XXII Encontro Nacional de Pesquisa em Ciência da Informação – XXII ENANCIB

ISSN 2177-3688

GT-8 – Informação e Tecnologia

CONTRIBUIÇÕES DA CIÊNCIA DA INFORMAÇÃO SOBRE TECNOLOGIAS APLICÁVEIS À PROTEÇÃO DA PRIVACIDADE NO AMBIENTE DIGITAL: UMA REVISÃO SISTEMÁTICA DE LITERATURA

INFORMATION SCIENCE CONTRIBUTIONS ON TECHNOLOGIES FOR PRIVACY PROTECTION IN THE DIGITAL ENVIRONMENT: A SYSTEMATIC LITERATURE REVIEW

Jonas Ferrigolo Melo. Univ. do Porto.

Moisés Rockembach. UFRGS.

Modalidade: Trabalho Completo

Resumo: Com o crescente uso de dispositivos e sensores inteligentes, enormes quantidades de dados estão sendo geradas continuamente. Esses dados são comumente armazenados em plataformas de nuvem centralizadas essencialmente para fins comerciais. E, sendo assim, os consumidores perderam o controle de seus próprios dados pessoais, fazendo com que a privacidade do usuário no ambiente digital possa ser exposta e utilizada indevidamente. Essa realidade deixa evidente a assimetria de informação entre titulares e controladores de dados. Essa revisão sistemática de literatura analisou 31 artigos sobre tecnologia e privacidade no âmbito da Ciência da Informação. Foi realizada uma pesquisa bibliográfica, apresentando análise qualitativa das abordagens tecnológicas utilizadas com a intenção de incrementar a privacidade no ambiente tecnológico. Foram identificadas as abordagens tecnológicas mais amplamente adotadas, que incluem a criptografia, pseudonimização, anonimização, *Privacy By Design* e o *Blockchain*. Também foi possível elencar projetos empíricos nesta perspectiva. Conclui-se que a tecnologia, por meio das abordagens identificadas, tem condições de conduzir o desenvolvimento de plataformas tecnológicas, contribuindo na conformidade com as legislações de proteção de dados; oportunizar que a privacidade do indivíduo seja protegida por padrão sem prejudicar os modelos de negócio dos controladores; e compensar o equilíbrio da assimetria de informação.

Palavras-Chave: Privacidade. Proteção de Dados. Privacy By Design. Blockchain.

Abstract: With the increasing use of smart devices and sensors, huge amounts of data are being generated continuously. This data is stored on centralized cloud platforms primarily for business purposes. Therefore, consumers have lost control of their own personal data, making user privacy in the technological environment always at stake. This reality makes evident the asymmetry of information between data subjects and controllers. This systematic literature review analyzed 31 articles on technology and privacy in the field of Information Science. Bibliographic research was carried out, presenting a qualitative analysis of the approaches, methodologies, and technological tools used to increase privacy in the technological environment. The analyzed articles present several technologies that improve user privacy. The most widely adopted include encryption, pseudonymization, anonymization, Privacy by Design, and the Blockchain. It was also possible to list

empirical projects from this perspective. It is concluded that technology can drive the development of technological platforms, contribute to compliance with data protection legislation; provide the opportunity for the privacy of the data subjects to be protected by default without harming the controllers' business models; and contribute to the balance of information asymmetry.

Keywords: Technology. Privacy. Data Protection. Privacy By Design. Blockchain.

1 INTRODUÇÃO

Estudos indicam que o uso de grandes conjuntos de dados, os chamados *Big Data*, pode ter resultados positivos na política social (BLUMENSTOCK; CADAMURO; ON, 2015), visando a identificação e o controle do comportamento criminoso (BERK, 2012), otimizando a prestação de cuidados médicos e outros serviços de saúde (OBERMEYER; EMANUEL, 2016), abordando a desigualdade e a pobreza (GLAESER et al., 2016, 2018) e incrementando cidades inteligentes que trazem benefícios à sociedade (FORESTI et al., 2020). Entretanto, ao mesmo tempo em que a quantidade de dados e a sofisticação das análises possibilitaram diversos ganhos, os riscos à privacidade aumentaram.

O fenômeno da vigilância moderna baseada em dados iniciou com o desenvolvimento do comércio pela Internet na década de 1990, introduzindo um "novo escopo e escala de rastreamento" e "práticas de coleta de dados" (WEST, 2019, p. 06), que foram refinados por algumas empresas estadunidenses como *Google* e *Facebook*. O acúmulo de informações pessoais por essas grandes organizações, por meio da vigilância digital, abre caminhos para os riscos com a privacidade (ANDREW; BAKER, 2021).

Embora a extração de recursos valiosos pelas corporações não seja uma prática nova, o que é novo na atual era do capitalismo de vigilância são as "reivindicações da experiência humana como matéria-prima gratuita para tradução em dados comportamentais" (ZUBOFF, 2019, p. 08). O valor econômico desse excedente comportamental é aumentado ainda mais quando combinado com inteligência de máquina, como algoritmos, que geram modelagem preditiva de atividades humanas (ZUBOFF, 2019, p. 74). Os dados comportamentais são coletados por um número crescente de dispositivos e aplicativos e, embora o público em geral possa estar ciente de que a *Alexa*, o *Google Home* e o *Google Maps* coletam seus dados pessoais, há menos consciência da extração contínua de padrões comportamentais detalhados (ANDREW; BAKER, 2021).

Da mesma forma que os recursos tecnológicos são utilizados para coleta e tratamento dos dados, também podem ser usados para incrementar e assegurar o tratamento legítimo

dos dados pessoais, contribuir com o cumprimento das legislações de proteção de dados, minimizando a chance de os responsáveis pelo tratamento serem sancionados por atividades ilegais de processamento (RUBINSTEIN, 2011) e reduzindo a assimetria informacional entre titulares e controladores de dados.

Com o advento das leis de proteção de dados e interesses contemporâneos no âmbito da ética da informação no ambiente digital, assim como a necessidade de desenvolver sistemas de informação que presem pela privacidade e segurança nas plataformas digitais, este artigo tem como objetivo identificar e demonstrar as abordagens tecnológicas utilizadas em ações com foco central na privacidade no âmbito das pesquisas em Ciência da Informação, a partir do seguinte questionamento: como a CI pode contribuir no alcance de maior privacidade aos usuários de sistemas de informação, no desenvolvimento de produtos científicos e na pesquisa aplicada. Para isso, foram analisados 31 artigos da área da Ciência da Informação que abordam a privacidade no ambiente digital, por meio de um Revisão Sistemática de Literatura (RSL). É apresentada uma análise qualitativa das abordagens tecnológicas utilizadas com a intenção de incrementar a privacidade no ambiente tecnológico, assim como são apresentados casos empíricos nessa perspectiva.

Este artigo é parte de uma revisão teórica relacionada à privacidade no ambiente digital e surgiu da necessidade de uma contribuição científica que consolidasse algumas das soluções tecnológicas utilizadas neste domínio. Acredita-se que essas abordagens podem ser utilizadas em conjunto para ampliar ainda mais a proteção da privacidade do utilizador de plataformas digitais. Também foi identificado que existes outras revisões de literatura sobre privacidade, mas sempre atreladas a uma temática específica, tal como Internet das Coisas, direito, ética, saúde e outros. Na CI, de modo geral, não foi identificada revisão de literatura sobre privacidade. Se percebe, também, que há poucos trabalhos sobre tecnologia e privacidade que contemplem profissionais da área da informação, sendo possível verificar que àqueles que atuam com Tecnologia são os que mais se envolvem neste tema. Entende-se, entretanto, que os profissionais da Ciência da Informação podem contribuir ativamente nesta área de pesquisa.

Se espera que essa contribuição demonstre que a CI e os profissionais da informação podem contribuir no desenvolvimento e na promoção do conhecimento sobre a privacidade no âmbito da CI, considerando que os ensinamentos advindos da área da informação são

essenciais na tecnologia, especialmente quando atrelada à proteção da privacidade, ensejando, inclusive uma mudança curricular na formação destes profissionais (MELO; ROCKEMBACH, 2019). Além disso, os objetivos da Agenda 2030 da Organização das Nações Unidas dizem que é necessário garantir a privacidade para alcançar um desenvolvimento pleno da sociedade. O artigo está dividido em Introdução; Procedimentos metodológicos; Abordagens tecnológicas para incremento da privacidade, onde são apresentados os resultados; e, Considerações finais.

2 PROCEDIMENTOS METODOLÓGICOS

A pesquisa se apoiou na metodologia de Revisão Sistemática de Literatura (RSL), um método de síntese de evidências que avalia criticamente e interpreta as pesquisas disponíveis para uma questão particular, área do conhecimento ou fenômeno de interesse (BRASIL; MINISTÉRIO DA SAÚDE, 2021), com o objetivo de identificar e demonstrar as abordagens tecnológicas utilizadas em ações com foco central na privacidade no âmbito das pesquisas em Ciência da Informação.

Para a realização desta pesquisa elegeu-se como fonte as bases de dados *Web of Science* (WoS) e *Scopus*. A escolha se deu em razão destas serem as maiores bases de referências bibliográficas de literatura científica revisada por pares e por apresentarem um grande número de artigos científicos na área da Ciência da Informação.

Para a definição da equação da pesquisa foram realizados testes nas plataformas elegidas e se percebeu que a recuperação não foi satisfatória em razão dos resultados terem apresentado centenas de artigos que não compreendiam o campo da Ciência da Informação. O melhor resultado encontrado foi ao utilizar o campo título. Deste modo, a equação de pesquisa consistiu na utilização combinada dos descritores *privacy AND technology AND information* no campo título.

Os critérios de elegibilidade: (i) artigos científicos; (ii) artigos redigidos em inglês; e (iii) publicados entre 2017 e 2021. Foram selecionados 50 artigos aos quais foram atribuídos outros critérios de exclusão: (i) artigos que não estivessem diretamente relacionados à temática de interesse; (ii) artigos em que não se teve acesso ao texto na íntegra; e (iii) artigos repetidos. Ao fim da aplicação dos critérios foram selecionados e analisados 31 artigos, dos quais foram extraídas as seguintes informações: *título*, *autor(es)*, *ano de publicação*, *número*

do DOI, *resumo* e *identificação se o artigo se relacionava com alguma abordagem tecnológica específica*. Os procedimentos metodológicos adotados estão sistematizados no *Quadro 1*.

A coleta dos dados se deu em maio de 2022 e revisados em agosto de 2022. A escolha dos campos descritores, assim como os procedimentos metodológicos foram definidos com base nos exemplos extraídos de Jesson; Matheson; Lacey (2011), e ajustados conforme a necessidade identificada pelos autores.

Quadro 1 - Procedimentos metodológicos para a Revisão Sistemática da Literatura

Objetivo	Identificar e demonstrar abordagens tecnológicas utilizadas em ações com foco central na privacidade
Âmbito da pesquisa	Scopus e Web of Science
Equações da pesquisa	**Na Scopus:** TITLE (privacy AND technology AND information) AND PUBYEAR > 2017 AND PUBYEAR < 2022 **Na WoS:** Título (privacy AND technology AND information), de 2018 a 2021
Critérios de inclusão	Artigos científicos 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, artigos em que não fosse possível acesso integral do texto, 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 *software Wordcloud*.

Fonte: Elaborado pelos autores.

A partir de então, se procedeu a leitura dos artigos com a intenção de extrair as informações sobre abordagens tecnológicas utilizadas em ações com foco central na privacidade. Também foram utilizadas ferramentas online de elaboração de nuvem de palavras, na tentativa de extrair informações generalizadas dos artigos que pudessem contribuir com a busca por resultados.

3 ABORDAGENS TECNOLÓGICAS PARA INCREMENTO DA PRIVACIDADE

Com base na leitura e tabulação dos dados, assim como a análise das imagens produzidas, foi possível identificar algumas das abordagens tecnológicas que estão mais presentes nos artigos analisados, quais sejam: *Privacy Enhancing Technologies* (PETs), anonimização, pseudonimização, *Privacy by Design* e *Blockchain*. Importante destacar que outras abordagens são descritas nos artigos, entretanto, para o interesse específico desta contribuição foram selecionadas para descrição detalhada aquelas com maior destaque.

Uma análise qualitativa é apresentada nas sessões a seguir que sistematizam os resultados encontrados, assim como são apresentados alguns dos casos empíricos presentes nos artigos selecionados. O referencial teórico se pautou pelos artigos analisados, assim como algumas das referências por eles utilizadas.

3.1 Tecnologias para aprimoramento da privacidade: *Privacy Enhancing Technologies*

Poullet (2010) diz que se a tecnologia é vista como o maior desafio para nossa privacidade, também pode ser a solução. O papel da tecnologia deve ser reavaliado e novos esforços de pesquisa devem ser dedicados para o desenvolvimento de sistemas que garantam a privacidade (POULLET, 2010). Com as PETs, as tecnologias podem ser utilizadas para melhorar a autonomia do titular, por exemplo, fornecendo meios para garantir a ocultação de seus dados pessoais ou, ainda, oferecer garantias no consentimento informado por meio de recursos computacionais.

Essas ferramentas tecnológicas também podem ser utilizadas nas relações com a legislação, seja fazendo cumprir ou facilitando o cumprimento dos compromissos legais dos controladores, desenvolvendo uma política de padronização de equipamentos que considerem os requisitos de privacidade (POULLET, 2010). As PETs podem ser qualquer meio tecnológico desenvolvido para atuar em ferramentas por meio de ações específicas com foco central na privacidade. A criptografia, por exemplo, aumenta a privacidade ao permitir que os aplicativos processem, armazenem e compartilhem dados criptografados em vez dos dados originais (JAVED et al., 2021). Já as técnicas de anonimização e pseudonimização são usadas para remover informações pessoais do conjunto de dados, permitindo que os titulares permaneçam não identificáveis (MAUGER; MAHEC; DEQUEN, 2020). A anonimização é completamente irreversível, enquanto a pseudonimização permite que o proprietário dos dados seja reidentificado.

A sumarização de dados, por sua vez, é a tarefa de encontrar um subconjunto representativo, com condições de ser gerenciável, em um grande conjunto de dados (MIRZASOLEIMAN; ZADIMOGHADDAM; KARBASI, 2016; TSCHIATSCHEK et al., 2014). Essa também não é aplicável a serviços personalizados, pois criam variantes resumidas de conjuntos de dados que ocultam as informações reais dos indivíduos (JAVED et al., 2021). Já o aprendizado descentralizado (JEON et al., 2021) permite que dados confidenciais sejam

descarregados para dispositivos do usuário final, onde o processamento será feito. Isso aumenta a privacidade eliminando o risco de exposição de dados confidenciais.

As técnicas de privacidade diferencial permitem coletar e compartilhar informações de vários usuários de forma desordenada, mantendo a privacidade dos usuários individuais. Ainda que seja uma técnica que preserva a privacidade individual, a quantidade de ruído adicionado impacta fortemente a precisão e exatidão dos dados (ELSALAMOUNY; GAMBS, 2016). Além disso, os dados que forem tratados por meio da privacidade diferencial não poderão ser utilizados para serviços personalizados.

3.2 *Privacy by Design*

Anne Cavoukian é uma das responsáveis pelo desenvolvimento do conceito de *Privacy by Design* (PbD), 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 32ª edição da conferência, em 2010, o termo foi aceito pela comunidade científica, ocasião em que a *Resolution on Privacy by Design* (COMMISSIONERS, 2010) 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 (DAVIES, 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), alicerçando o essencial em um sistema de negócio, à luz das legislações que vigoram a respeito da privacidade dos dados pessoais (CAVOUKIAN; CHIBBA, 2016).

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.

O PbD e os PETs podem ser confundidos em razão de seus objetivos estarem ambos ligados ao *background* tecnológico do processamento de dados, mas não são sinônimos. Apesar da sobreposição em relação ao seu uso, os PETs são abordagens claras de engenharia que focam no potencial positivo da tecnologia, em ferramentas usadas para manter o anonimato, confidencialidade ou controle sobre informações pessoais (RUBINSTEIN, 2011), enquanto PbD é um conceito mais amplo que inclui elementos de desenvolvimento, concepção, usabilidade e poderá incluir em seu escopo as PETs, equilibrando aspectos tecnológicos com o processo e seus componentes fundamentais (CAVOUKIAN, 2009).

3.3 *Blockchain* na proteção da privacidade

A indústria de tecnologia da informação está se desenvolvendo rapidamente, ao passo que os especialistas muitas vezes não têm tempo de reagir ao seu aparecimento (OKSIIUK; DMYRIEVA, 2020). Isso aconteceu com o *Blockchain* (BCT), que foi adotado como uma técnica para implementar a criptomoeda *Bitcoin* que por muito tempo passou despercebida. Ultimamente o conceito tem se popularizado: "O BCT tem sido aclamado como um dos avanços tecnológicos mais significativos em vários setores" (JOSHI et al., 2022, p. 02).

Os conceitos fundamentais da BCT surgiram no final dos anos 1980 e início dos anos 1990. Lamport desenvolveu o protocolo *Paxos* em 1989 e publicou o *Part-Time Parliament in ACM Transactions on Computer Systems*, em 1990 (LAMPORT, 2019)[1]. Somente em 2008 *o* conceito como conhecemos hoje iniciou sua popularização quando da publicação do artigo *Bitcoin: A Peer-to-Peer Electronic Cash System,* de Satoshi Nakamoto (2008). Trata-se de um acrônimo que se refere a um registro descentralizado, criptografado e distribuído para arquivar dados que permite a criação de *logs* em tempo real à prova de adulteração (RAJAWAT et al., 2021; TRINKS; FELDEN, 2018). É uma tecnologia descentralizada de transações e gerenciamento de dados (OKSIIUK; DMYRIEVA, 2020), que por meio de um sistema de armazenamento e transferência de dados opera em uma base *peer-to-peer* – P2P (JOSHI et al., 2022). Isso se dá por meio de um banco de dados distribuído, em que cada bloco de informação carrega os dados da transação, um *timestamp* e um valor de *hash* criptografado

[1] O artigo foi posteriormente reimpresso na edição de 1998 da mesma revista (NAIR et al., 2020).

do bloco anterior (JAVED et al., 2021), formando uma corrente de blocos criptografados (BELOTTI et al., 2019).

A tecnologia BCT emprega contratos inteligentes para lidar com questões de confiança mútua e identidade entre os participantes. Isso é posto por meio de um conceito central para a tecnologia de BCT: o mecanismo de consenso (AHMED et al., 2020). Em vez de confiar em uma autoridade central, a confiança é colocada nos algoritmos subjacentes ao mecanismo de consenso. Esta é a base para a caracterização do BCT como um *trustless system*[2]*:* "A tecnologia *Blockchain* pode ser entendida como uma tecnologia emergente de razão distribuída que permite que os aplicativos operem de maneira totalmente descentralizada, sem a necessidade de qualquer autoridade central confiável" (AHMED et al., 2020, p. 05). Joshi et al. (2022) dizem que o BCT é uma das próximas tecnologias digitais que serão utilizadas durante a Quarta Revolução Industrial – Indústria 4.0. Segurança, privacidade e transparência de dados podem ser aprimoradas com a implementação do BCT nas operações de pequenas e grandes empresas. Como resultado, áreas como bancos, negócios e governo, mostram um interesse crescente na tecnologia *blockchain* (OKSIIUK; DMYRIEVA, 2020).

Estudos sobre várias tecnologias da Indústria 4.0, incluindo Inteligência Artificial (IA), Internet das Coisas (IoT), *big data* e *blockchain*, foram feitos nos últimos anos para estabelecer o potencial dessa tecnologia (JOSHI et al., 2022). Zheng; Cai; Li (2018) e Tapscott (2018) discutem o aumento do número de violações de vigilância e segurança que permitem a privacidade do usuário. O crescimento da pesquisa e da indústria em relação à IoT e a forma como a tecnologia *blockchain* é usada para fornecer segurança e privacidade em redes *peer-to-peer* com topologias como IoT (CAI et al., 2016; HAN; DUAN; LI, 2017), são descritos por Park and Park (2017) e Dorri et al. (2016).

Joshi (2022) identificou cinco abordagens de preservação da privacidade utilizando o *Blockchain*: *Criptomoedas*; *E-governo* em que é possível usar o modelo SSI[3] para lidar com questões de privacidade, como o caso que está sendo empregado na Suíça (com base no *uPort*[4]), na Finlândia para serviços de imigração, e na Estônia, em sistema de imigração para emissão do *e-residentes* (KONDOVA; ERBGUTH, 2020); *Smart Cities; Cooperative Intelligent*

[2] Um *trustless system* significa que os participantes envolvidos não precisam conhecer ou confiar uns nos outros ou em terceiros para que o sistema funcione (ROOKSBY; DIMITROV, 2017).
[3] *Self-sovereign identity* ou, na tradução literal para o português, *Auto Identidade Soberana* (AIS).
[4] Lundkvist, C.; Heck, R.; Torstensson, J.; Mitton, Z. and Sena, M. (2017). Uport: a platform for self-sovereign identity.

Transportation Systems – C-ITS (em português, *Sistemas Cooperativos de Transporte Inteligente*; e *e-Saúde*. Os tecnólogos acreditam que o BCT poderá substituir informações como nomes de usuário e senhas, fornecendo identidades digitais personalizadas e criptografadas que poderiam gerenciar informações na Internet até registros médicos pessoais, por exemplo (OKSIIUK; DMYRIEVA, 2020). Oksiiuk e Dmyrieva (2020) deduzem que o BCT rastreará e armazenará todos os dados pessoais e, devido à sua natureza invariável, essas informações permanecerão seguras.

3.4 Casos empíricos

Algumas das primeiras soluções baseadas em *blockchain* para mídias sociais *online* são *Ushare* e *Tawki*. *Ushare* é uma rede suportada por BCT, centrada no usuário, que permite controle, rastreamento e reivindicação de propriedade do conteúdo que é compartilhado em mídia social (CHAKRAVORTY; RONG, 2017). *Tawki* é um serviço descentralizado para comunicação social que permite aos usuários o controle de seus dados pessoais (WESTERKAMP; GÖNDÖR; KÜPPER, 2019).

O armazenador de dados *Tawki*, baseado em BCT, é implementado por meio de uma API que permite aos usuários enviar e solicitar dados de e para o armazenamento de dados pessoais de outros usuários (WESTERKAMP; GÖNDÖR; KÜPPER, 2019). Já os pesquisadores Ush Shahid et al. (2021) exploram uma estratégia para eliminar notícias falsas nas mídias sociais *online* utilizando BCT: "Isso se dá ao emitir uma classificação de conteúdo de *token* não fungível, podendo detectar e garantir notícias apropriadas" (USH SHAHID et al., 2021). Por sua vez, Rahman et al. (2019) apresenta um *framework* de controle de acesso orientado ao usuário para a rede social *online* descentralizada que permite ao usuário definir suas políticas de privacidade.

Cardoso et al. (2019) discutem as vantagens de incorporar um sistema de autenticação de dois fatores BCT em um *website Word-Press* para ajudar a proteger os dados de autenticação do usuário. As principais conclusões indicaram que o uso de tecnologia descentralizada melhora significativamente a autenticação do usuário, fortalecendo assim a proteção de informações e ativos de indivíduos e organizações (CARDOSO et al., 2019).

Angrish, Craver, Hasan e Starly (2018) analisaram as vantagens de utilizar o sistema de autenticação multifatorial *Hydro Raindrop* em uma página *Word-Press*. Entretanto, nesta pesquisa foi introduzido o *FabRec*: um método descentralizado de gerenciamento de

informações, composto por uma rede descentralizada de máquinas automatizadas, que garantem a transparência de uma operação com base em eventos históricos, auxiliando a firmar contratos sem papel entre participantes por meio de contratos inteligentes (ANGRISH et al., 2018).

Para aplicações da indústria 4.0, Lahbib *et al.* (2019) apresentam uma estrutura de gerenciamento de recursos distribuídos com base na tecnologia de contrato inteligente. Wang, Wang e Zhang (2019) apresentam uma pesquisa em que contratos inteligentes são utilizados para fornecer controle de acesso baseado em atributos para sistemas de armazenamento em nuvem. Truong *et al.* (2019) apresentam uma solução de gerenciamento de dados baseada em *blockchain* que garante a conformidade com GDPR e evita violações de segurança; há, também, um procedimento padronizado para processar dados pessoais usando a tecnologia *blockchain*; Li *et al.* (2018) apresentam um sistema de armazenamento que permite gerenciar e comercializar dados gerados por dispositivos IoT de forma segura e eficiente. Com o objetivo de proteger os direitos dos indivíduos relacionados aos dados pessoais, Alamri, Javed e Margaria (2020) desenvolveram uma solução que preserva a privacidade de pacientes para aplicativos médicos de IoT.

Rahman *et al.* (2020) desenvolveram um controle de acesso no qual os relacionamentos entre usuários são visíveis publicamente no *blockchain*. Estes são alguns exemplos identificados que têm relação direta com a privacidade e proteção de dados. Alguns dos casos citados estabeleceram apenas os protótipos; outros já foram implantados e ainda servem de base para estudos técnicos e científicos.

O *Solid* é um ecossistema baseado na *web* que separa os dados pessoais dos aplicativos instalados num sistema, fornecendo às pessoas um POD (*Personal Online Data Store*)[5] de dados pessoais, no qual elas podem armazenar dados independentemente dos aplicativos que os utilizam (BERNERS-LEE; VERBORGH, 2018). As pessoas podem decidir quais atores e aplicativos podem ler ou gravar seus dados, contrastando com as arquiteturas atuais para aplicativos, as quais atuam como armazenadores dos dados das pessoas. Os aplicativos precisam, portanto, solicitar ao usuário o acesso aos dados, os colocando no controle sobre essas informações. Isso dá aos usuários controle real sobre seus dados, pois eles podem escolher onde eles residem e quem pode acessá-los (BUYLE et al., 2019).

[5] É também chamado de *Personal Data Store* (PDS) em alguns artigos.

O *HAT Project* é semelhante ao *Solid* no sentido de que propõe uma entidade centralizada para armazenar as informações pessoais. Este microservidor centralizado fornece as informações pessoais dos usuários aos aplicativos externos, que consomem os dados sem precisar armazená-los de forma privada (NG, 2018). É uma proposta que partilha o propósito com o *Solid*, no entanto, está mais centrada na forma de distribuir a informação com as entidades externas enquanto a HAT traz um modelo baseado na combinação, produção e troca de informação.

Aplicativos web emergentes como o *MeWe*, uma rede social que promete não coletar dados e não se utiliza de algoritmos, assim como o projeto *Solid*, pretendem quebrar o cenário de internet altamente monopolizado formado por gigantes da tecnologia (MANSOUR et al., 2016), retomando o equilíbrio assimétrico da informação entre titulares e controladores de dados. Em se tratando de um ecossistema, o Solid está em constante movimento e diversos projetos, protótipos e modelos tecnológicos estão sendo apresentados.

4 CONSIDERAÇÕES FINAIS

Esta revisão descreveu algumas das soluções apresentadas nos artigos selecionados demonstrando as abordagens tecnológicas que podem ser utilizadas com a intenção de proteger a privacidade de usuários individuais no ambiente digital, controlar a quantidade de informações pessoais que são divulgadas em uma transação *online*, e permitir que os indivíduos assumam o controle sobre seus dados. Essas ações buscam devolver o controle dos dados pessoais aos titulares, estabelecendo um equilíbrio na assimetria da informação desses titulares em relação aos controladores de dados.

Abordagens tecnológicas como a criptografia, pseudonimização, anonimização, *Privacy By Design* e o *Blockchain* têm o potencial de liderar o processo de desenvolvimento de ferramentas tecnológicas sem prejudicar a coleta e o tratamento de dados desejado pelas corporações. Ao mesmo tempo, oferecem garantias de privacidade e proteção de dados dos titulares. Além de serem ferramentas que podem ser utilizadas individualmente, tal como demonstram os exemplos levantados em que o potencial dessas abordagens aumenta, quando utilizadas de forma combinada.

Essas abordagens tecnológicas oportunizam que a privacidade do indivíduo seja protegida por padrão, mesmo que a coleta e o tratamento dos dados aconteçam por meio dessas plataformas. Compreende-se, por fim, que as técnicas, ferramentas e tecnologias

existentes, assim como sua combinação, podem garantir a privacidade dos titulares no ambiente digital, sem prejudicar os modelos de negócio dos controladores de dados.

Além disso, o uso dessas ferramentas contribui de forma eficaz nos princípios e deveres de conformidade no tratamento de dados estabelecidas pelas legislações de proteção e, portanto, as corporações tecnológicas e desenvolvedores de plataformas, não precisam colocam em risco a privacidade dos titulares. O uso dessas ferramentas tecnológicas identificadas poderá compensar o equilíbrio de poder entre os atores que desejam coletar informações pessoais no ambiente digital e o indivíduo que deseja manter sua privacidade e a proteção de seus dados.

Entende-se, portanto, que esta pesquisa atendeu ao objetivo geral proposto, assim como respondeu à pergunta científica ao demonstrar que a CI pode contribuir no alcance de maior privacidade aos usuários de sistemas de informação, no desenvolvimento de produtos científicos e na pesquisa aplicada. Além disso, destaca-se que a Agenda 2030 da Organização das Nações Unidas diz que é necessário garantir a privacidade para alcançar um desenvolvimento pleno da sociedade. E, sendo assim, os profissionais da informação podem aderir a esta Agenda ao atuar na definição e na condução dos procedimentos para que ferramentas tecnológicas sejam desenvolvidas de modo que garantam a proteção da privacidade dos utilizadores de sistemas digitais.

REFERÊNCIAS

AHMED, J. *et al*. Towards Blockchain-Based GDPR-Compliant Online Social Networks: Challenges, Opportunities and Way Forward. Advances in Intelligent Systems and Computing. **Anais**...Springer, 2020.

ALAMRI, B.; JAVED, I. T.; MARGARIA, T. Preserving patients' privacy in medical IoT using blockchain. International Conference on Edge Computing. **Anais**...Springer, 2020.

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.

ANGRISH, A. *et al*. A case study for Blockchain in manufacturing:"FabRec": A prototype for peer-to-peer network of manufacturing nodes. **Procedia Manufacturing**, v. 26, p. 1180-1192, 2018.

BELOTTI, M. et al. A vademecum on blockchain technologies: When, which, and how. **IEEE Communications Surveys & Tutorials**, v. 21, n. 4, p. 3796-3838, 2019.

BERK, R. **Criminal justice forecasts of risk: A machine learning approach**. [*s. l.*] Springer Science & Business Media, 2012.

BERNERS-LEE, T.; VERBORGH, R. **Berners-Lee, T.; Verborgh, R. Welcome to Solid**. 2018. Disponível em: <https://web.archive.org/web/20220418234622/https://rubenverborgh.github.io/Solid-DeSemWeb-2018/>. Acesso em: 19 abr. 2022.

BLUMENSTOCK, J.; CADAMURO, G.; ON, R. Predicting poverty and wealth from mobile phone metadata. **Science**, v. 350, n. 6264, p. 1073-1076, 2015.

BRASIL; MINISTÉRIO DA SAÚDE. **Diretrizes metodológicas: elaboração de revisão sistemática e meta-análise de ensaios clínicos randomizados**. Brasília, DF: Ministério da Saúde, 2021.

BUYLE, R. *et al*. Streamlining governmental processes by putting citizens in control of their personal data. International Conference on Electronic Governance and Open Society: Challenges in Eurasia. **Anais**...Springer, 2019.

CAI, Z. *et al*. Collective data-sanitization for preventing sensitive information inference attacks in social networks. **IEEE Transactions on Dependable and Secure Computing**, v. 15, n. 4, p. 577-590, 2016.

CARDOSO, J. A. A. *et al*. Blockchain Based MFA Solution: The use of hydro raindrop MFA for information security on WordPress websites. **Brazilian Journal of Operations & Production Management**, v. 16, n. 2, p. 281-293, 2019.

CAVOUKIAN, A. Privacy by design: The 7 foundational principles. **Information and privacy commissioner of Ontario,** Canada, v. 5, p. 12, 2009.

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. *In*: PORTMANN, E., FINGER, M. (eds.). **Towards Cognitive Cities. Studies in Systems, Decision and Control**, v. 63. Springer [*s. l: s. n.].* p. 61-82.

CHAKRAVORTY, A.; RONG, C. Ushare: user controlled social media based on blockchain. Proceedings of the 11th international conference on ubiquitous information management and communication. **Anais**...2017.

COMMISSIONERS, D. P. AND P. Resolution on Privacy by Design. **Icdppc**, p. 1-2, 2010.

DAVIES, S. **Why Privacy by Design is the next crucial step for privacy protection**. Academic Press, 2010.

DORRI, A.; KANHERE, S. S.; JURDAK, R. Blockchain in internet of things: challenges and solutions. **arXiv preprint arXiv:1608.05187**, 2016.

ELSALAMOUNY, E.; GAMBS, S. Differential privacy models for location-based services. **Transactions on Data Privacy**, v. 9, n. 1, p. 15-48, 2016.

FORESTI, R. *et al*. Smart society and artificial intelligence: big data scheduling and the global standard method applied to smart maintenance. **Engineering**, v. 6, n. 7, p. 835-846, 2020.

GLAESER, E. L. *et al*. Crowdsourcing city government: Using tournaments to improve inspection accuracy. **American Economic Review**, v. 106, n. 5, p. 114-118, 2016.

GLAESER, E. L. *et al*. Big data and big cities: The promises and limitations of improved measures of urban life. **Economic Inquiry**, v. 56, n. 1, p. 114-137, 2018.

HAN, M.; DUAN, Z.; LI, Y. Privacy issues for transportation cyber physical systems. *In*: **Secure and Trustworthy Transportation Cyber-Physical Systems**. [*s. l.*] Springer, 2017. p. 67-86.

HUSTINX, P. Privacy by Design: The Definitive Workshop. **IDIS**, n. 3, p. 247-251, 2010.

JAVED, I. T. et al. PETchain: A Blockchain-Based Privacy Enhancing Technology. **IEEE Access**, v. 9, p. 41129-41143, 2021.

JEON, B. et al. Privacy-preserving decentralized aggregation for federated learning. IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). **Anais**...IEEE, 2021.

JESSON, J.; MATHESON, L.; LACEY, F. M. **Doing your literature review:** Traditional and systematic techniques. 2011.

JOSHI, S. et al. Adoption of Blockchain Technology for Privacy and Security in the Context of Industry 4.0. **Wireless Communications and Mobile Computing**, v. 2022, 2022.

KONDOVA, G.; ERBGUTH, J. **Self-sovereign identity on public blockchains and the GDPR**. Proceedings of the 35th Annual ACM Symposium on Applied Computing. **Anais**...2020.

LAHBIB, A. *et al*. DRMF: a Distributed Resource Management Framework for industry 4.0 environments. 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA). **Anais**...IEEE, 2019.

LAMPORT, L. The part-time parliament. *In:* **Concurrency: the Works of Leslie Lamport**. [*s. l.: s. n.*]. p. 277-317.

LI, R. *et al*. Blockchain for large-scale internet of things data storage and protection. **IEEE Transactions on Services Computing**, v. 12, n. 5, p. 762-771, 2018.

MANSOUR, E. *et al*. A demonstration of the solid platform for social web applications. Proceedings of the 25th international conference companion on world wide web. **Anais**...2016.

MAUGER, C.; MAHEC, G. LE; DEQUEN, G. Multi-criteria Optimization Using l-diversity and t-closeness for k-anonymization. *In*: **Data Privacy Management, Cryptocurrencies and Blockchain Technology**. [s.l.] Springer, 2020. p. 73-88.

MELO, J. F.; ROCKEMBACH, M. Arquivologia e Ciência da Informação na Era do Big Data: Perspectivas de Pesquisa e Atuação Profissional em Arquivos Digitais. **Prisma.com**, v. 40, n. 39, p. 14-28, 2019.

MIRZASOLEIMAN, B.; ZADIMOGHADDAM, M.; KARBASI, A. Fast distributed submodular cover: Public-private data summarization. **Advances in Neural Information Processing Systems**, v. 29, 2016.

NAIR, R. *et al*. An approach to minimize the energy consumption during blockchain transaction. **Materials Today: Proceedings**, 2020.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, p. 21260, 2008.

NG, I. C. L. **Can you own your personal data? the hat (hub-of-all-things) data ownership model**. 2018.

OBERMEYER, Z.; EMANUEL, E. J. Predicting the future—big data, machine learning, and clinical medicine. **The New England journal of medicine**, v. 375, n. 13, p. 1216, 2016.

OKSIIUK, O.; DMYRIEVA, I. Security and privacy issues of blockchain technology. 2020. IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). **Anais**...IEEE, 2020.

PARK, J. H.; PARK, J. H. Blockchain security in cloud computing: Use cases, challenges, and solutions. **Symmetry**, v. 9, n. 8, p. 164, 2017.

POULLET, Y. About the E-Privacy Directive: towards a third generation of data protection legislation? *In*: **Data protection in a profiled world**. [*s. l.*] Springer, 2010. p. 3-30.

RAHMAN, M. U. *et al*. **Protecting personal data using smart contracts**. International Conference on Internet and Distributed Computing Systems. **Anais**...Springer, 2019.

RAHMAN, M. U. et al. **Context-aware and dynamic role-based access control using blockchain**. International Conference on Advanced Information Networking and Applications. **Anais**...Springer, 2020.

RAJAWAT, A. S. *et al*. Securing 5G-IoT Device Connectivity and Coverage Using Boltzmann Machine Keys Generation. **Mathematical Problems in Engineering**, v. 2021, 2021.

ROOKSBY, J.; DIMITROV, K. Trustless education? A blockchain system for university grades. New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations, Workshop at DIS. **Anais**...2017.

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

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain revolution**. [*s. l.*] Senai-SP Editora, 2018.

TRINKS, S.; FELDEN, C. Edge computing architecture to support real time analytic applications: A state-of-the-art within the application area of smart factory and industry 4.0. 2018. IEEE International Conference on Big Data (Big Data). **Anais**...IEEE, 2018.

TRUONG, N. B. et al. Gdpr-compliant personal data management: A blockchain-based solution. **IEEE Transactions on Information Forensics and Security**, v. 15, p. 1746-1761, 2019.

TSCHIATSCHEK, S. *et al*. Learning mixtures of submodular functions for image collection summarization. **Advances in neural information processing systems**, v. 27, 2014.

USH SHAHID, I. *et al*. Authentic Facts: A Blockchain Based Solution for Reducing Fake News in Social Media. 2021 4th International Conference on Blockchain Technology and Applications. **Anais**...2021.

WANG, S.; WANG, X.; ZHANG, Y. A secure cloud storage framework with access control based on blockchain. **IEEE access**, v. 7, p. 112713-112725, 2019.

WEST, S. M. Data capitalism: Redefining the logics of surveillance and privacy. **Business & society**, v. 58, n. 1, p. 20-41, 2019.

WESTERKAMP, M.; GÖNDÖR, S.; KÜPPER, A. Tawki: Towards self-sovereign social communication. 2019. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). **Anais**...IEEE, 2019.

ZHENG, X.; CAI, Z.; LI, Y. Data linkage in smart internet of things systems: a consideration from a privacy perspective. **IEEE Communications Magazine**, v. 56, n. 9, p. 55-61, 2018.

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