LOGEION
Filosofia da Informação

ARTIGO

DOI: https://doi.org/10.21728/logeion.2023v9n2.p124-143

CIÊNCIA DA INFORMAÇÃO E PRIVACY BY DESIGN
aspectos éticos e possibilidades de pesquisa

Jonas Ferrigolo Melo[1]
Universidade do Porto
jonasferrigolo@gmail.com

Moisés Rockembach[2]
Universidade Federal do Rio Grande do Sul
moises.rockembach@ufrgs.br

Armando Malheiro da Silva[3]
Universidade do Porto
armando.malheiro@gmail.com

Resumo

Este artigo apresenta o mapeamento das possibilidades de pesquisa no âmbito da Ciência da Informação (CI) que tratam sobre o conceito de *Privacy by Design* (PbD). Se busca responder como a CI e os usos da teoria do PbD podem influenciar no alcance de maior privacidade aos usuários de sistemas de informação desde a concepção de produtos científicos até a pesquisa aplicada. Para responder esta pergunta, foram analisados 202 artigos,que balizaram a composição do mapa de possibilidades de pesquisa. O mapeamento abrange temas como o controle e o acesso aos dados, privacidade como um bem social e a visão de que a privacidade toma forma de acordo com as tecnologias. Foram problematizados os aspectos éticos da privacidade no ambiente tecnológico e contextualizada a presença do conceito de PbD nas legislações de proteção de dados. Conclui-se que este estudo contribui ao reunir proposições para o ponto de partida na busca por pesquisas científicas transdisciplinares em CI e privacidade, que os profissionais de CI podem estar envolvidos na observância da privacidade em todas as camadas de negócio no desenvolvimento de sistemas, e que a área pode contribuir com os debates relacionados ao PbD em razão da privacidade ser bem social fundamental.

Palavras-chave: Privacy by Design. Proteção de dados. Capitalismo da Vigilância. Ética da informação. Privacidade.

INFORMATION SCIENCE AND PRIVACY BY DESIGN
Ethical aspects and research possibilities

Abstract

This paper presents a mapping of research possibilities in the field of Information Science that deal with the concept of Privacy by Design (PbD). It seeks to answer how Information Science and the uses of PbD theory can influence the achievement of greater privacy for users of information systems, from the conception of scientific products to applied research. To answer this question, 202 articles were analyzed, which guided the composition of the map of research possibilities. The mapping covers topics such as data control and access, privacy as a social good, and the view that privacy takes shape according to technologies. The ethical aspects of privacy in the technological environment were problematized and the presence of the concept of PbD in data protection legislation was contextualized. It is concluded that this study contributes by gathering propositions for the starting point in the search for transdisciplinary scientific research in Information Science and privacy, and the professionals can be involved in the observance of privacy in all layers of business in the development of systems, and that the area can contribute to the debates related to PbD because privacy is a fundamental social good.

Keywords: Privacy by Design. Data protection. Surveillance Capitalism. Information ethic. Privacy.

1 Doutorando em Informação e Comunicação em Plataformas Digital, na Universidade do Porto.
2 Prof. Dr. em Ciência da Informação na Universidade Federal do Rio Grande do Sul.
3 Prof. Dr. em Ciência da Informação na Universidade do Porto.

1 INTRODUÇÃO

A crescente utilização de meios de comunicação e informação com alto grau de mobilidade e o uso cada vez maior da Internet demarcam novos desafios para a sociedade contemporânea. A forma como as pessoas fazem suas compras, pagamentos ou mesmo como a vida social é organizada implica no armazenamento e no uso de uma quantidade desconhecida de dados pessoais (ROMANOU, 2018). As tecnologias da infocomunicação[4] estão cada vez mais interconectadas e o volume de informações pessoais coletadas eclodiu, tornando evidente a necessidade de pensar sobre privacidade. Neste cenário repleto de dados e informações em diferentes fontes, suportes e formatos, vem emergindo novos nichos de estudos relacionados à privacidade no ambiente digital, que assim como as tecnologias que moldam a sociedade contemporânea, os estudos sobre privacidade devem renovar e aprimorar continuamente sua abordagem.

Floridi (2014) e Taylor et al. (2016), argumentaram que a pesquisa em privacidade priorizou a preocupação com os direitos individuais em relação às ameaças externas, de grupos poderosos com interesses, tais como o estado ou corporações privadas. Essa lógica criou uma preferência ontológica pelos direitos individuais em relação aos direitos dos grupos (ANDREW; BAKER, 2021). Os conceitos de privacidade vão ao encontro desta preferência na busca por assegurar a privacidade como um direito fundamental, essencial para a liberdade, para a democracia, para o bem-estar psicológico, individualidade e a criatividade (SOLOVE, 2008).

De acordo com a Declaração Universal dos Direitos Humanos das Nações Unidas, de 1948, “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência […]” (ASSEMBLY, 1948, artigo 12). Da mesma forma, a Carta dos Direitos Fundamentais da União Europeia (UNIÃO EUROPEIA, 2007), trata do direito ao “Respeito pela vida familiar e privada” (artigo 7º) e à “Proteção dos dados pessoais” (artigo 8º). E, assim, parece haver um consenso mundial sobre a importância da privacidade e a necessidade de sua proteção – ao menos na parte ocidental do Globo.

Assume-se, portanto, que a privacidade apoia a liberdade, a dignidade, a autonomia, a justiça e a democracia (WAHLSTROM; ULHAQ; BURMEISTER, 2020) e dada sua importância, seu panorama continua a evoluir. E, nesse sentido, o respeito e a proteção da

[4] Infocomunicação é um termo cunhado a partir de diferentes e complementares abordagens científicas compondo novos significados conceituais para ciências da informação e da comunicação. O conceito busca criar e explicitar os parâmetros de um novo campo disciplinar em construção, assumindo um diálogo e uma prática interdisciplinares e a construção de um objeto científico decorrentes das dinâmicas profissionais (Ribeiro and Silva, 2019; Passarelli, Silva and Ramos, 2014).

privacidade é a pedra angular da dignidade das pessoas e do livre arbítrio, e uma prioridade em toda a sociedade democrática (ROMANOU, 2018).

Com base nessa prerrogativa, pode-se tentar assegurar a privacidade, especialmente com a iminência de que invasões de estatais podem representar uma ameaça aos fundamentos culturais da esfera civil (ALEXANDER; SMITH, 1993). Além disso, as invasões corporativas de privacidade são consistentes com a ascensão da economia de dados e dos sistemas neoliberais de governança (FOUCAULT; DAVIDSON; BURCHELL, 2008). Com a ascensão de uma sociedade digitalmente conectada, ao lado de tendências de privatização e limitação do papel do Estado, essa diferença entre os atores torna-se cada vez mais relevante para entender como os indivíduos percebem a privacidade e as ameaças dela em seu cotidiano (CONNOR; DOAN, 2021). É por meio do desenvolvimento do "direito à privacidade" como um direito fundamental que se percebe que a necessidade funcional levou ao desdobramento da privacidade em doutrinas legislativa, jurídica (DONEDA, 2020) e científica.

Na busca pela defesa deste direito fundamental, e por meio de diferentes Tecnologias de Aprimoramento de Privacidade, conhecidas como PETs (*Privacy Enhancing Technologies*), procura-se amenizar as preocupações dos usuários em relação à privacidade no ambiente digital. Isso se dá por meio da implementação de um conjunto de princípios, tais como limitações na coleta de dados, especificação de quais dados estão sendo coletados, e avisos aos usuários sobre o processamento de seus dados. Disso emerge uma abordagem na tentativa de assegurar a privacidade dos cidadãos e a proteção de dados pessoais na sociedade moderna da informação chamada de *Privacy by Design* (PbD). A abordagem PbD pode ser brevemente explicada como a implementação de princípios de privacidade diretamente nas especificações do projeto dos sistemas tecnológicos, de forma que as regras de privacidade sejam incorporadas nas operações e na gestão do processamento de dados.

Este artigo tem como objetivo mapear possíveis relações em torno do PbD no âmbito da Ciência da Informação (CI) a partir do seguinte questionamento: como a CI e os usos da teoria do *Privacy by Design* podem influenciar no alcance de maior privacidade aos usuários de sistemas de informação desde a concepção de produtos científicos ou na pesquisa aplicada. Para alcançar o objetivo, foram analisados 202 artigos da área da Ciência da Informação que abordam a teoria do PbD. A pesquisa também se apoia nas legislações de proteção de dados para sustentação teórica.

Se pretende com essa contribuição incentivar a promoção do conhecimento sobre a privacidade no âmbito da CI, considerando que a informação e as tecnologias são essenciais para os processos infocomunicacionais. Além disso, é necessário garantir a privacidade na

busca por um desenvolvimento pleno da sociedade, em alinhamento com os objetivos da Agenda 2030 da Organização das Nações Unidas. Para isso, o artigo abordará a privacidade à luz da ética da informação; o conceito de *Privacy by Design* e as legislações de proteção de dados; e o *Privacy by Design* aplicado à CI.

2 PROCEDIMENTOS METODOLÓGICOS

O ponto de partida para identificar as possíveis relações entre *Privacy by Design* e CI advém da seguinte questão: como a CI e os usos do Privacy by Design, desde a concepção de produtos científicos ou na pesquisa aplicada, podem influenciar no alcance de maior privacidade aos usuários de sistemas de informação? Por sua vez, o objetivo geral foi mapear possíveis relações em torno do PbD no âmbito da CI com base na análise bibliográfica sobre o tema.

Para isso, elegeu-se como fonte as bases de dados *Web of Science* (WoS) e *Scopus*. A escolha das plataformas justifica-se por serem as maiores bases de referências bibliográficas de literatura científica revisadas por pares e por apresentarem um grande número de artigos científicos na área da CI. A busca nas plataformas utilizou como filtro *Article*, *Conference Paper* e *Reviews*, publicados nos últimos 5 anos, em inglês, que veiculassem o termo "*Privacy by Design*". Os parâmetros completos da pesquisa estão sistematizados no Quadro 1. Ao fim do processo de seleção, o estudo se pautou na análise de 202 artigos. Para fins de compreensão das temáticas foram utilizados recursos metodológicos tais como planilhas, nuvem de palavras, análise de frequência e mapa conceitual.

Quadro 1 – Parâmetros de pesquisa

Objetivo	Identificar os artigos publicados sobre "Privacy by Design".
Âmbito da pesquisa	Scopus e Web of Science
Data da pesquisa	Agosto de 2022
Equações da pesquisa	Na Scopus: TITLE AND ABSTRACT (privacy by design) AND PUBYEAR > 2017 AND PUBYEAR < 2021 Na WoS: Title AND Abstract (privacy by design), de 2017 a 2021
Critérios de inclusão	Article, Conference Paper e Reviews publicados entre Janeiro de 2017 e 2021
Critérios de exclusão	Literatura cinzenta, capítulos de livros, monografias, dissertações, teses, artigos que não estivessem relacionados a temática da pesquisa, artigos repetidos, e artigos não redigidos em inglês.
Critérios de validade metodológica	Dupla checagem, verificação manual dos critérios de inclusão e exclusão.
Resultados	Registro dos procedimentos metodológicos e descrição da pesquisa e seus resultados.
Tratamento dos dados	Sistematização em planilhas e uso do *softwareMonkeylearn*.

Fonte: Elaborado pelos autores.

Em relação à abordagem, essa pesquisa é classificada como exploratória-descritiva, ao proporcionar familiaridade com o problema proposto, com a intenção de torná-lo mais explícito, além disso, descreve as características que suportam o fenômeno da privacidade no ambiente digital e do *Privacy by Design*, incorporando os problemas éticos-epistemológicos advindos deste conhecimento científico. Antonio Carlos Gil (2002, p. 42), diz que "As pesquisas descritivas são, juntamente com as exploratórias, as que habitualmente realizam os pesquisadores sociais preocupados com a atuação prática". A pesquisa utiliza-se de métodos mistos, em razão dos dados terem sido analisados quali e quantitativamente. Como procedimentos técnicos, foi adotada a pesquisa bibliográfica.

3 PRIVACIDADE À LUZ DA ÉTICA DA INFORMAÇÃO

A privacidade possui um caráter polissêmico, no sentido em que seu conceito é composto por diferentes significados e, portanto, é relevante compreender a amplitude do termona tentativa de uma melhor compreensão do fenômeno. Solove (2008), no clássico *Understanding Privacy*, diz que ao buscar por uma conclusão definitiva reconheceu que "[…] a privacidade é uma pluralidade de coisas diferentes e que a busca por uma essência singular leva a um beco sem saída" (2008, prefácio), concluindo, portanto, que a privacidade "[…] deve ser mapeada como terreno, estudando minuciosamente a paisagem"(2008).

Young (1978) destaca que é mais fácil reconhecer o direito da privacidade do que descrevê-lo. Os obstáculos que impedem a construção de um conceito único para privacidade foram detalhados no relatório da Comissão do Governo Britânico sobre Privacidade, em 1972, descritos por MacNeil (2019):

> Primeiramente, dentre as 'coisas' que sentimos a necessidade de preservar dos curiosos olhares alheios estão os sentimentos, crenças ou questões de conduta, os quais são, essencialmente, irracionais; em segundo lugar, o escopo da privacidade é estipulado, em grande parte, por padrões e costumes de determinada sociedade, sendo esses padrões sujeitos a constantes mudanças. O Relatório Yunger concluiu que o 'conceito de privacidade não pode ser definido satisfatoriamente' […].(MACNEIL, 2019, p. 25–26).

Na busca por uma compreensão do termo, alguns excertos foram levantados e são utilizados atualmente para argumentar e descrever sobre a temática. O juiz da Suprema Corte dos EUA, Louis Brandeis, o declarou como "o mais abrangente dos direitos e o direito mais valorizado pelos homens civilizados"; outros o declaram como "essencial para um governo

democrático", crítico para "nossa capacidade de criar e manter diferentes tipos de relações sociais com pessoas diferentes", necessário para "permitir e proteger uma vida autônoma" e importante para "tranquilidade emocional e psicológica"; foi citado como "parte integrante de nossa humanidade", o "coração de nossa liberdade" e "o início de toda liberdade" (SOLOVE, 2008).

Muito antes destas tentativas de definir privacidade, em 1890, Warren e Brandeis publicaram o artigo "The Right to Privacy"[5]. Nesse artigo, que se tornou um marco no direito estadunidense, a privacidade foi explorada como um direito legal, sendo definida como uma proteção de um indivíduo e seu direito de "ser deixado em paz"[6].

De acordo com essas conceituações, pode-se deduzir que uma divulgação voluntária sobre si mesmo não envolveria uma perda de privacidade, uma vez que essa divulgação poderia ser considerada como um exercício de controle, ao invés de uma perda de controle. A definição de privacidade de Shils (1966, p. 286) reforça essa noção: "[…] a privacidade existe quando indivíduos, cujas ações geram ou se tornam objetos de informação, logram manter a posse dessa informação; e quando qualquer fluxo dessa informação em direção externa, desencadeado pelos indivíduos aos quais ela se refere [...] ocorre por iniciativa de quem detém sua posse […]". A privacidade é, portanto, um conceito fluído, variável com relação ao país e aos grupos culturais ou espaços de informação (GUIMARÃES et al., 2019), transcorrendo pela relação multidisciplinar que envolve cultura, geografia, liberdade, segurança, direito e outras áreas.

Rafael Capurro diz que "um dos principais dilemas ético-epistemológicos da era da informação é a relação entre liberdade e segurança" (SCHNEIDER; SALDANHA, 2015, p. 326). Hoje em dia, a privacidade está sob pressão crescente de diferentes forças, incluindo redes sociais online e serviços oferecidos por governos e empresas, altamente individualizados e dependentes de informações (CAVOUKIAN, 2010). Numa tentativa de o Estado democrático defender a segurança da sociedade por meio da vigilância, faz com que o próprio Estado de direito entre em conflito com o estabelecido pela Constituição, que é facilitar o exercício das liberdades individuais. Assim como existe este dilema ético-epistemológico, há de se observar, também, a recolha de dados pessoais de forma massiva, não apenas por agentes estatais, mas também por agentes privados (SCHNEIDER; SALDANHA, 2015), o que pode conduzir a graves conflitos de direito à privacidade.

---

5 Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. https://doi.org/10.2307/1321160.

6 A noção do "direito de ser deixado em paz" foi primeiramente desenvolvida por Thomas M. Cooley, *The right to be let alone*, Torts 29, 2. ed., 1888.

Nesse sentido, é prudente perceber que Capurro (2005) entende a privacidade sob a denominação de “autonomia informacional”, que consiste no poder do indivíduo em escolher o uso da informação no ambiente digital. E, portanto, o indivíduo tem a liberdade no processo de escolha que compreende desde a busca e seleção, até ao efetivo uso da informação (SILVA; ARAÚJO; PAULA, 2020). A partir do momento em que a autonomia dos indivíduos é infringida, tem-se a violação de sua própria liberdade. Capurro, Eldred e Nagel (2012, p. 79), dizem que “[...] a autonomia de proteção da privacidade é a base da liberdade, e não o contrário”.

Como acontece com muitas discussões sobre ética ou raciocínio moral, determinações específicas são complicadas em razão da possibilidade da existência de direitos conflitantes (BASKERVILLE; DULIPOVICI, 2006). De acordo com a teoria da privacidade dos dados pessoais, os indivíduos têm o direito de proteger o seu conhecimento pessoal, e as instituições de tratamento destes dados devem ter autorização dos titulares para o tratamento e compartilhamento deste conteúdo coletado (CHOWDHURY et al., 2018).

Entretanto, neste cenário é comum perceber o problema da assimetria de informações (ACQUISTI; GROSS, 2006; BORGESIUS, 2015; METCALF; CRAWFORD, 2016; UR et al., 2012) entre empresas e titulares de dados. Os titulares raramente sabem o que uma empresa faz com seus dados pessoais e é difícil prever as consequências dos seus usos futuros(BORGESIUS, 2015). Para os usuários é mais difícil ainda detectar se seus dados estão sendo capturados durante uma visita ao website, mesmo que se saiba que as pessoas são rastreadas para segmentação comportamental em praticamente todos os websites populares (VILA; GREENSTADT; MOLNAR, 2003).

Essa compreensão se dá ao perceber que as tecnologias são cada vez mais capazes de inferir informações pessoais ou comportamentais e, portanto, o conhecimento de atividades e tendências individuais pode ser acumulado sem violar, necessariamente, problemas de privacidade (ZUBOFF, 2019). Ao operar fora das leis de privacidade, os dados comportamentais representam uma frente de preocupação para estudiosos como Zuboff (2015, 2019), que denominam a coleta desses dados de "capitalismo de vigilância". Em essência, para Zuboff (2019, p. 8), o capitalismo de vigilância é "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para que práticas comerciais ocultas de extração, previsão e modificação comportamental possam ocorrer". Esse capitalismo é facilitado pelo uso do *Big Data*, e não se trata de um programa controlado pelo Estado que observa indivíduos, mas um mercado, onde dados comportamentais e de produtos com previsões que antecipam o que se fará agora, em breve e depois (ZUBOFF, 2019, p. 14).

Aqui, a questão ética de Zuboff com o capitalismo de vigilância não está primariamente relacionada à privacidade, mas sim às possíveis mudanças de comportamento que essas mercadorias são capazes de proporcionar. Nesse sentido, talvez, o mais importante nas provocações trazidas pelo capitalismo da vigilância, não sejam os processos que buscam conhecer os utilizadores, mas especialmente aqueles processos que busquem moldar o comportamento em escala.

Essa abordagem apresenta desafios éticos complexos e, para alguns, a privacidade pode ser uma impossibilidade na era do *Big Data*, em que os métodos de coleta e análise podem superar até mesmo a capacidade do consumidor mais informado de proteger informações confidenciais (ALLEN, 2011, 2016) e o seu uso indevido pode criar problemas significativos de privacidade (PARKER; PINE; ERNST, 2018).

Um conflito de interesses e direitos surge nos ambientes organizacionais como um conflito econômico, afinal os dados se tornaram um ativo valioso na economia contemporânea, equivocadamente[7] considerado como o petróleo do século 21 (ECONOMIST, 2017; LEMOS, 2014), que não só está alimentando o sucesso dos gigantes da tecnologia, mas também impulsionando a inovação e o crescimento econômico. E, portanto, o compartilhamento do conhecimento advindo dos dados pessoais representa uma transferência de valor econômico do indivíduo para outros indivíduos ou organizações (BASKERVILLE; DULIPOVICI, 2006).

Portanto, mesmo com seu tratamento regido via legislações de proteção de dados, os dados pessoais e comportamentais têm o potencial de desempenhar um novo papel central na gestão da economia política (KITCHIN, 2014, p. 165) e levar ao que Zuboff (2015, 2019) se refere como uma perda de "reciprocidade entre as elites dominantes e a população, usurpando cada vez mais a capacidade dos indivíduos de tomar decisões".

A dimensão digital envolve a existência e obscurece a consciência de que além da integridade física, adequadamente protegida pela distância gerada pela ferramenta de TI, há riscos para a pessoa ligada à capacidade de um algoritmo se tornar uma chave por meio da qual escolhas e comportamentos são previstos e orientados em uma manipulação das mentes e da vontade imperceptível. O que entra em jogo é o necessário equilíbrio entre o respeito ao limite, vinculado ao exercício da liberdade e da dignidade da pessoa humana, e o exercício da iniciativa econômica privada.

---

[7] Essas metáforas que equiparam a datificação a outros processos extrativistas ajudam a obscurecer as relações de poder das *BigTechs* e outras ações de apropriação de dados pessoais para fins econômicos. Considerando que os "dados são o novo petróleo", significa que se trata de algo que pode ser extraído naturalmente, pois existe no "solo" da vida social. Entretanto, entendemos que essa metáfora deturpa a avaliação de uma apropriação indébita ou exploração que possa surgir do uso de dados.

A partir dessas provocações teóricas, e também com ações na vida cotidiana, se percebe a necessidade latente nas sociedades modernas em compreender a ética da informação no que diz respeito ao direito fundamental à privacidade. Isso porque a ética da informação tem se fortalecido cada vez mais em um cenário de uso intenso das Tecnologias da Informação e Comunicação (TICs). Não obstante, o direito de exigir respeito pela vida privada como garantia da liberdade individual está incluso nos princípios básicos previstos pela *European Convention for the Protection Human Rights and Fundamental Freedoms* (FUGAZZA; SALDANHA, 2017a). As TICs têm, portanto, um alto impacto nos mais diversos setores da sociedade contemporânea e, assim sendo, a ética da informação é atravessada por um viés intercultural ao ser marcada pelo pluralismo dos diferentes contextos culturais (SILVA; PALETTA, 2016).

A privacidade coexiste com outros requisitos críticos tais como a segurança, vigilância, funcionalidade, eficiência operacional, controle organizacional, processos de negócios e usabilidade (CAVOUKIAN, 2010). O repertório de questões neste âmbito, somado ao surgimento do controle de informações baseado em tecnologia, torna este cenário mais difícil de identificar, reconhecer, discutir e apontar possíveis caminhos de resolução dos problemas éticos. Acredita-se, entretanto, que a interconexão com essas disciplinas é necessária para se compreender o conjunto de problemas evocados pelo campo da ética no território das políticas de direito social e na participação cidadã crítica, segurança e privacidade.

4 PRIVACY BY DESIGN E AS LEGISLAÇÕES DE PROTEÇÃO DE DADOS

Por meio de algoritmos, as plataformas da web conseguiram mudar o comportamento *online* e *offline* de maneiras que são benéficas para seus próprios objetivos(LYON, 2014; ZUBOFF, 2019). Em um experimento de 2014, o *Facebook* não apenas foi capaz de influenciar diretamente a opinião de seus usuários através da alteração de seu *feed* de notícias, mas também descobriu que essas "manipulações" também afetavam a opinião de amigos e familiares conectados na mesma rede local (KRAMER; GUILLORY; HANCOCK, 2014). Desta forma, o valor dos serviços de publicidade de plataformas tecnológicas é o acesso a dados pessoais, algoritmos e técnicas de modificação comportamental.

Entretanto, os dados pessoais nem sempre são percebidos como uma propriedade da pessoa natural, muito menos como um ativo econômico que pode moldar o comportamento das pessoas. O relatório do *PEW Research Center* sobre as percepções do público em relação

à privacidade indica que 91% dos adultos norte-americanos acreditam que perderam o controle sobre seus dados pessoais (MADDEN et al., 2014). Neste cenário, passam a ganhar maior notoriedade os Regulamentos de Proteção de Dados que impõem às organizações mudanças radicais em relação à privacidade e a proteção dos dados dos cidadãos. O *General Data Protection Regulation* (GDPR) da União Europeia e a Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, por exemplo, impõem um determinado conjunto de requisitos aos controladores e processadores de dados. Esses requisitos não só oferecem mais controle aos titulares sobre os seus dados pessoais, mas também permitem transparência nas atividades de processamento.

Nesse sentido, indo ao encontro da temática no contexto tecnológico, o conceito de *data protection by design* veicula nas pesquisas em privacidade e tecnologia há cerca de 20 anos. Anne Cavoukian é uma das responsáveis pelo desenvolvimento do conceito *Privacy by Design*, cunhado desde a década de 90 e apresentado em 2009 durante a *31st International Conference of Data Protection and Privacy Commissioners* (CAVOUKIAN, 2010; HUSTINX, 2009). Na *32 st* edição da conferência, em 2010, o termo foi aceito pela comunidade científica, ocasião em que a *Resolution on Privacy by Design*[8] foi adotada.

A resolução parte do pressuposto que os avanços tecnológicos fizeram surgir desafios à privacidade, tanto no cumprimento das demandas legais por parte das empresas, quanto ao exercício da cidadania tendo os direitos de informação assegurados aos cidadãos. O documento reconhece a importância de incorporar os Princípios Fundamentais de Privacidade nos processos de concepção, funcionamento e gestão de sistemas, a fim de atingir um quadro de proteção integral no que diz respeito à proteção de dados, convidando as Autoridades de Proteção de Dados a promover a inclusão da PbD nas políticas e legislação sobre proteção de dados em seus respectivos Estados.

O conceito de PbD prescreve que a privacidade deve estar presente desde a concepção do projeto e funcionamento de um sistema ou negócio ultrapassando, inclusive, os limites tecnológicos de modo a atuar no âmbito operacional, nos processos de trabalho, nas estruturas de gestão, nos espaços físicos e na rede de infraestrutura. Nesse sentido, PbD é o próximo passo na evolução dos diálogos sobre privacidade (CAVOUKIAN, 2010).

Envolver-se nessa temática significa estar em proximidade com a tecnologia em todo o processo de concepção, ao passo que cada evolução é uma oportunidade de levar os valores fundamentais da privacidade à diante em sua base teórica e prática (CAVOUKIAN, 2010),

[8] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem (Israel). 2010 https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

alicerçando o essencial em um sistema de negócio, à luz das legislações que vigoram a respeito da privacidade dos dados pessoais (CAVOUKIAN; CHIBBA, 2016). Cavoukian (2010)defende que PbD se estende a uma trilogia composta por sistemas de TI; práticas de negócios responsáveis; e design físico e infraestrutura em rede.

O aprimoramento das tecnologias para privacidade desde a concepção dos sistemas permite-nos incorporar o tema em todas as camadas do negócio. Ao fazer isso, acredita-se que a PbD ajudará na criação de uma determinada cultura de privacidade (CAVOUKIAN, 2010). Esta cultura de privacidade surge à medida que as organizações passam a abordar a privacidade, não como uma conformidade, mas como uma questão de negócios (RUBINSTEIN, 2011).

O GDPR traz em seu núcleo o conceito de "proteção de dados por design e por padrão" (EUROPEAN PARLIAMENT, 2016). Ao instituir o tema na introdução dos artigos da GDPR, faz com que seja estabelecida uma reconfiguração geral em relação a regulamentação de dados. Em vez de compreender a proteção de dados como uma conformidade presente nas interações legislativas anteriores, a segurança é reposicionada como uma função central em torno de como os dados são coletados, armazenados e explorados, incorporando-os em suas bases operacionais (ZERLANG, 2017). O regulamento possibilita que sejam incorporados sistemas que considerem a privacidade como padrão, abrindo caminho para concretizar e consagrar a autonomia individual na arquitetura do sistema que coleta dados (MALGIERI; COMANDÉ, 2017). Mesmo antes do GDPR, Kiss and Szőke (2015) afirmavam que:

> A tecnologia pode, em conjunto, aumentar o nível de segurança dos dados e aumentar o nível de proteção das informações pessoais, definindo a proteção de dados pessoais como 'padrão' em diferentes serviços, tornando seu uso um dos elementos-chave de uma nova proposta europeia de legislação. (KISS; SZŐKE, 2015, p. 323).

Rubinstein(2011, p. 1411) diz que ao introduzir o conceito de PbD no regulamento de proteção de dados pessoais abre-se um importante caminho na formação de um novo quadro jurídico na União Europeia, como também no Canadá e nos EUA.

Ainda que o autor não tenha citado o Brasil, verifica-se que esse reflexo também chegou na legislação brasileira. A Lei Geral de Proteção de Dados (LGPD), em seu artigo 46, estabelece que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas que protejam os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação

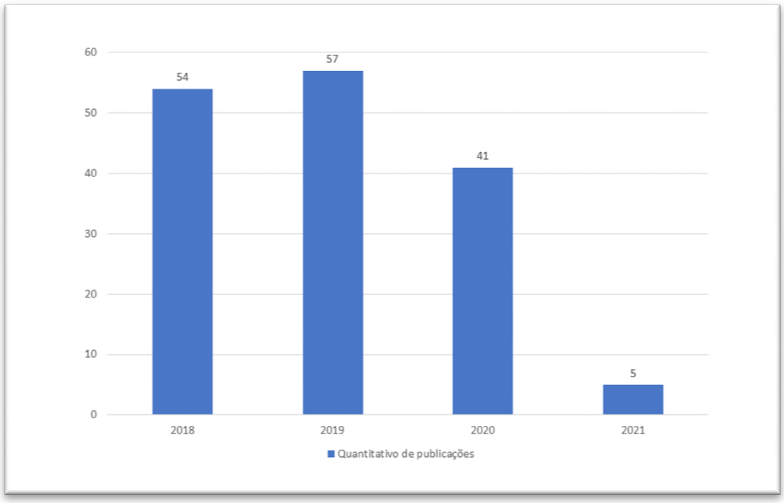
ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018, art. 46). Mais que esperar uma mudança de comportamento individual em prol de uma consciência em relação ao uso dos dados pessoais, os agentes de tratamento são condicionados a empreender esforços que coordenem ações de privacidade desde o início do projeto. Isso é a base do conceito de PbD.

O uso deste conceito objetiva restaurar o equilíbrio de poder entre os atores que desejam coletar informações pessoais no ambiente *online* e o indivíduo que deseja manter sua privacidade. Rockembach e Silva (2021) dizem que é imperativo discutir as características necessárias para que a sociedade respeite os valores éticos e legais relativos à privacidade dos dados e aos usos consentidos dos mesmos. Para isso, essas iniciativas precisam tornar a aplicação do conceito de PbD uma realidade prática e implementar estruturas de políticas destinadas a minimizar as ocasiões em que são tentadas violações de privacidade, restringindo certas práticas e proporcionando segurança do usuário a respeito da coleta de seus dados. O objetivo é que a privacidade do indivíduo seja protegida por padrão e os atos de transgressão possam ser tratados por meio de uma estrutura de políticas habilitadas pela implementação de mecanismos apropriados.

5 RELAÇÕES ENTRE PRIVACY BY DESIGN E A CIÊNCIA DA INFORMAÇÃO

Apresentamos aqui o resultado dos dados coletados da análise dos 202 artigos. Inicialmente, se verificou a quantidade de artigos publicados por ano analisado. Percebe-se que de 2017 a 2019 houve uma crescente de artigos publicados, entretanto nos anos seguintes, 2020 e 2021, nota-se uma queda de produções científicas sobre o tema. A GDPR entrou em vigor em 2016 e, portanto, a quantidade de artigos por ano, tende a demonstrar um maior interesse na temática logo após a publicação do GDPR. A Figura 1 sistematiza os dados coletados.

Figura1 – Quantidade de artigos publicados por ano



Fonte: Elaborado pelos autores.

Com base nos títulos e nos resumos dos artigos analisados foi gerada uma nuvem de palavras para verificar os cinquenta termos que mais veiculam nos documentos analisados. Para isso, foi utilizada a ferramenta *Monkeylearn*. É possível perceber que os termos, em sua maioria, estão no âmbito taxonômico da tecnologia e da legislação (Figura 2).

Figura 2 – Nuvem de palavras – título e resumo dos artigos

Fonte: Elaborado pelos autores.

O mesmo exercício de sintetização foi realizado com o conjunto de palavras-chave dos artigos selecionados (Figura 3). Pode-se perceber que os termos de maior destaque também

estão relacionados a taxonomia da tecnologia e das legislações de proteção de dados. Entretanto, na nuvem das palavras-chave se percebe o termo “ethics” dentre os destaques.

Figura 3 – Nuvem de palavras – palavras-chave dos artigos

Fonte: Elaborado pelos autores.

Esse resultado corrobora com outros estudos que mostram que na Ciência da Informação brasileira a privacidade vem sendo discutida em linhas de pesquisa relacionadas à ética epistemológica, economia da informação e na tecnologia (ARAÚJO, 2018; FUGAZZA; SALDANHA, 2017b; LOTT; CIANCONI, 2018; SANTOS NETO et al., 2017). Um exemplo disso são os trabalhos apresentados no GT 1 – Estudos Históricos e Epistemológicos da Ciência da Informação, GT 5 – Política e Economia da Informação (LOTT; CIANCONI, 2018) e, mais recentemente, no GT 8 – Informação e Tecnologia do Encontro Nacional de Pesquisa e Pós-graduação em Ciência da Informação – ENANCIB (SANTANA, 2021).

Pinheiro e Loureiro (1995)esboçaram um mapa conceitual com os campos interdisciplinares da ciência da informação, que foi aprofundado e atualizado por Pinheiro (2006). Esse mapa apresenta os principais teóricos e respectivas correntes de pensamento, a interdisciplinaridade e as dimensões tecnológica e social da CI. Por sua amplitude e por apresentarem a relação interdisciplinar da CI com outras áreas do conhecimento, entende-se que se trata de um material que auxilia na identificação de estudos que compreendem a área da CI, de modo que este estudo foi utilizado para realização das análises.

Da análise macro do conjunto de artigos selecionados, assim como a leitura dos resumos, foram extraídas as contribuições que nos levam a mapear possíveis relações em

torno do PbD no âmbito da CI. Essas possíveis relações foram estabelecidas ao comparar os temas que cada um dos artigos apresentava, com o mapa conceitual dos campos interdisciplinares da CI (PINHEIRO, 2006). Desta análise, resultou a seguinte relação de termos:*Information Privacy, Computer ethics, Ethics education, Ethics simulation, Privacy Law, Personal data, GDPR, Participatory design, Informed consent, Privacy Settings, Surveillance and control, Online Privacy, Risk assessment, Safety, Security and secure, Algorithmic accountability, Privacy and security, Practical implementation of Privacy by Design, Design of information systems, User experience in digital platforms*.

Os materiais analisados permitem outras relações, de modo que essa é uma das relações possíveis na pesquisa em PbD no âmbito da CI. As contribuições dos investigadores vão ao encontro da observação do fenômeno da informação e da necessidade da privacidade na concepção dos sistemas informacionais, e partem da observação da privacidade como um fenômeno global, que permeia desde uma ciência *mainstream*, advindo de uma tradição anglo-saxónica na CI(RODRIGUES; CARRIERI, 2001), até a desenvolvida na cartografia do Sul Global do sistema científico internacional (MÜLLER; DE SOUSA, 2021).

6 CONSIDERAÇÕES FINAIS

A pesquisa investigou, com base na produção científica composta por artigos de revista e de conferências e revisões de literatura, como a Ciência da Informação e os usos da teoria do *Privacy by Design* podem influenciar no alcance de maior privacidade aos usuários de sistemas de informação desde a concepção de produtos científicos ou na pesquisa aplicada. Com este ponto de partida foram analisados 202 artigos que tendo seus dados minerados, contribuíram para alcançar o objetivo geral desta pesquisa, qual seja, mapear possíveis relações em torno do PbD no âmbito da CI.

Considerando que a privacidade é um bem social fundamental, conclui-se que pensar a privacidade desde a concepção é fundamental pois apoia a liberdade, dignidade, autonomia, justiça e a democracia e, portanto, é relevante que seja estudada de várias vertentes ontológicas. Algumas das atividades clássicas da CI, tais como gestão da informação e governança, por exemplo, têm criado desafios em relação à privacidade para muitas empresas e organizações, pois a informação é vista como um ativo econômico estratégico e está no cerne do debate legislativo com o advento e incremento das leis gerais de proteção de dados pessoais.

As possibilidades de pesquisa abrangem diversos temas que permeiam a CI e o PbD, incluindo o controle e o acesso aos dados, privacidade como um bem social e a visão de que a privacidade toma forma de acordo com as tecnologias. Assuntos estreitamente relacionados com a tecnologia e desenvolvimento de plataformas também permeiam as possibilidades de pesquisa. Destaca-se, também, que a observância da privacidade em todas as camadas de negócio no desenvolvimento de sistemas, bem como sua aplicação como um valor a ser seguido pelos profissionais da Ciência da Informação, pode facilitar a implementação efetiva dos objetivos da Agenda das Nações Unidas para 2030.

O trabalho trouxe contribuições para que se possa compreender o estado atual de investigação no que concerne ao *Privacy by Design* na Ciência da Informação. Espera-se que essa pesquisa oriente a construção de estudos que reconheçam a inter e a transdisciplinaridade e a complexidade das relações entre diferentes campos científicos e disciplinas. Apresenta-se, portanto, uma contribuição técnica e científica ao reunir proposições para um ponto de partida na busca por pesquisas que relacionem CI e PbD.

REFERÊNCIAS

ACQUISTI, A.; GROSS, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Em: [s.l: s.n.]. p. 36–58.

ALEXANDER, J. C.; SMITH, P. The discourse of American civil society: A new proposal for cultural studies. **Theory and society**, p. 151–207, 1993.

ALLEN, A. L. **Unpopular privacy: What must we hide?** [s.l.] Oxford University Press, 2011.

ALLEN, A. L. Protecting one's own privacy in a big data economy. **Harvard Law Review Forum**, v. 130, p. 71–80, 2016.

ANDREW, J.; BAKER, M. The general data protection regulation in the age of surveillance capitalism. **Journal of Business Ethics**, v. 168, n. 3, p. 565–578, 2021.

ARAÚJO, C. A. Á. Um mapa da ciência da informação: história, subáreas e paradigmas. **ConCI: convergências em ciência da informação**, v. 1, n. 1, p. 47–72, 2018.

ASSEMBLY, U. N. G. Universal declaration of human rights. **UN General Assembly**, v. 302, n. 2, p. 14–25, 1948.

BASKERVILLE, R.; DULIPOVICI, A. **The ethics of knowledge transfers and conversions: property or privacy rights?** Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). **Anais**...IEEE, 2006.

BORGESIUS, F. Z. Informed consent: We can do better to defend privacy. **IEEE Security and Privacy**, v. 13, n. 2, p. 103–107, 2015.

BRASIL. **Lei n. 13.708, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. BrasíliaPresidência da República, , 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 ago. 2022

CAPURRO, R. Privacy. An intercultural perspective. **Ethics and information technology**, v. 7, n. 1, p. 37–47, 2005.

CAPURRO, R.; ELDRED, M.; NAGEL, D. It and Privacy from an Ethical Perspective Digital Whoness: Identity, Privacy and Freedom in the Cyberworld171. Em: [s.l: s.n.]. p. 63–142.

CAVOUKIAN, A. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. **Identity in the Information Society**, v. 3, n. 2, p. 247–251, 2010.

CAVOUKIAN, A.; CHIBBA, M. Cognitive Cities, Big Data and Citizen Participation: The Essentials of Privacy and Security. Em: [s.l: s.n.]. p. 61–82.

CHOWDHURY, M. J. M. et al. Blockchain as a notarization service for data sharing with personal data store. In: **2018 17th ieee international conference on trust, security and privacy in computing and communications/12th ieee international conference on big data science and engineering (TrustCom/BigDataSE)**. IEEE, 2018. p. 1330-1335.

CONNOR, B. T.; DOAN, L. Government and corporate surveillance: moral discourse on privacy in the civil sphere. **Information, Communication & Society**, v. 24, n. 1, p. 52–68, 2021.

DONEDA, D. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados**. 2. ed. rev. e atual ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2020.

ECONOMIST, T. The world's most valuable resource is no longer oil, but data. **The Economist: New York, NY, USA**, 2017.

EUROPEAN PARLIAMENT. Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation. **Regulation (eu)**, v. 679, p. 2016, 2016.

FLORIDI, L. Open data, data protection, and group privacy. **Philosophy & Technology**, v. 27, n. 1, p. 1–3, 2014.

FOUCAULT, M.; DAVIDSON, A. I.; BURCHELL, G. **The birth of biopolitics: lectures at the Collège de France, 1978-1979**. [s.l.] Springer, 2008.

FUGAZZA, G. Q.; SALDANHA, G. S. Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, v. 22, n. 50, p. 91–101, 2017a.

GIL, A. C. **Como elaborar projetos de pesquisa**. [s.l.] Atlas São Paulo, 2002. v. 4

GUIMARÃES, J. A. C. et al. **Ethical Challenges in Archival Knowledge Organization: the description of personal data for long-term preservation**. The Human Position in an Artificial World: Creativity, Ethics and AI in Knowledge Organization. **Anais**...Ergon-Verlag, 2019.

HUSTINX, P. "Privacy by Design: The Definitive Workshop". n**. November**, 2009.

KISS, A.; SZŐKE, G. L. Evolution or revolution? Steps forward to a new generation of data protection regulation. Em: **Reforming European data protection law**. [s.l.] Springer, 2015. p. 311–331.

KITCHIN, R. **The data revolution: Big data, open data, data infrastructures and their consequences**. London: Sage, 2014.

KRAMER, A. D. I.; GUILLORY, J. E.; HANCOCK, J. T. Experimental evidence of massive-scale emotional contagion through social networks. **Proceedings of the National Academy of Sciences**, v. 111, n. 24, p. 8788–8790, 17 jun. 2014.

LEMOS, R. **"Ou sociedade acompanha internet ou democracia começa a ficar em xeque"**. Disponível em: <https://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/>. Acesso em: 3 mar. 2022.

LOTT, Y. M.; CIANCONI, R. DE B. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. **Perspectivas em Ciência da Informação**, v. 23, p. 117–132, 2018.

LYON, D. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, v. 1, n. 2, p. 205395171454186, 1 jul. 2014.

MACNEIL, H. **Sem consentimento: a ética na divulgação de informações pessoais em arquivos públicos**. Belo Horizonte: Editora UFMG, 2019.

MADDEN, M. et al. Public perceptions of privacy and security in the post-Snowden era. **Pew Research Center**, v. 12, 2014.

MALGIERI, G.; COMANDÉ, G. Why a right to legibility of automated decision-making exists in the general data protection regulation. **International Data Privacy Law**, 2017.

METCALF, J.; CRAWFORD, K. Where are human subjects in Big Data research? The emerging ethics divide. **Big Data & Society**, v. 3, n. 1, p. 205395171665021, 1 jun. 2016.

MÜLLER, J. P. M.; DE SOUSA, R. S. C. Cartografias Subalternas: travessias epistemológicas para a Ciência da Informação. **Liinc em Revista**, v. 17, n. 2, p. e5786–e5786, 2021.

PARKER, D. M.; PINE, S. G.; ERNST, Z. W. Privacy and informed consent for research in the age of big data. **Penn St. L. Rev.**, v. 123, p. 703, 2018.

PINHEIRO, L. V. R. Ciência da Informação: desdobramentos disciplinares, interdisciplinaridade e transdisciplinaridade. 2006.

PINHEIRO, L. V. R.; LOUREIRO, J. M. M. Traçados e limites da ciência da informação. **Ciência da informação**, v. 24, n. 1, 1995.

ROCKEMBACH, M.; DA SILVA, A. M. Web Data and the Relationship Between the General Data Protection Regulation in Europe and Brazil. Em: **Handbook of Research on Digital Transformation and Challenges to Data Security and Privacy**. [s.l.] IGI Global, 2021. p. 222–233.

RODRIGUES, S. B.; CARRIERI, A. DE P. A tradição anglo-saxônica nos estudos organizacionais brasileiros. **Revista de Administração Contemporânea**, v. 5, p. 81–102, 2001.

ROMANOU, A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. **Computer law & security review**, v. 34, n. 1, p. 99–110, 2018.

RUBINSTEIN, I. S. Regulating Privacy by Design. **Berkeley Technology Law Journal**, v. 26, 2011.

SANTANA, F. J. C. DE. **A Segurança da Informação na Ciência da Informação no Brasil**. [s.l: s.n.].

SANTOS NETO, J. A. DOS et al. Interdisciplinaridade no contexto da Ciência da Informação: correntes e questionamentos. **Em Questão**, p. 9–35, 2017.

SCHNEIDER, M.; SALDANHA, G. Entrevista com Rafael Capurro (07-10-2015). **Liinc em Revista**, v. 11, n. 2, 2015.

SHILS, E. Privacy: Its constitution and vicissitudes. **Law and Contemporary Problems**, v. 31, n. 2, p. 281–306, 1966.

SILVA, A. M. DA; ARAÚJO, E. P. O.; PAULA, C. P. A. DE. O Fyborg e a ética da informação ou os limites de uma ética antropocêntrica. **Revista UFMG**, v. 27, n. 1, p. 60–77, 2020.

SILVA, A. M. DA; PALETTA, F. C. **A ética da informação na era digital: desenho de uma experiência pedagógica no âmbito da cooperação científica luso-brasileira**. Descobrimentos da Ciência da Informação: desafios da Multi, Inter e Transdisciplinaridade (MIT) : XVII Encontro Nacional de Pesquisa em Ciência da Informação (ENANCIB). **Anais**...Faculdade de Letras, 2016. Disponível em: <https://repositorio-aberto.up.pt/handle/10216/90843>

SOLOVE, D. J. Understanding privacy. 2008.

TAYLOR, L.; FLORIDI, L.; VAN DER SLOOT, B. **Group privacy: New challenges of data technologies**. [s.l.] Springer, 2016. v. 126

UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia. **DIREITO E DEMOCRACIA**, p. 457, 2007.

UR, B. et al. **Smart, useful, scary, creepy**. Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12. **Anais**...New York, New York, USA: ACM Press, 2012.

VILA, T.; GREENSTADT, R.; MOLNAR, D. **Why we can't be bothered to read privacy policies models of privacy economics as a lemons market**. Proceedings of the 5th international conference on Electronic commerce - ICEC '03. **Anais**...New York, New York, USA: ACM Press, 2003.

WAHLSTROM, K.; ULHAQ, A.; BURMEISTER, O. Privacy by design: A Holochain exploration. **Australasian Journal of Information Systems**, v. 24, 2020.

YOUNG, J. B. **Privacy**. New York: Chichester , 1978.

ZERLANG, J. GDPR: a milestone in convergence for cyber-security and compliance. **Network Security**, v. 2017, n. 6, p. 8–11, 2017.

ZUBOFF, S. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, n. 1, p. 75–89, 2015.

ZUBOFF, S. **The age of surveillance capitalism: The fight for a human future at the new frontier of power**. [s.l.] Profile books, 2019.