *et. al.* (org.). Transversalidade e verticalidade na Ciência da Informação. Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2025. p.185-198. DOI: https://doi.org/10.36311/2025.978-65-5954-613-8.p185-198

Capítulo 10

Competências digitais e a proteção de dados pessoais e privacidade

José Augusto Bagatini Lopes Pinto[1] *e Helen de Castro Silva Casarin*[2]

Introdução

Com os recentes avanços das tecnologias da informação, um debate sobre o direito à privacidade vem se desenvolvendo e tomando contornos mais profundos em diversos campos do saber. Isso acontece porque existe uma demanda global por menos intromissão de governos e empresas na vida privada da população, a qual convive com a constante vigilância que se instalou paulatinamente após a Segunda Guerra Mundial e que se aprofundou após os ataques de 11 de setembro de 2001 nos Estados Unidos. Contudo, ressalta-se que vigiar não é uma característica única da sociedade contemporânea, haja vista que registros de atividades relacionadas ao vigiar existem desde a antiguidade. O que torna a vigilância contemporânea diferente é a sua penetrabilidade, uma vez que ela se projeta a partir de dispositivos e protocolos de comunicação fundamentais para o desenvolvimento da vida cotidiana de grande parte da população global.

[1] Doutorando em Ciência da Informação na Universidade Estadual Paulista – UNESP. E-mail: jose.bagatini@unesp.br. ORCID: https://orcid.org/0000-0002-8830-2075. Lattes: http://lattes.cnpq.br/9620353634513776.

[2] Doutora em Letras. Professora na Universidade Estadual Paulista – UNESP. E-mail: helen.castro@unesp.br. ORCID: https://orcid.org/0000-0002-3997-9207. Lattes: http://lattes.cnpq.br/0592809928580900.

https://doi.org/10.36311/2025.978-65-5954-613-8.p185-198

Assim como a vigilância, a noção de privacidade não é uma construção da humanidade contemporânea, e como preconizado por Westin (1967) em seu livro *Privacy and Freedom* (seminal para os estudos sobre privacidade e vigilância) a partir dos estudos de Edward T. Hall (*The Hidden Dimension*) e Robert Andrey (*Territorial Imperative e Territory in Bird Life*), pode ser uma herança ancestral herdada durante o processo evolutivo da raça humana e compartilhada com outras espécies de animais. Com base nesses estudos, Westin (1967, p. 56) destaca que:

> virtually all animals seek periods of individual seclusion or small-group intimacy. This is usually described as the tendency toward territoriality, in which an organism lays private claim to an area of land, water, or air and defends it against intrusion by members of its own species. […] Animals and man also share elaborate distance-setting mechanisms to define territorial spacing of individuals in the group. The distance set between one non-contact animal and another (illustrated by the spacing of birds on a telephone wire) has been called "personal distance (Westin, 1967, p. 56).

Portanto, segundo Westin (1967), a privacidade pode ser definida como sendo "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*". Suas funções podem agrupar-se a quatro categorias maiores, sendo "*personal autonomy*", "*emotional release*", "*self-evaluation*", e "*limited and protected communication*", as quais fluem constantemente transpassando umas às outras (Westin, 1967, p.7).

Essas e as outras contribuições da obra de Westin compõem um importante marco na história do desenvolvimento da privacidade quanto direito ao redor do mundo. Entretanto, sua publicação serve também como uma antecipação de como esse direito viria a ser atacado e enfraquecido ao longo dos últimos cinquenta anos pelas novas dinâmicas impostas pelo Capitalismo de Vigilância.

A reconfiguração capitalista que ocorre após a Segunda Guerra mundial toma impulso na esteira das inovativas Tecnologias da Informação

(TIC), alterando drasticamente os fundamentos de produção e vida. Ou seja, a sociedade incorporou no seu exercício cotidiano uma série de tecnologias (Castells, 2009; Harvey, 1992). Somado a isso, a Guerra Fria é conhecidamente um período em que o direito à privacidade se enfraqueceu diante da ameaça ideológica que Estados Unidos e União Soviética representavam um para o outro e seus aliados, construindo assim, um imperativo social onde é privilegiado o ato de exposição. Esses contornos se aprofundam com a popularização da computação pessoal e a disseminação da internet como meio de comunicação, o que proporcionou um aumento significativo da produção de dados de natureza pessoal. Essa trilha de dados é definida pelo termo "*data shadow*", que tem sua origem atribuída tanto a Alan F. Westin quanto a Kerstin Anér, político sueco (Bellovin, 2021).

A preocupação sobre como a computação pessoal e a internet afetaria a privacidade e a autonomia pessoal ganhou tração na década de 1990, onde se instalou uma competição ideológica sobre o futuro da rede mundial de computadores. É na referida década em que documentos e ações reconhecidamente pró-privacidade tomam forma, tais como: *Common Rule Human Subject Research Privacy* (1991), *A Cypherpunk's Manifesto* (1993), *EU Data Protection Directive* (1995), *HIPAA Health and Medical Privacy* (1996), *COPPA Children's Online Privacy (1998), Chief Counselor for Privacy in Federal Government* (1999), *Gramm Leach Bliley Act* (1999) e *First Chief Privacy Officer* (1999).

Contudo, o início de uma guinada ocorre durante os primeiros anos do segundo milênio. A popularização da internet gerou um bioma perfeito para a especulação do capital do risco, uma grande quantidade de dinheiro foi investido em empresas que prometiam ser lucrativas no meio digital, entretanto, ao passo que isso não se confirmava, os principais investidores retiraram seus aportes financeiros, instaurando assim um pânico generalizado, resultando na falência de grande parte das companhias do ecossistema. As que sobreviveram, passaram a sofrer com uma grande pressão para apresentarem lucros o mais breve possível. Marca-se o efetivo estourar da bolha no ano de 2001. No mesmo ano, no dia 11 de setembro, quatro aviões foram sequestrados e usados como arma para um ataque coordenado às Torres Gêmeas, Pentágono e o prédio do Governo Federal dos Estados Unidos. A identificação dos executores enfrentou percalços,

principalmente em relação a interoperabilidade das bases de dados e informações disponíveis sobre os suspeitos, tal situação gerou assim um clamor para reformas no sistema de segurança do país.

Essa tensão gerada pelas questões econômica e de segurança nacional resultou em uma aliança público-privada para o desenvolvimento e aplicação de tecnologias de espionagem. Véliz (2021) preconiza que o Google (hoje parte do conglomerado Alphabet), é o principal expoente do setor privado nessa fase do desenvolvimento do capitalismo de vigilância, sendo a responsável por transformar a maneira como os dados pessoais eram utilizados, abandonando uma lógica de aprimoramento de serviços a partir de um pequeno conjunto de dados, e adotando práticas de exploração, onde o conjunto de dados extraídos dos usuários cresceu e passou a fornecer subsídios para aprimoramento de acúmulo de capital. No mesmo sentido, Zuboff (2021) afirma que o Google é para o capitalismo de vigilância o que a *Ford Motor Company* e *General Motors* foram para o capitalismo gerencial com base na produção em massa – na nossa era, o Google tornou-se o pioneiro, descobridor, desenvolvedor, experimentador, principal praticante, exemplo e centro de difusão do capitalismo de vigilância.

A principal descoberta do Google foi publicidade direcionada com base em dados pessoais. Esse foi o ponto de inflexão onde o capitalismo de vigilância nasceu, o aperfeiçoamento das suas práticas de extração de dados pessoais foi o que solidificou e a alta rentabilidade dos seus produtos e gerou um enorme interesse no Capital em replicar o modelo de negócios, foi o pontapé inicial para a reinvenção do capitalismo, onde transacionamos de um modelo de mercado baseado no mecanismo de precificação, para um mercado fundamentado e enriquecido com dados (Mayer-Schönberger; Ramge, 2018).

Esse novo modelo predatório de exploração de dados só obteve êxito em sua disseminação, porque como já preconizado, havia um interesse do governo estadunidense em utilizar as tecnologias e bases de dados dos capitalistas de vigilância para cumprimento de sua agenda de segurança pública. Tais práticas se enraizaram na sociedade contemporânea e não temos garantia de que a internet voltará a ser um ambiente livre do extrativismo de dados pessoais, na verdade, o que podemos esperar é que tais práticas de vigilância continuem se tornando cada vez mais ubíquas.

Diante do exposto, é possível notar que o imperativo vigente durante as últimas duas décadas é o da exploração dos dados pessoais e do enfraquecimento da privacidade. Casos famosos ilustram como o capitalismo de dados é predatório e prejudicial a população global, ao exemplo das denúncias de Edward Snowden sobre a espionagem da NSA, a eleição de Donald Trump para a presidência dos Estados Unidos, os megas vazamentos de dados de *data brokers* etc.

Proteção de dados pessoais e privacidade no DigCComp 2.2

Em busca de minimizar os danos causados por situações análogas às citadas acima, iniciativas foram tomadas ao redor do mundo e consolidou um movimento global de regularização da exploração dos dados pessoais que objetiva equalizar a relação de poder entre o proprietário dos dados pessoais e os interessados em explorar esses dados. No que diz respeito ao campo jurídico, leis que buscam regular o mercado da privacidade passaram a ser desenvolvidas e adotadas ao redor do mundo. Dos 194 países listados pela *United Nations Conference on Trade and Development* (UNCTAD), 66% já contam com legislações que contemplam a proteção de dados pessoais, 10% se encontram em processo de desenvolvimento de *frameworks* jurídicos acerca do tema, 19% dos países não possuem legislação e nenhum projeto em trâmite, e por fim, 5% dos 194 países, não possuem dados armazenados em seu território (UNCTAD, 2020). Na América Latina, o primeiro país a adotar uma lei dessa natureza foi o Chile em 1999, seguido pela Argentina em 2000, e mais recentemente outros países vêm seguindo a tendência, ao exemplo do Uruguai (2008), México (2010), Peru (2011), Colômbia (2012), Brasil (2018), Barbados (2019) e Panamá (2019) (Rodriguez; Alimonti, 2020).

Das legislações que abordam o tema de proteção de dados e privacidade, a *General Data Protection Regulation* (GDPR) é a mais proeminente. Teve sua aprovação em maio de 2016 e entrou em vigor em maio de 2018, revogando 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 caraterísticas modernas, tornou-se um modelo a ser seguido por outros países. Forneceu base também para a atualização 2.2 do Quadro Europeu de Competência Digital para Cidadãos (DigComp), publicado em 2022.

O DigComp foi publicado pela primeira vez em 2013 (1.0), teve sua primeira atualização em 2016 (2.0) e uma segunda em 2018 (2.1). A versão 2.2 foi publicada em 2022, sendo a quarta atualização, que apresenta uma reformulação dos exemplos de conhecimentos, capacidades e atitudes que constam na primeira versão. 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; Kluzer; Punie, 2022).

O documento define competência digital como sendo competências essenciais para a aprendizagem ao longo da vida e envolve o uso confiante, crítico e responsável, e o envolvimento com tecnologias digitais para aprendizagem, o trabalho e a participação na sociedade, inclui a literacia de informação e de dados, a comunicação e colaboração, a literacia dos media, a criação de conteúdos digitais (incluindo programação), a segurança (incluindo o bem-estar digital e competências relacionadas com a cibersegurança), questões relacionadas com a propriedade intelectual, a resolução de problemas e o pensamento crítico (Vuorikari; Kluzer; Punie, 2022).

Especificamente no que diz respeito a divisão das competências digitais, o documento descreve que existem cinco áreas, as quais englobam (Quadro 1): Literacia de Informação e de dados; Comunicação e colaboração; Criação de conteúdo digital; Segurança; e Resolução de problemas (Vuorikari; Kluzer; Punie, 2022).

A área de competência número 4. Segurança é subdividido nas competências: 4.1 Proteção de Dispositivos – proteger dispositivos e conteúdo digital e perceber os riscos e ameaças em ambientes digitais. Ter conhecimento sobre proteção e medidas de segurança e ter em conta a confiabilidade e privacidade; 4.2 Proteção de Dados Pessoais e Privacidade – Proteger os dados pessoais e a privacidade em ambientes digitais. Compreender como utilizar e partilhar informação pessoalmente identificável, sendo ao

mesmo tempo capaz de se proteger a si próprio e aos outros de danos. Compreender que os serviços digitais utilizam uma "política de privacidade" para informar como são utilizados os dados pessoais; 4.3 Proteção da Saúde e do Bem-Estar – ser capaz de evitar riscos para a saúde e ameaças ao bem-estar físico e psicológico enquanto utiliza tecnologias digitais. Ser capaz de se proteger a si e aos outros de possíveis perigos em ambientes digitais (por exemplo, *cyberbullying*). Ter consciência das tecnologias digitais dedicadas ao bem-estar social e à inclusão social; e 4.4 Proteção do Meio Ambiente – ter consciência do impacto ambiental das tecnologias digitais e da sua utilização (Vuorikari; Kluzer; Punie, 2022).

Quadro 1 – Áreas de competência e seus descritores

1. Literacia de informação e de dados
• Articular necessidades de informação, localizar e recuperar dados, informação e conteúdo digital; • Ajuizar sobre a relevância da fonte e do seu conteúdo; • Armazenar, gerir e organizar dados, informação e conteúdo digital.
2. Comunicação e colaboração
• Interagir, comunicar e colaborar através de tecnologias digitais enquanto simultaneamente consciente da diversidade cultural e geracional; • Participar na sociedade através de serviços digitais públicos e privados e cidadania participativa; • Gerir a sua identidade e reputação digital.
3. Criação de conteúdo digital
• Criar e editar conteúdo digital; • Aperfeiçoar e integrar informação e conteúdo num corpo de conhecimento existente compreendendo simultaneamente como se aplicam direitos de autor e licenças; • Saber como fornecer instruções compreensíveis para um sistema de computação.
4. Segurança
• Proteger dispositivos, conteúdo, dados pessoais e privacidade em ambientes digitais; • Proteger a saúde física e psicológica e ter consciência das tecnologias digitais para o bem-estar social e inclusão social; • Estar ciente do impacto ambiental das tecnologias digitais e da sua utilização.
5. Resolução de problemas
• Identificar necessidades e problemas e resolver problemas conceptuais e situações problema em ambientes digitais; • Utilizar ferramentas digitais para inovar processos e produtos; • Manter-se a par da evolução digital.

Fonte: Autores, adaptado de Vuorikari, Kluzer e Punie (2022, p.7).

Cada uma das competências se divide em quatro níveis de proficiência (Quadro 2), que se dividem também em mais dois subníveis cada. Isso posto, a presente seção busca evidenciar especificamente como os temas proteção de dados e privacidade são abordados na área de competência número 4. Segurança, portanto, a análise debruçar-se-á sobre o item número 4.2 Proteção de Dados Pessoais e Privacidade, as especificações de cada nível de proficiência se apresenta da seguinte maneira:

Quadro 2 – Níveis de proficiência

Básico (com orientação)
• Selecionar formas simples de proteger os dados pessoais e privacidade em ambientes digitais; identificar formas simples de usar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; identificar declarações da política de privacidade simples sobre como os dados pessoais são usados em serviços digitais.
Básico (com autonomia e orientação apropriada onde necessário)
• Selecionar formas simples de proteger os dados pessoais e privacidade em ambientes digitais; identificar formas simples de usar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; identificar declarações da política de privacidade simples sobre como os dados pessoais são usados em serviços digitais.
Intermediário (sozinho e a resolver problemas simples)
• Explicar formas bem definidas e rotineiras de proteger os meus dados pessoais e a privacidade em ambientes digitais; explicar formas bem definidas e rotineiras de usar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; indicar declarações da política de privacidade bem definidas e rotineiras de como os dados pessoais são usados em serviços digitais.
Intermediário (independente de acordo com minhas próprias necessidades e resolvendo problemas bem definidos)
• Discutir formas de proteger os meus dados pessoais e privacidade em ambientes digitais; discutir formas de utilizar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; indicar declarações da política de privacidade sobre como os dados pessoais são usados em serviços digitais.
Avançado (para além de orientar outros)
• Aplicar diferentes formas de proteger os meus dados pessoais e privacidade em ambientes digitais; aplicar diferentes formas específicas de partilhar os meus dados, enquanto me protejo a mim e aos outros contra perigos; explicar as declarações da política de privacidade que abordam a forma como os dados pessoais são usados em serviços digitais.

Avançado (de acordo com as minhas próprias necessidades e as de outros, em contextos complexos)
• Escolher as formas mais apropriadas de proteger os dados pessoais e privacidade em ambientes digitais; avaliar as formas mais apropriadas de utilizar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; avaliar a adequação de declarações da política de privacidade sobre como os dados pessoais são usados.
Altamente especializado (no nível altamente especializado, sou capaz de)
• Criar soluções para problemas complexos, com definição limitada, relacionadas com a proteção dos dados pessoais e a privacidade em ambientes digitais, utilizando e partilhando informação pessoalmente identificável, protegendo-me e aos outros de danos, e políticas de privacidade para usar os meus dados pessoais; integrar o meu conhecimento para contribuir para a prática e conhecimento profissional e orientar outros na proteção dos dados pessoais e privacidade;
Altamente especializado (no nível mais avançado e especializado, sou capaz de):
• Criar soluções para resolver problemas complexos, com muitos fatores que interagem entre si, relacionadas com a proteção de dados pessoais e privacidade em ambientes digitais, utilizando e partilhando informação pessoalmente identificável, protegendo-me aos outros de danos, e políticas de privacidade para usar os meus dados pessoais; propor novas ideias e processos para a área.

Fonte: Autores adaptado de Vuorikari, Kluzer e Punie (2022, p.35).

O documento apresenta também exemplos de conhecimento, capacidades e atitudes relativas à proteção de dados pessoais e privacidade. Sendo eles os que estão apresentados no Quadro 3.

Quadro 3 – Conhecimentos, capacidade e atitudes

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 como terceiros.
• Sabe que o processamento de dados pessoais está sujeito a regulamentos locais, tais como o regulamento Geral de Proteção de Dados da UE (RGPD) (por exemplo, as interações de voz com um assistente virtual são dados pessoais em termos do RGPD e podem expor os utilizadores a determinados riscos de proteção de dados, privacidade e segurança. (IA)

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 eletrônico 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 eletrônica 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). As atitudes se apresentam como:
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.

Fonte: Autores, adaptado de Vuorikari, Kluzer e Punie (2022, p. 37).

Fica evidente a partir da leitura da versão 2.2 do DigComp que a questão da proteção de dados e a privacidade é abordada quase que totalmente de maneira centrada no indivíduo, embora faça menções ao componente coletivo, aspecto mais importante na visão de Masur (2020). Para o autor, isso se dá porque as discussões contemporâneas sobre privacidade adotam quase que exclusivamente uma perspectiva enraizada em teorias liberais, ou seja, nesse espectro liberal da privacidade, o foco está na proteção do indivíduo, portanto, as soluções propostas incluem, mas se limitam, ao fortalecimento de conhecimentos e habilidades individuais para autopreservação e a implementação de regulações de proteção à privacidade e dados em nível político (Masur, 2020). É proposto então pelo autor, que haja a promoção da capacidade crítica de um indivíduo decidir por si mesmo, quando e dentro de quais limites as informações sobre si devem ser coletadas, analisadas e disseminadas, possibilitando que o atual para-

digma seja desafiado com alternativas baseadas em premissas diferentes, não liberais (Masur, 2020).

Nesse sentido, a Ciência da Informação desempenha papel fundamental na promoção das competências digitais, todavia, cabe ressaltar que ambas florescem em um momento de avanço do liberalismo econômico, tornando-se assim necessário uma profunda reflexão acerca do que é perpetuado no campo. A partir do evidenciado, em busca de verificar como a Ciência da Informação e sua literatura vem tratando a relação das competências digitais, proteção de dados e privacidade, foi realizada uma busca na base de dados *Library and Information Science Abstracts* (LISA), no dia 30/11/2022, a partir da expressão de busca "*digital competen**" *and* "*data protect**" *and* "*privacy*".

Foram recuperados 12 artigos, os quais foram publicados nos anos de 2022 (1), 2021 (4), 2020 (2), 2019 (2), 2018 (1), 2016 (1), 2010 (1). Demonstrando assim que a temática vem ganhando relevância ao longo dos últimos anos, principalmente após 2016, ano em que entra vigor a GDPR. Dentre os artigos, destacam-se os intitulados "*La protección de datos personales em las bibliotecas universitárias españolas em el entorno digital*" (Varela-Orol; Ameneiros Rodríguez, 2018), "A *study of higher education students' self-perceived digital competences for learning and everyday life online participation*" (Martzoukou *et al.*, 2020) e "*Privacy and default*" *and active* "*informed consent*" (Noain-Sánchez, 2016), sendo os artigos que mais se aproximam da temática aqui analisada. Os itens recuperados mesclam-se em aqueles que fogem da temática ou fazem menções tímidas a mesma e não se ocupam da mesma como item principal:

- A *Digital Patient-Provider Communication Intervention* (InvolveMe): *Qualitative Study on the Implementation Preparation Based on Identified Facilitators and Barriers* (Seljelid *et al.*, 2021);
- *Digital Health Competencies Among Health Care Professionals: Systematic Review* (Longhini;Rossettini; Palese, 2022);
- *Formation of the Business Model of Crypto Asset Management* (Glubokova *et al.*, 2021);

- *Indicadores compuestos como metodología innovadora en Comunicación. Aplicación para la evaluación de los medios* públicos *europeos* (Blasco-Blasco; Rodríguez-Castro; Túñez-López, 2020);
- *Learning and Use of eHealth Among Older Adults Living at Home in Rural and Nonrural Settings: Systematic Review* (Airola, 2021);
- *Literature on Wearable Technology for Connected Health: Scoping Review of Research Trends, Advances, and Barriers* (Loncar-Turukalo *et al.*, 2019);
- *Measurement of Digital Literacy Among Older Adults: Systematic Review* (OH *et al.*, 2021);
- *Structuring stakeholder e-inclusion needs* (Wright, 2010); e
- *The contribution of ICT adoption to sustainability: households' perspective* (Ziemba, 2018).

O baixo número de artigos recuperados representa a incipiência da temática, e isso é corroborado pelo percentual ainda menor de trabalhos relevantes, demonstrando assim que a Ciência da Informação vem ocupando-se timidamente das questões aqui apresentadas.

Conclusões

A vista do exposto, fica evidente que existe a necessidade de aprimoramento das competências digitais que se relacionam com a proteção de dados e o direito à privacidade, as quais, evidentemente, são essenciais para o desempenho da vida cotidiana contemporânea. Em relação ao conteúdo do DigComp 2.2, pode-se atribuir ao documento a característica de um ponto de partida o qual oferece direcionamentos para o desenvolvimento de ações que visam o aprimoramento de competências digitais focadas na proteção de dados e privacidade, em qualquer nível. Todavia, ressalta-se a necessidade de ampliação do escopo, visando não somente soluções focadas nos indivíduos.

Em relação à abordagem da Ciência da Informação sobre a temática, os resultados obtidos evidenciam que pouco tem sido explorado sobre o tema no campo. Desse modo, é necessário uma nova investigação, em bases de dados que incluam uma gama maior de fontes, tais como SCOPUS e *Web of Science* e/ou a partir de termos que representem melhor a temática.

Referências

AFFONSO, E. P. **A insciência do usuário na fase de coleta de dados:** privacidade em foco. 325 f. 2018. Tese (Doutorado) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2018.

AIROLA, E. Learning and Use of eHealth Among Older Adults Living at Home in Rural and Nonrural Settings: Systematic Review. **Journal of Medical Internet Research**, Toronto, v. 23, n. 12, p. e23804, 2 dez. 2021.

BELLOVIN, S. **Where Did "Data Shadow" Come From?.** CircleID, June 2021. Disponível em: https://circleid.com/posts/20210629-where-did-data-shadow-come-from. Acesso em: 9 jan. 2023.

BLASCO-BLASCO, O.; RODRÍGUEZ-CASTRO, M.; TÚÑEZ-LÓPEZ, M. Indicadores compuestos como metodología innovadora en Comunicación. Aplicación para la evaluación de los medios públicos europeos. **Profesional de la información**, España, v. 29, n. 4, 27 ago. 2020.

CASTELLS, M. **The Rise of the Network Society**. 2. ed. Oxford: Wiley-blackwell, 2009.

GLUBOKOVA, N. *et al*. Formation of the Business Model of Crypto Asset Management. **Webology**, v. 18, special issue on Computing Technology and Information Management, p. 1292–1310, 2021.

HARVEY, D. **Condição pós-moderna**: uma pesquisa sobre as origens da mudança cultural. São Paulo: Loyola, 1992.

LONCAR-TURUKALO, T. *et al*. Literature on Wearable Technology for Connected Health: Scoping Review of Research Trends, Advances, and Barriers. **Journal of Medical Internet Research**, Toronto, v. 21, n. 9, p. e14017, 5 set. 2019.

LONGHINI, J.; ROSSETTINI, G.; PALESE, A. Digital Health Competencies Among Health Care Professionals: Systematic Review. **Journal of Medical Internet Research**, Toronto, v. 24, n. 8, p. e36414, 18 ago. 2022.

MARTZOUKOU, K. *et al*. A study of higher education students' self-perceived digital competences for learning and everyday life online participation. **Journal of Documentation**, Bingley, v. 76, n. 6, p. 1413–1458, 1 Jan. 2020.

MASUR, P. K. How online privacy literacy supports self-data protection and self-determination in the age of information. **Media and Communication**, Lisbon, v. 8, n. 2, p. 258–269, 2020.

MAYER-SCHÖNBERGER, V.; RAMGE, T. **Reinventing Capitalism in the age of Big Data**. Nova Iorque: Basic Books, 2018.

NOAIN-SÁNCHEZ, A. "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. **Journal of Information, Communication and Ethics in Society**, Bingley, v. 14, n. 2, p. 124–138, 1 Jan. 2016.

OH, S. S. *et al*. Measurement of Digital Literacy Among Older Adults: Systematic Review. **Journal of Medical Internet Research**, Toronto, v. 23, n. 2, p. e26145, 3 fev. 2021.

RODRIGUEZ, K.; ALIMONTI, V. **Un panorama retrospectivo y futuro de la protección de datos en América Latina y España**. Disponível em: https://www.eff.org/es/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain. Acesso em: 29 jan. 2021.

SELJELID, B. *et al*. A Digital Patient-Provider Communication Intervention (InvolveMe): Qualitative Study on the Implementation Preparation Based on Identified Facilitators and Barriers. **Journal of Medical Internet Research**, Toronto, v. 23, n. 4, p. e22399, 8 abr. 2021.

UNCTAD. **Data Protection and Privacy Legislation Worldwide | UNCTAD**. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 28 jan. 2021.

VARELA-OROL, C.; AMENEIROS RODRÍGUEZ, R. La protección de datos personales en las bibliotecas universitarias españolas en el entorno digital. **Revista general de información y documentación**, Madrid, v. 28, n. 2, p. 685–702, 2018.

VÉLIZ, C. **Privacy is Power**: why and how you should take back control of your data. London: Bantam Press, 2021.

VUORIKARI, R.; KLUZER, S.; PUNIE, Y. **DigComp 2.2**: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes. Disponível em: https://publications.jrc.ec.europa.eu/repository/handle/JRC128415. Acesso em: 9 jan. 2023.

WESTIN, A. **Privacy and Freedom**. Nova York: Ig Publishing, 1967.

WRIGHT, D. Structuring stakeholder e-inclusion needs. **Journal of Information, Communication and Ethics in Society**, Bingley, v. 8, n. 2, p. 178–205, 1 Jan. 2010.

ZIEMBA, E. The contribution of ICT adoption to sustainability: households' perspective. **Information Technology & People**, Bingley, v. 32, n. 3, p. 731–753, 1 Jan. 2018.

ZUBOFF, S. **A era do Capitalismo de Vigilância**. Rio de Janeiro: Editora Intrínseca, 2021.