Fabiana França, Claudia Mont'Alvão *

Privacidade no governo digital no contexto do design centrado no usuário e do design centrado no humano: uma revisão de literatura

Resumo A revolução da internet e a aplicação das TICs emergiram na era dos dados em que os serviços são guiados por informações coletadas das pessoas. Isso inclui serviços governamentais dos sistemas do governo eletrônico. O que pode representar um risco à liberdade das pessoas, à democracia e especialmente à proteção da privacidade. Organizações devem estar prontas para implementar tecnologias, requisitos e normas que garantam a proteção dos dados dos cidadãos, considerando seus contextos e necessidades. Este artigo apresenta o resultado de um estudo cujo objetivo é identificar temas e oportunidades relacionadas à proteção da privacidade no governo digital dentro do escopo do design centrado no usuário e no humano. Para isso, uma pesquisa qualitativa foi realizada através de revisão sistemática de literatura na base de dados ScienceDirect no período de 2019 a 2023. Como resultado alguns temas comuns como segurança e proteção de dados, riscos, transparência e confiança foram identificados como pontos de discussão que poderiam servir de base para pesquisas futuras.

Palavras-chave Privacidade, UCD, HCD, Governo digital.

*

Fabiana França é aluna de mestrado pelo Programa de Pós-Graduação em Design da Universidade Federal do Maranhão - UFMA, na linha Design e Ergonomia. É Bacharel em Comunicação Social, com habilitação em Rádio e Televisão pela mesma Universidade. Atualmente pesquisa sobre privacidade, governo digital e design.
<fabiana.fs@outlook.com>
ORCID 0009-0008-5974-8976

Claudia Mont'Alvão possui graduação em Desenho Industrial/Projeto de Produto, pelo Centro Universitário da Cidade (1994), Mestrado e Doutorado em Engenharia de Transportes pela Universidade Federal do Rio de Janeiro (1997 e 2001). Professora visitante na Kookmin University (Coréia do Sul) em 2022, como parte da pesquisa de Pós-Doutorado sobre 'UX Methodology.' Atualmente é professora associada do Programa de Pós Graduação em Design da Pontifícia Universidade Católica do Rio de Janeiro, PPGDesign PUC-Rio e Vice Decana de

Desenvolvimento e Inovação do Centro de Teologia e Ciências Humanas (CTCH/PUC-Rio).
<cmontalvao@puc-rio.br>
ORCID 0000-0002-1048-2993

Privacy at the e-government within user-centered design and human-centered design context: a literature review

Abstract *The Internet revolution and the ICTs application emerged in the data era in which the services are guided by the personal information which is collected from people. Including governmental services in e-government systems. It may represent a risk to people's freedom, democracy, and especially to privacy protection. Organizations must be prepared to implement technologies, requirements, and laws that secure citizens' data protection, considering their contexts and needs. This paper presents the result of a study that aims to identify themes and opportunities related to privacy protection in e-government in the scope of user-centered and human-centered design. For that, qualitative research was conducted through a literature review of the ScienceDirect database from 2019 to 2023. As a result, some common themes such as data security, data protection, risks, transparency, and trust were identified, as issues to be discussed and that could serve as new foundations for future research.*

Keywords *Privacy, UCD, HCD, E-government.*

Privacidad en el gobierno electrónico dentro del contexto del diseño centrado en el usuario y el diseño centrado en las personas: una revisión de la literatura

Resumen *La revolución de Internet y la aplicación de las TICs surgieron en la era de los datos, donde los servicios son guiados por la información recopilada de las personas, incluyendo servicios de sistemas de gobierno electrónico. Esto puede representar un riesgo para la libertad, la democracia y la protección de la privacidad. Las organizaciones deben estar preparadas para implementar tecnologías, requisitos y normas que garanticen la protección de los datos de los ciudadanos, considerando sus contextos y necesidades. Este artículo presenta un estudio que busca identificar temas y oportunidades relacionados con la protección de la privacidad en el gobierno digital, dentro del diseño centrado en el usuario y en el humano. Para ello, se realizó una investigación cualitativa mediante una revisión sistemática de la literatura en ScienceDirect entre 2019 y 2023. Como resultado, se identificaron temas comunes como la seguridad y protección de datos, los riesgos, la transparencia y la confianza, como puntos de discusión que podrían servir de base para investigaciones futuras.*

Palabras clave *Privacidad, UCD, HCD, Gobierno electrónico.*

Introduction

The Information and Communication Technologies (ICTs) application changed globally the individuals-technology interaction as well as governmental communications and its citizens' interaction practices (Balbe, 2014; Cerquinho; 2017). This made the e-government possible (Diniz *et al.*, 2009) and implied more personal data generation. Great data quantities personalize digital services but could be a risk to data protection, privacy, freedom, and democracy. It is a challenging context embodied by data capitalism, data surveillance, and data economy concepts (Mafra, 2020; Netto, 2020; Zuboff, 2018). They mean that nowadays data gathered from people through digital services and Internet of Things devices (Magrani, 2019) are profitable and important to Big Techs to help to know more about users, and their preferences and push their decision-making (Fonseca, 2020).

In this scenario, the emergence of policies such as the GDPR, the General Data Protection Regulation of the European Union, and the LGPD, the Brazilian General Data Protection Law, is important. These regulations legislate in favor of the privacy rights of citizens. However, in the Brazilian application of LGPD, the experience of the users can be frustrating, because of the legal language applied in the privacy policies and consent terms accepted by the citizens, which means they do not currently comprehend what is in those documents. According to the 2021 Privacy and Personal Data Protection research conducted by the Internet Steering Committee in Brazil, regarding the reading of privacy policies on websites and applications screens in the country, 81% of internet users do not read them in full due to their excessive length, and 69% find them difficult to understand (Núcleo de Informação e Coordenação do Ponto BR, 2022).

For Brazilian users, interacting with privacy policies can be a challenging experience, as socioeconomic indicators reveal a typically developing country's range of complexities. In essence, the access to information and communication technologies, provided by The Internet Civil Rights Framework Law and Smart Cities Brazilian letter (Brasil, 2014; Brasil, 2021a), does not seem to be comprehensive.

This background is also reflected within the e-government ecosystem, an important initiative to provide services and public policies to guarantee population citizenship inside the web. As stipulated by the Digital Government Law (Brasil, 2021b), privacy should be respected, consent must be authorized, and services need to be accessible. Consequently, to secure citizens' access to public policies through e-government and privacy protection, the user perspective should be considered, specifically their particularities and necessities.

The potential approaches that could be adopted to address this issue include User-Centered Design (UCD) and Human-Centered Design (HCD) due to their characteristics. Using ergonomic criteria and usability techniques, UCD considers various effects of interactive systems on user performance. Some of its principles stipulate that projects should be grou-

nded in an explicit understanding of users, and their active involvement and assessments should be centered around them (Chammas *et al.*, 2015).

According to Giacomin (2014), while UCD involves product, system, and service optimization, the HCD is focused on the people who the product or service is intended for. Regarded as a multidisciplinary activity and a pragmatic, empirical approach, HCD is employed to make sense of and engage individuals in the understanding of their needs, desires, and experiences, even when these are not entirely clear to them.

Preserving privacy and ensuring secure access to e-government, and consequently to ICTs and IoTs, constitute challenges within the complex contemporary world. Thus, UCD and HCD could serve as essential tools to address the issues related to the context, prioritizing individuals and their needs, thereby enhancing systems and products more positively. Besides contributing to designers' work by considering privacy since the beginning of the projects (Oliveira, 2022).

To ensure compliance of digital systems and services with data protection laws, methodologies emerge to address privacy effectively. Privacy by Design is a concept that emphasizes incorporating privacy from the outset of developing a service rather than adding it later. The goal is to proactively protect users' data and privacy by integrating them as fundamental components throughout all stages of the process (Cavoukian, 2011; Oliveira, 2022).

These concepts prove to be important in the current context of data collection and storage to propose solutions related to individuals and privacy. Therefore, the principal aim of this research is to answer the question: how can UCD and HCD contribute to increasing citizen awareness and addressing privacy concerns? To understand how to achieve this, a systematic literature review is proposed.

This article is divided into five sections. In this first section, the theoretical foundation and objective of this research were addressed. In the second section, the research method and its four stages are elucidated. In the third, there is a presentation of the results found from the summary of the themes common to the works completely read. The themes presented in this section relate to concepts of data protection, data security, risks, transparency, trust, and a user-centric approach. In the fourth section of this paper, a discussion based on the related results is presented. The fifth and final section concludes with a return to the principal aim, limitations found, and perspectives for future research.

Method

The methodology adopted to conduct this study was a systematic literature review (SLR). This type of search narrows the discussion now it positions the researcher's work as well as it "reports and assess acknowledgment produced in previous studies, highlighting concepts, procedures,

results, discussions, and relevant conclusions", according to Prodanov and Freitas (2013, p. 79).

This literature review was structured in four steps to raise previous studies which can contribute to this paper. The first step consisted of the search criteria definition. The database, keywords, search strings, and filters were delimited through a research protocol.

The ScienceDirect database was chosen based on the variety of journals available as well as the science areas covered by it. The period of research was the last five years, from 2019 to 2023 The search keywords defined were UCD; HCD; privacy; privacy by design; and e-government, based on the background previously presented. The delimited criteria of exclusion were papers not related to the research's principal aim, duplicated and not available for free; computing papers, and focused on the architecture of information and the web. The search protocol generated in this step is shown in the table below (Chart 1).

Chart 1. Method first step: the protocol definition
Source: The authors, 2023

Literature Review Protocol	
Database	ScienceDirect
Type	Review articles and research articles
Period	2019 to 2023
Keywords	UCD; HCD; privacy; privacy by design; e-government
Criteria of exclusion	Papers not related to the research's principal aim, duplicated and not available for free; computing papers and focused on the architecture of information and the web.

In the second step of this methodology, following the protocol criteria, six strings were formulated by combining the protocol keywords to initiate the 1st filtering process in the database. In this procedure, the combined strings yielded 330 available papers (open access and open achievement). Of these, 29 were preselected after a brief review of their abstracts and keywords as 2nd filtering. The process is illustrated in the subsequent chart (Chart 2).

Chart 2. Second step: strings combination, 1st and 2nd filter application, and the results found
Source: The authors, 2023

Search strings	Available	Selected
"UCD" AND "privacy by design"	6	1
"UCD" AND "privacy"	64	5
"HCD" AND "privacy"	29	1
"HCD" AND "privacy by design"	1	0
"e-government" AND "privacy by design"	10	6
"e-government" AND "privacy"	220	16
Total	330	29

In the third step, the 3rd filter of the search was applied. After a previous reading of the introduction and conclusion, 9 articles were included to be completely read. 21 papers were disregarded according to this research's principal aim. The complete filtering application is explained in the following scheme. The fourth step of this research includes the complete read of the 8 papers selected during 3rd filtering. The entire process can be seen in Image 1.

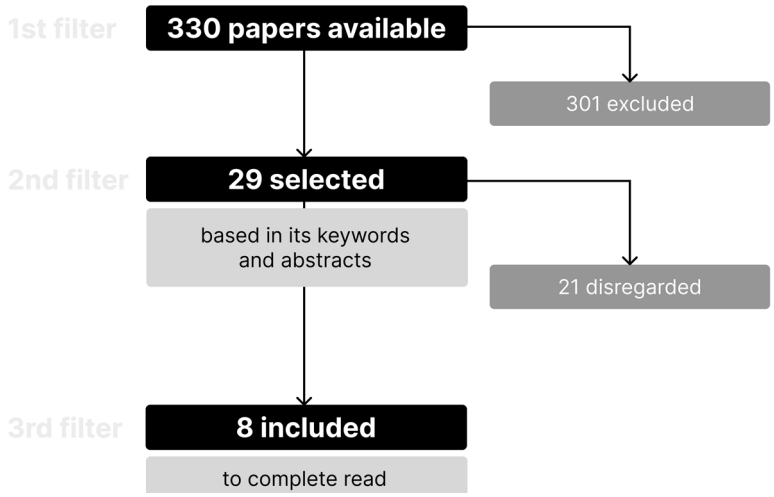

Image 1. Filtering scheme
Source: The authors, 2023

The eight selected papers were thoroughly read for inclusion in this research, as well as for the identification of common themes and future opportunities. Subsequently, the obtained results from the applied method will be presented.

Results

Eight articles were selected in the third filter. The aim is to discuss their findings and incorporate more relevant concepts into this study. The list of selected works is provided in the chart below (Chart 3).

Chart 3. Papers selected through the 2nd filter
Source: The authors, 2023

Papers selected	Authors
An experiment on data sharing options designs for eHealth interventions	Bartali; Van Velsen, 2023
Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX-design methods	Von Grafenstein *et al.*, 2022
Assessing behavioral data science privacy issues in government artificial intelligence deployment	Saura *et al.*, 2022
Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security	Pleger *et al.*, 2021

Smart City Dimensions and Associated Risks: Review of literature	Sharif; Pokharel, 2021
Using e-government services and ensuring the protection of sensitive data in EU member countries	Zakrzewska; Miciuła, 2021
Design principles for creating digital transparency in government	Matheus *et al.*, 2020
Data-driven urban management: mapping the landscape	Engin *et al.*, 2019

Throughout the reading of these articles, common themes were identified. The results will be delimited based on these findings. The themes involve the difference between data security and data protection; a user-centric perspective; participation, transparency, trust, and freedom; and the risks.

Data security and data protection and privacy

The first common point among the authors is terminological, given the variety of terms involved in privacy-related issues. They argue about the existence of terms with distinct meanings and emphasize the significance of conceptualizing these terms in addressing the subject. Once it will be revealed as an impact factor to individuals.

Understanding the population's level of awareness regarding data protection and security is crucial, as indicated by Pleger *et al.* (2021). In the realm of city management, data serves as a source for developing policies, delivering personalized services to citizens, and automating stewardship. Various types of data, including governmental data, open data, governmental data platforms, public data, and organic data, are available. However, the attention must be directed towards the data-sharing integration process, the knowledge derived from it, and the user interaction technologies, as highlighted by Engin *et al.* (2019).

Data security and privacy challenges are evident in applications that empower users to control their devices within smart cities and foster social collaboration through information and communication technologies in the context of smart governance applications. These challenges extend to smart buildings, e-health systems, home re-habitation applications, tourism initiatives in the scope of smart living applications, and educational and social platforms. The importance of addressing these challenges is underscored by Sharif and Pokharel (2021).

While terms such as data security and privacy are widely recognized, their comprehension by end-users is insufficient. The public discourse lacks a specific target audience and often employs terms that are challenging to understand. Governmental efforts to clarify and educate citizens on these matters, including policies and laws during the implementation development process, are essential, especially considering the cultural context influences and the subjective perspective of the individuals (Pleger *et al.*, 2021).

The definition of personal data remains unclear, even in literature and legislation. In urban contexts, it may encompass a combination of data derived from official records and collected from people's digital activities in their daily lives (Engin *et al.*, 2019). This ambiguity is especially relevant as citizens are the focal point of data protection and privacy, leading to significant ethical and regulatory implications associated with data collection (Pleger *et al.*, 2021; Engin *et al.*, 2019).

Risks and laws

Comprehending or not aspects involving privacy issues may pose risks to the citizen. That is the second common point to the authors. Risks are associated with the effects on people, their data, and the consequences that exist to mitigate them. The researchers agree that risks need to be evaluated and addressed, starting with the possible loopholes in the laws.

The risks, as delineated by Matheus *et al.* (2020), encompass political and legal barriers, the absence of privacy policies, mass surveillance, inadequate data protection, and the lack of stable regulatory frameworks. Illustratively, the use of trackers, such as those predicting citizens' behavior, can be justified by national security and collective intelligence. But it brings concerns related to citizens' privacy, especially with the emergence of AI usage for governments, according to Saura *et al.* (2022).

> with respect to surveillance capitalism and the use of AI by governments, specific regulation should ensure that the used data sources are legitimate and that they are not used, consciously or unconsciously, to manipulate the population so that to obtain economic benefits from both the government and the companies working with the data (Saura *et al.*, 2022).

The 'unfavorable data use' or privacy risks include, from users' point of view, knowledge acquired by others about them, that may be used against the users who generated the data (Von Grafenstein *et al.*, 2022). Privacy issues reflected by mass surveillance are a rising ethical concern. It can unveil barriers that involve bias which cause discriminatory decisions in this increasing human-machine and machine-machine interaction in the data generation context (Engin *et al.*, 2019; Matheus *et al.*, 2020).

Ways to make privacy laws more effective are not new (Von Grafenstein *et al.*, 2022). It's important to reduce the risks involving sensitive data and also contribute to citizens' confidence (Zakrzewska *et al.*, 2021). The Legislations aim to give control to individuals through the simplification of regulations. Still, the concepts involved in it like ownership, portability, right to rectification and erasure, and transparency are not technologically clarified (Engin *et al.*, 2019).

GDPR remains unclear about how the controller can achieve the specification of the purpose of the data gathering (Von Grafenstein *et al.*, 2022). Open data, a guidance concept in smart governance, has been used

in opaque ways creating a paradox of digital transparency (Matheus *et al.*, 2020). To rectify these issues, it is essential to empower people and communities through information, fostering engagement in public administration (Engin *et al.*, 2019).

The correct implementation of the legal principles since the beginning of the design process can mitigate the risk caused by controller data processing. Despite this, in law, there is no to ensure how to design this process and how to assess the effectiveness of the implementation. To change it, the implantation of a clear methodology, and an interdisciplinary approach may be the solution (Von Grafenstein *et al.*, 2022).

Transparency and trust

Privacy is related to institutions being able to safeguard citizens. It is reflected by the relationship of transparency and trust they can establish with the individuals. These two aspects are necessary to any approach used to reinforce privacy respect and rights guarantee. They are good for governance, protecting people, avoiding mistakes, and bringing citizens closer.

According to Saura *et al.* (2022), privacy is a powerful strategy that can be used for digital surveillance. Sometimes it is almost impossible for end-users to understand "what personal data is collected, and how this data is shared with external actors or organizations", but data sharing should be 'easy to use' (Bartali; Van Velsen, 2023). Citizens feel as if they are losing control over how their personal information is gathered and used by organizations, and it is due to not understanding (Pleger *et al.*, 2021; Bartali; Van Velsen, 2023).

It is related to not comprehending data protection laws, for example (Von Grafenstein *et al.*, 2022), and affects people's trust in institutions. When there is trust, there are fewer privacy concerns (Bartali; Van Velsen, 2023). The increasing data generated made individuals more predictable and less private. Regulations are important to grow public awareness, trust, and privacy in this context as well as think of new resources to secure it like the Privacy Enhancing Technologies (PET) aside from minimization, anonymity, and encryption approach concepts (Engin *et al.*, 2019).

It is important to define trust, privacy concerns, information control, and ease of use concepts (Bartali; Van Velsen, 2023). The lack of comprehension impacts the government's transparency efficacy. It is essential to dialogue with citizens to understand their perspectives and thus improve transparency. The citizens' trust is necessary for e-government development (Pleger *et al.*, 2021).

Because of the privacy and trust values of the people resulting in unnecessary information being released and undesirable effects, for instance, large-scale surveillance, bias, and discrimination against the citizens. Because it is important to apply design principles like privacy to protect personal data to digital transparency (Matheus *et al.*, 2020).

User-centric perspective

A variety of methods are being applied to manage the complex situation involving the increase of data generation in the cities, like machine learning algorithms, but it seems that is not enough for the ones focused on data involving human context and people's consent. How to introduce human factors into the system is a real challenge but seems more promising involving users, generating empirical data, to make the specification purpose more effective (Engin *et al.*, 2019; Von Grafenstein *et al.*, 2022).

With the digital increase in society, social interaction is related to personal data being processed (Von Grafenstein *et al.*, 2022) like

> User-generated data (UGD) The data publicly generated by users in digital ecosystems; User-generated content (UGC) The content published by users of social networks and online platforms; User-generated behavior (UGB) The set of connotations derived from user online behavior; Internet history History of user searches and website visits; Digital customer journey Map of user actions to make a purchase, visit a website, or send information; User location One of the fundamental indicators to measure the movement of the society. It can be consulted through its intelligent devices, such as smartphones or smartwatches; Connected devices Connected devices such as thermostats, home assistants, lamps, bulbs (Saura *et al.*, 2022).

Privacy, or the separation of privacy-sensitive and -insensitive data; comprehension, or avoiding incomprehensible terms; visualization, or standardized formats should be a design principle for digital transparency. Their use depends on the particular organization context and its preparation for transparency before the developmental phase. Achieving genuine digital transparency necessitates the implementation of design principles that involve costs, time, human resources, and the designing of a system aligned with user preferences and requirements. This includes the incorporation of a well-designed user interface and user experience in its visualization (Matheus *et al.*, 2020).

An approach centered on the user to data protection is adequate to incorporate legal compliance and transparency about the consequences for data subjects. Indeed, as argued by Von Grafenstein *et al.* (2022), User Centered Design perspectives have a lot to contribute, like their methods of evaluating, effectiveness, transparency, and controllability. They are more versatile due to their interdisciplinarity.

As also stated by the author, the pragmatic methodological, not ideological, quantitatively tested combination of viewpoints and different stakeholders' expertise brings designing solutions. In the UCD which has origins in ergonomics and brings the term usability initially to measure effectiveness, efficiency, and satisfaction, the users are the primary resource for understanding needs in system design (Von Grafenstein *et al.*, 2022).

A user-centered process is helpful to people's understanding of rights they have not considered before and how these rights can be effectively implemented. Focuses efforts on design resources that will help to increase user awareness about privacy implications when using digital services (Von Grafenstein *et al.*, 2022).

In their study, Von Grafenstein *et al.* (2022) utilized focus groups to analyze and understand the risks associated with unfavorable data use in the context of web pages, voice assistants, and autonomous vehicles. The identified concerns among users encompassed fears of being tracked, facing financial discrimination, and potential misuse of citizens' data by the state. The study advocates for the continuation of a user-centered approach, incorporating the perspectives of various stakeholders to address privacy concerns effectively.

Respect for user privacy by design principle is about a user-centric approach, which means always asking for consent and guaranteeing users access to their data. Data sharing could bring benefits like personalized medical assistance, but for it is important to include privacy by design features. It might decrease privacy concerns and increase trust and information control (Bartali; Van Velsen, 2023).

Discussion

Privacy is a subjective issue. It is related to the user's perspective and beliefs. Although privacy can be threatened by the advance of the information age. Because data related to individuals' personal information has been gathered due to economic interests. People are becoming subjects and their individuality can be converted into currency trading.

The guidance question of this research was: how can UCD and HCD contribute to enhancing citizen awareness and addressing privacy concerns? Through research results, four central thematics surrounding the main theme were found. The data protection and the data security, the risk and the law, the transparency and the trust, and the user-centric perspective.

The first approach included in the question, the User-Centered Design was only focused in two articles. But its postulates could be seen through a user-centered perspective which was present in four more papers. Its assumption is relevant to discuss privacy awareness. Although this perspective may not be the full UCD field of research, it is important to get a glimpse of the potential of this approach in the context of protecting privacy in the digital environment.

Although the term e-government was shown in just one paper, the state digitized, the institutions, and the public administration were found in others. Privacy protection reveals itself as important to governance through the transparency and trust that connect citizens and the state. And a user-centric approach would be helpful to increase it and strengthen those involved.

However, the results did not yield articles specifically focused on Human-Centered Design. Despite consistently demonstrating concern for citizens and individuals, the number of papers obtained through the string formulated with the keyword HCD did not provide clearer indicators about the potential of this approach. This does not imply that it is not adaptable. Its primary assumption of focusing on the human reveals that an application would be fruitful in enhancing citizens' awareness of privacy in e-government.

In summary, all the results included for review in this research revolved around citizen awareness, specifically emphasizing the significance of comprehension or lack thereof and the risks it entails, and the necessity of the consideration of privacy since the beginning of the project. Based on the reviewed literature, a user-centric perspective would be essential in mitigating risks by aiding in the understanding process of individuals, whether in comprehending data collection, types of data, collectors' intentions, or data protection law provisions.

Conclusion

This study aimed to explore the potential contributions of User-Centered Design (UCD) and Human-Centered Design (HCD) to enhance citizens' awareness of privacy in e-government. The findings indicated that the adoption of a user-centered approach by institutions holds promise in mitigating risks and promoting citizens' comprehension. It implies privacy by default and by design.

Although specific outcomes regarding human-centered design were not presented, this research does not entirely dismiss its relevance for future investigations. On the contrary, it underscores the need for further exploration of research avenues that investigate the interplay between HCD, privacy, and e-government. Considering the discovered results and the ensuing discussion, this study asserts that addressing privacy concerns necessitates a comprehensive approach integrating legal compliance, transparency, and UCD.

Such an approach can contribute to the establishment of a more sustainable environment that respects citizens and their rights, emphasizing the significance of treating data collection seriously within the evolving landscape of digital privacy. For future research, the aim is to focus on a local context approaching Brazilian specificities that were not covered by the results found.

Acknowledgements

This work has been supported by the Federal University of Maranhão (UFMA), the Pontifical Catholic University of Rio de Janeiro (PUC-Rio), the Foundation for Support to Research and Scientific and Technological

Development of Maranhão (Fapema) and the Brazilian National Council for Scientific and Technological Development (CNPQ).

Referências

BALBE, R. da S. **Uso de tecnologias de informação e comunicação na gestão pública**: exemplos no governo federal. 2010. Available in: https://revista.enap.gov.br/index.php/RSP/article/view/45. Accessed on: 13 nov. 2023

BARTALI, V.; VAN VELSEN, L. **An experiment on data sharing options designs for eHealth interventions**. 2023. Available in: https://www.sciencedirect.com/science/article/pii/S2214782923000428. Accessed on: 25 Nov. 2023.

BRASIL - LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco civil da internet**. 2014. Available online: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 25 Nov. 2023.

BRASIL. **Carta brasileira para as cidades inteligentes**. 2021a. Available online: https://www.gov.br/cidades/pt-br/acesso-a-informacao/acoes-e-programas/desenvolvimento-urbano-e-metropolitano/projeto-andus/carta-brasileira-para-cidades-inteligentes. Accessed on: 25 Nov. 2023.

BRASIL - LEI Nº 14.129, DE 29 DE MARÇO DE 2021. **Lei do governo digital**. 2021b. Available online: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on: 25 Nov. 2023.

CAVOUKIAN, A. **Privacy by design the 7 foundational principles implementation and mapping of fair information practices**. Information and Privacy Commissioner of Ontario. 2011. Available online:https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf. Accessed on: 25 Nov. 2023.

CERQUINHO, K. G. **Governo digital no Brasil**: o portal gov.br. Manaus: EDUA, 2017.

CHAMAS, A.; QUARESMA, M.; MONT'ALVÃO, C. **A Closer Look On The User Centred Design**. 2015. Available in: https://www.sciencedirect.com/science/article/pii/S2351978915006575. Accessed on: 24 Aug. 2023.

DINIZ, E. H.; BARBOSA, A. F.; JUNQUEIRA, A. R. B.; PRADO, O. **O governo eletrônico no Brasil:** perspectiva histórica a partir de um modelo estruturado de análise. 2009. Available in: https://www.scielo.br/j/rap/a/f9ZFfjhYtRBMVxLPjCJMKNJ/?format=pdf&lang=pt. Accessed on: 13 Nov. 2023.

ENGIN, Z.; VAN DIJK, J.; LAN, T.; LONGLEY, P. A.; TRELEAVEN, P.; BATTY, M.; PENN, A. **Data-driven urban management**: Mapping the landscape. 2020. Available in: https://www.sciencedirect.com/science/article/pii/S2226585619301153. Accessed on: 25 Nov. 2023.

FONSECA, R. A. **A vida mobile no capitalismo de dados**: narrativas de negócios digitais e a constituição do consumidor conectado. São Paulo: Pimenta Cultural, 2020.

GIACOMIN, J. **What is human centered design?** 2014. Available in: https://www.tandfonline.com/doi/abs/10.2752/175630614X14056185480186. Accessed in: 16 aug. 2023.

MAFRA, W. **A privacidade como direito fundamental da pessoa humana**. In: DAWBOR, L. Sociedade vigiada. São Paulo: Autonomia Literária, 2020.

MAGRANI, E. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. Porto Alegre: Arquipélago Editorial, 2019.

MATHEUS, R.; JANSSEN, M.; JANOWSKI, T. **Design principles for creating digital transparency in government**. 2021. Available in: https://www.sciencedirect.com/science/article/pii/S0740624X20303294. Accessed on: 25 Nov. 2023.

NETTO, V. A. **A importância de regulamentar e proteger os dados pessoais**. In: DAWBOR, L. Sociedade vigiada. São Paulo: Autonomia Literária, 2020.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Privacidade e proteção de dados pessoais**. 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2022.

OLIVEIRA, R. D. de; BARBOSA, M. L. de A.; KLEIN, A. A.; KISTMANN, V. B.; OKIMOTO, M. L. L. R. **Privacidade por Definição e os aspectos de privacidade de dados pessoais no contexto do design inclusivo e de serviços**. DAT Journal, [S. l.], v. 7, n. 2, p. 179–197, 2022. DOI: 10.29147/datjournal.v7i2.613. Available online: https://datjournal.emnuvens.com.br/dat/article/view/613. Accessed on: 27 Nov. 2023.

PLEGER, L. E.; GUIRGUIS, K.; MERTES, A. **Making public concerns tangible**: An empirical study of German and UK citizens' perception of data protection and data security. 2021. Available in: https://www.sciencedirect.com/science/article/pii/S0747563221001539. Accessed on: 25 Nov. 2023.

PRODANOV, C.; FREITAS, E. C. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho. 2. ed. Novo Hamburgo: Feevale, 2013.

SAURA, J. R.; RIBEIRO-SORIANO, D.; PALACIOS-MARQUÉS, D. **Assessing behavioral data science privacy issues in government artificial intelligence deployment**. 2022. Available in: https://www.sciencedirect.com/science/article/pii/S0740624X22000120. Accessed on: 25 Nov. 2023.

SHARIF, R. A.; POKHAREL, S. **Smart City Dimensions and Associated Risks**: Review of literature. 2022. Available in: https://www.sciencedirect.com/science/article/pii/S2210670721008088. Accessed on: 25 Nov. 2023.

VON GRAFENSTEIN, M.; JAKOBI, T.; STEVENS, G. **Effective data protection by design through interdisciplinary research methods**: The example of effective purpose specification by applying user-Centred UX-design methods. 2022. Available in: https://www.sciencedirect.com/science/article/pii/S026736492200067X. Accessed on: 25 Nov. 2023.

ZAKRZEWSKA, M.; MICIUŁA, I. **Using e-government services and ensuring the protection of sensitive data in EU member countries**. 2021. Available in: https://www.sciencedirect.com/science/article/pii/S1877050921018585. Accessed on: 25 Nov. 2023.

ZUBOFF, S. **Big other**: capitalismo de vigilância e perspectivas para uma civilização de Informação. In: BRUNO, F.; CARDOSO, B.; KANASHIRO, M.; GUILHON, L.; MELGAÇO, L. Tecnopolíticas da vigilância: perspectivas da margem. São Paulo: Boitempo, 2018.

Recebido: 04 de fevereiro de 2024
Aprovado: 12 de julho de 2024