Rodrigo Diego de Oliveira, Maria Lílian de Araújo Barbosa, Alison Alfred Klein, Virginia Borges Kistmann, Maria Lucia Leite Ribeiro Okimoto*

Privacy by design and the privacy aspects of personal data in the context of inclusive design and services

Abstract This article presents the result of a study that sought to identify conducts, techniques and good practices related to data privacy, which can be incorporated into the user-centered process, within the scope of service design and inclusive design, using the Internet of Things (IoT). It is important to identify new guidelines that can be incorporated into service design and inclusive design. This study was supported by a Systematic Bibliographic Review, covering 150 articles in a 5-year period (2017-2021), in the Web of Science databases, Scopus databases and the Periodic Journal Portal of CAPES. As a result, it brings a list of recommendations for good practices that can be adopted in design processes, especially to the Privacy by Design (PbD) framework.

Keywords Service Design, Inclusive Design, Technology, User-centered Design, Privacy by Design.

*

Rodrigo Diego de Oliveira é doutorando em Design de Sistemas de Produção e Utilização na UFPR (2021-2024), Mestre em Design Sistemas de Informação pela UFPR (2021), especialista em Design Centrado no Usuário (2013) e MBA em Gestão de Projetos (2016) pela Universidade Positivo, Designer Gráfico pela Universidade Tuiuti do Paraná (2007). Atualmente é pesquisador do Laberg (Laboratório de Ergonomia e Usabilidade da UFPR) acerca de tecnologias assistivas e experiência do usuário. *<rodrigodiego@ufpr.br>*
ORCID: 0000-0003-0957-891X

Maria Lílian de Araújo Barbosa é Doutoranda em Design (Produto-UFPR). Mestre Eng. Mecânica (Produto), Prêmio de 1º Lugar na apresentação de sua dissertação no WORKSHOP INTERNACIONAL TECNOLOGIAS ASSISTIVAS promovido pela FUNDAÇÃO ARAUCÁRIA | SETI-PR | SEJUF- PR (2019). Especialização em Ergonomia (UFPR). Graduação em Lic. Desenho. Como pesquisadora é integrante do Laboratório de Ergonomia

e Usabilidade (LABERG-UFPR) e da Rede de Pesquisa e Desenvolvimento em Tecnologia Assistiva (RPDTA). *<maria.lilian@ufpr.br>*
ORCID: 0000-0002-5438-9061

Alison Alfred Klein possui graduação em Fisioterapia pela UTP - Universidade Tuiuti do Paraná (1999), especialização em Fisioterapia do Trabalho pelo CBES (2002) e mestrado em Engenharia Mecânica - Ergonomia pela Universidade Federal do Paraná (2008). Atualmente cursa Doutorado em Design - UFPR. Somada a formação em Perícia Judicial - IBRAFA (2004), Estágio na Universidade de La Corunha - Espanha (1997). Foi presidente da ABRAFIT - Associação Brasileira de Fisioterapia do Trabalho (2006-10). Atualmente é Ergonomista do KINEBOT. *<alison.klein@ufpr.br>*
ORCID: 0000-0001-7725-9959

Virginia Borges Kistmann possui graduação em Desenho Industrial pela Escola Superior de Desenho Industrial do Rio de Janeiro - ESDI (1974), mestrado em Design pelo Royal College of Art - RCA, na Inglaterra (1984), e doutorado em Engenharia de Produção pela Universidade Federal de Santa Catarina - UFSC (2001), com programa sanduíche na Koeln International School of Design-KISD, Alemanha. Foi professora da graduação em Design da UFPR (1975-2005) e da PUCPr até (2005-2017). Atuou como professora visitante na graduação da Hochshcule der Bildende Kunst Berlin e da Universidade da Savóia no Mestrado Internacional em Hipermídia e Comunicação. *<vkistmann@ufpr.br>*
ORCID: 0000-0001-6845-6459

Maria Lucia Leite Ribeiro Okimoto fez Pós-doutorado na Technische Universitat München, Fakultät für Maschinenwesen Lehrsthul für Ergonomie de

Privacidad por diseño y los aspectos de privacidad de los datos personales en el contexto del diseño y los servicios inclusivos

Resumen *Este artículo presenta el resultado de un estudio que buscó identificar conductas, técnicas y buenas prácticas relacionadas con la privacidad de datos, que puedan ser incorporadas al proceso centrado en el usuario, en el ámbito del diseño de servicios y el diseño inclusivo, utilizando el Internet de las Cosas (IoT). Es importante identificar nuevas pautas que se puedan incorporar en el diseño de servicios y el diseño inclusivo. Este estudio fue apoyado por una Revisión Bibliográfica Sistemática, que abarcó 150 artículos en un período de 5 años (2017-2021), en las bases de datos Web of Science, bases de datos Scopus y el Portal de Revistas Periódicas de la CAPES. Como resultado, trae una lista de recomendaciones de buenas prácticas que se pueden adoptar en los procesos de diseño, especialmente al marco de Privacidad por Diseño (PbD).*

Palabras clave *Diseño de servicios, Diseño inclusivo, Tecnología, Diseño centrado en el usuario, Privacidad por diseño.*

Privacidade por Definição e os aspectos de privacidade de dados pessoais no contexto do design inclusivo e de serviços

Resumo *Este artigo apresenta o resultado de um estudo que buscou identificar condutas, técnicas e boas práticas relacionadas à privacidade de dados, que podem ser incorporadas ao processo de design centrado no usuário, no âmbito do design de serviços e design inclusivo, utilizando a Internet das Coisas (IoT). É importante identificar novas diretrizes que possam ser incorporadas ao design de serviços e ao design inclusivo em virtude das novas legislações. Este estudo foi apoiado por uma Revisão Bibliográfica Sistemática, abrangendo 150 artigos em um período de 5 anos (2017-2021), nas bases de dados Web of Science, Scopus e no Portal de Periódicos da CAPES. Como resultado, traz uma lista de recomendações de boas práticas que podem ser adotadas em processos de design, especialmente para o modelo de Privacidade por Definição ou Privacy by Design (PbD).*

Palavras-chave *Design de Serviços, Design Inclusivo, Tecnologia, Design Centrado no Usuário, Privacidade por Definição.*

julho/2012 à fev/2013, Alemanha. Doutora na área de Engenharia de Produção pela Universidade Federal de Santa Catarina e RWTH-Aachen, Alemanha (2000). Mestrado em Engenharia de Produção pela Universidade Federal de Santa Catarina (1994). Graduação em Desenho Industrial pela Universidade Federal do Paraná (1983). Professora Titular do Departamento de Engenharia Mecânica na Universidade Federal do Paraná. Atuando no curso de Graduação em Engenharia Mecânica da UFPR e nos Programas de Pós-graduação: Engenharia Mecânica (PGMEC) e DESIGN (PPGDesign) da UFPR. Coordena o Laboratório de Ergonomia e Usabilidade (LABERG, UFPR). *<lucia.demec@ufpr.br>*
ORCID: 0000-0002-1968-1964

Introduction

A contribution in the search for the relationship between Privacy by Design and user-centered design practices (UCD), focused on service design and inclusive design, being what this article presents.

The development of smart cities is characterized by the use of new technologies and systems capable of modifying the relationships between citizens, institutions, the economy and between individuals themselves. Smart Cities magnify the use of artifacts compatible with the Internet of Things, or IoT (SCAVONI; BÜHRING, 2021; PREUVENEERS; JOSSEN, 2016; AN; KIM; KIM, 2020).

This is a technology that is growing everywhere, acting omnipresent, whether in products or services. It implies the constant collection of user data through numerous sensors, geolocation and an intelligent mesh of communication networks (GEA, PARADELLS, LAMARCA, ROLDÁN, 2013).

The unrestrained collection of user data in view of the increased use and application of these technologies has given rise to a discussion regarding the privacy of individuals' data, which seeks to ensure greater transparency, security, avoid leaks and the inappropriate use of this information (OLIVEIRA; GOMES; LOPES; NOBRE, 2019; ABDUL-GHANI; KONSTANTAS, 2019).

Therefore, the General Data Protection Law (LGPD), No. 13.709 of 2018, came to enforce in Brazil (BRASIL, 2018), which obliges companies, public and private institutions to adapt to its dispositions.

Both the concept of data privacy and the concept of Privacy by Design began to appear in the 90s decade. Since then, the importance of Privacy by Design, which can be translated as Privacy from Design, stands out for the orientation of the inclusion of privacy concepts since the beginning of the projects (ROMANOU, 2018; ROMERO; HEREDERO, 2017; CAVOUKIAN, 2012).

In this sense, the European Union started to consider it as privacy and data protection incorporated throughout the entire life cycle of technologies, from the initial design stage to its implementation, use and final disposal (ROMANOU, 2018).

Designers utilize user data collection techniques such as: interviews, questionnaires, field surveys, photography, focus groups, among others. These techniques help in decision making, thus ensuring that digital and/or physical products and/or services are being created that meet the real needs of users (LOWDERMILK, 2013).

However, to adopt practices aimed at ensuring data privacy through the UCD, it's necessary to identify conducts and recommendations that can be incorporated into the daily activities of designers, in order to comply with the dispositions listed in the Brazilian General Data Protection Law (BRASIL, 2018).

The emergence of this law, associated with the expansion of so-called smart cities, as well as the growth of artifacts that rely on IoT, that can impact in the design process, especially in service design, an activity that

aims to improve the quality of interactions between service providers and theirs consumers (STICKDORN; SCHNEIDER, 2014), and in the inclusive design, which focuses on the design of environments, products and/or services usable by all, regardless of any physical, social, age limitations, among others (GOMES; QUARESMA, 2018).

In this context, it was reached the guiding question of this article: **What are the good practices for respecting the privacy of personal data in service design and inclusive design?**

A possible approach to be considered is the framework called Privacy by Design (PbD), used as a guide in the construction of products and services respecting the privacy of users' data since their conception (PERERA et al., 2016).

Thus, with the main objective of identifying and relating possible good practices, conducts and recommendations that can be applied in the design of services and inclusive design based on IoT, a bibliographic survey about PbD and the Internet of Things was conducted, using the Bibliographical Revision Systematic Roadmap (BRSR) (CONFORTO; AMARAL; SILVA, 2011). Secondarily, based on the state of art of the PbD surveyed, we sought to point out specific practices of services that focus on inclusion to improve user-centered design processes.

The definition of conducts and/or recommendations can benefit designers, public and private companies and various institutions that seek to adapt projects based on IoT with data protection and privacy policies. It contributes for designers to know and apply techniques in the user-centered approach, considering data privacy from the conception of products and services. However, the main beneficiary of the study is the end user, who will be able to enjoy services and purchase products with greater transparency regarding the use of their personal data, considering that these behaviors will be adopted by the designers as a way of respecting ethics and the individual.

Therefore, the study seeks to collaborate with the economy of companies, institutions and, ultimately, with the country, highlighting numerous points of attention that can avoid operating costs and/or legal disputes, resulting from poor conduct in the product construction process and services, which can make them unfeasible due to the new legislation. The structure of the article was organized in the following sections: 1) introduction (context, problem question and justifications); 2) method (BRSR detailing); 3) Results (selected articles), The Internet of Things and service and/or inclusive design: concepts related to privacy and Privacy by Design: recommended practices; and 4) Final considerations.

Method

As this topic still has fewer studies and in order to answer the question asked, the Bibliographical Revision Systematic Roadmap (BRSR) was

adopted as the central method of conducting this study, adapted in 5 steps. BRSR is a rigorous scientific investigation, which aims to raise, gather and critically evaluate studies on the subject, summarizing the results obtained, as shown in (Figure 1) below.

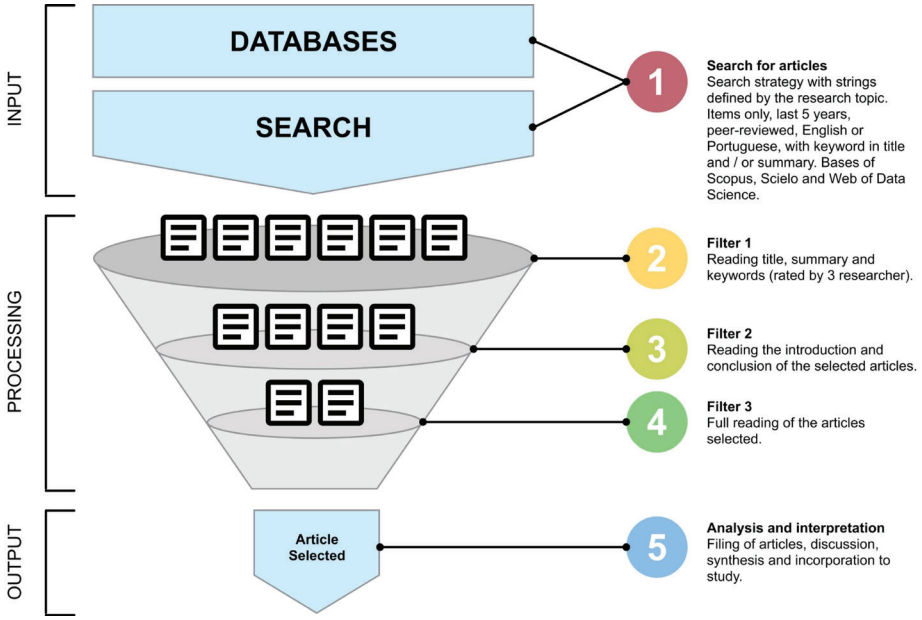

Fig 1. 5-step adaptation of the method BRS Roadmap.
Source: Adapted representation of the systematic review method based on Conforto, Amaral and Silva (2011).

These 5 steps are organized into 3 approaches: input, processing and output. The first, of an exploratory nature, aimed to gather more information about data privacy in IoT projects within the scope of service design and inclusive design, to define and elaborate a better outline of good practices that should be considered by designers in a user centered approach (PRODANOV; FREITAS, 2013).

The second, processing, can be classified as a qualitative research, which, due to its characteristic, does not require the use of statistical methods and techniques to analyse the data collected, requiring an approach based on the interpretation of phenomena, in a descriptive way (SAMPIERI; COLLADO; LUCIO, 2013).

This qualitative approach provides a broad view of information, however subjective, based on recurrent patterns identified after categorization and data analysis (PREECE; ROGERS; SHARP, 2013).

And the third, an output, consisting in a synthesis of the data collected and analyzed, in view of the research question. Initially, for the delimitation of the bibliographic survey, search strings were defined according to (Table 1), below, in a time span of 5 years (2017 to 2021), considering only peer-reviewed articles from three databases: Web of science, Scopus and the CAPES periodic journal portal. The keywords emerged from the research's guiding question.

Table 1. Search strings applied in the study.
Source: The Authors (2021).

Language	String
Portuguese	"Privacy by design" OR "Privacidade de dados" AND IoT AND "design de serviços" OR "design inclusive
Portuguese	"Privacy by design" OR "Privacidade de dados" AND "Internet das Coisas" AND "design de serviços" OR "design inclusivo"
English	"Privacy by design" OR "Data Privacy" AND IoT AND "inclusive design" OR "service design"
English	"Privacy by design" OR "Data Privacy" AND "Internet of Things" AND "service design" OR "inclusive design"

The selection of articles took place after tabulation in an electronic spreadsheet, reading of titles, abstracts, keywords and evaluation by three researchers based on the following scoring criteria: 0 for irrelevant, 1 for partially addressing the topic and 2 for articles relevant. Articles that obtained a score greater than or equal to 5 in the sum of the evaluations were selected for full reading.

As a strategy for analysing the selected articles, the bibliographic listing technique was applied, which consists of a summary, critical and/or commented review of the main ideas addressed by the authors (FRANCELIN, 2016).

The final interpretation of the data was carried out through discussions among researchers about the records.

Study Results

As a result of the BRSR, 173 articles were found, 39 in the Scopus database, 58 in the CAPES Periodic Journal Portal and 76 in the Web of Science (Figure 2).

A total of 150 articles were selected after the removal of duplicates between the researched bases, of which only 20 had a score greater than or equal to 5 after the researchers' evaluation, which are shown in (Table 2) below.

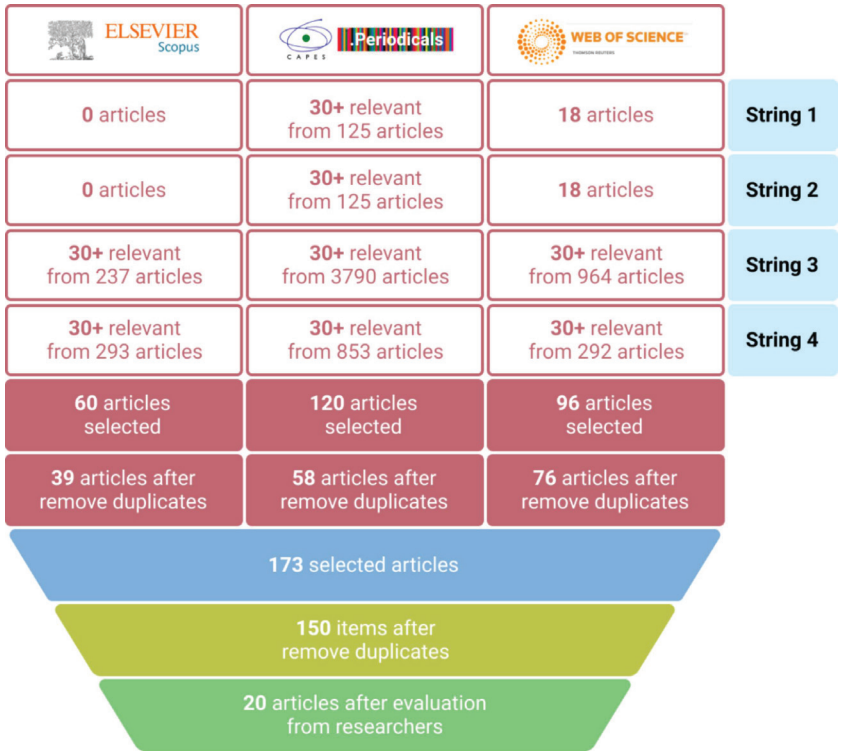

Fig 2. Total articles found per database.
Source: The authors (2021).

Table 2. Articles selected for full reading after the researchers' evaluation.
Source: The authors (2021).

Nº	Title	Authors
01	Motivating information system engineers' acceptance of Privacy by Design in China: An extended UTAUT model	Bu et al. (2021)
02	A Systematic Literature Review on Privacy by Design in the Healthcare Sector	Semantha et al. (2020)
03	Designing Technologies with and for Youth: Traps of Privacy by Design	Zaman (2020)
04	Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design	Robles et al. (2020)
05	Necessity of the Needs Map in the Service Design for Smart Cities	An, et al. (2020)
06	Privacy by design: a Holochain exploration	Wahlstrom et al. (2020)
07	"Privacy by Design" implementation: Information system engineers' perspective	Bu et al. (2020)
08	A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective	Abdul-Ghani e Konstantas (2019)
09	Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations	Padyab e Ståhlbröst (2018)

10	The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise	Romanou (2018)
11	The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design	Chaudhuri e Cavoukian (2018)
12	Contribution of Privacy by Design	Romero e De-Pablos--Heredero (2017)
13	Ethics and Privacy Implications of Using the Internet and social media to Recruit Participants for Health Research: A Privacy-by--Design Framework for Online Recruitment	Bender et al. (2017)
14	Opening the black box: Petri nets and Privacy by Design	Diver e Schafer (2017)
15	ARMY: Architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things	Hernandez-Ramos et al. (2016)
16	A Privacy-by-Design Contextual Suggestion System for Tourism	Efraimidis et al. (2016)
17	Designing Commercial Therapeutic Robots for Privacy Preserving Systems and Ethical Research Practices Within the Home	Sedenberg, Chuang e Mulligan (2016)
18	Making privacy by design operative	Schartum (2016)
19	Security and privacy controls for streaming data in extended intelligent environments	Preuveneers e Joosen (2016)
20	The Quest for Privacy in the Internet of Things	Porambage et al. (2016)

These selected articles were then read in full, filed and discussed in order to answer the research question of this study, and then the concepts, good conduct and/or practices related to the privacy of user data about the IoT were formulated, related to service design and/or inclusive design through a user-centric approach. In the next topics of this article, the theoretical results obtained are presented.

The Internet of Things and Service and/or Inclusive Design: Concepts Related to Privacy

> Privacy is a highly contextual social right that is fundamental to the perpetuation of other social rights such as freedom, dignity, autonomy, justice and democracy, far beyond data security. People exercise privacy through personal information preferences and practices that are specific to social contexts and change over time (WAHLSTROM et al., 2020, p. 2).

Therefore, users need help managing their privacy through awareness programs, communication of institutional practices, policy enhancement, and privacy-enhancing tools and technologies (PADYAB; STÅHLBRÖST, 2018).

The layperson may find it difficult to understand the architecture of IoT sensors and how they collect or not their data, or how the data is shared with the device manufacturers. The absence of the perception of privacy protection turns out to be an influencing factor in relation to the non-acceptance and adoption of IoT (CHAUDHURI; CAVOUKIAN, 2018).

Another fact to be considered is the right to be forgotten, which gives a person the legitimate right to request that their personal information be deleted from the Internet, so that they cannot be found by search engines. However, there are serious implications for business and access to information issues. After that decision, Google received 41,000 forget data requests. In response, Google removed several URLs from its search results. The right to be forgotten is a perpetual burden for companies and is considered very difficult in terms of implementation (WAHLSTROM et al., 2020).

In addition, privacy protection must be considered in the implementation policy, public policies and legal frameworks that promote individual rights, trust, ethical behaviour and harsher penalties in the event of improper behaviour, corruption and criminalization of those who use or disclose this data and issues involving the balance between the public and private domains (CHAUDHURI; CAVOUKIAN, 2018).

The Internet of Things ecosystem – IoT is composed of elements that are being incorporated into everyday life around the world, due to the increase in the offer of smart devices and/or smart services in various segments: wearable devices, connected homes, connected cars, connected health, smart cities and many other potential service offerings, with privacy being a key issue across all sectors (BENDER et al., 2017). The Internet of Things is believed to drive the development of products and services for smart environments, but the anticipated exponential data growth will give rise to serious security and privacy issues. The technologies installed in these environments collect and process personal information to help individuals in their daily activities, improve their experiences and adapt to the needs of users with different profiles (PORAMBAGE et al., 2016).

In this context, the demand for methods that address the issue in the Internet of Things and data security is seen as urgent, despite the fact that IoT is an emerging technology, which has not yet reached maturity in a level of stability and understanding of the lifecycle of this technology adoption (BENDER et al., 2017). In this sense, Privacy by Design - PbD proposes a set of recommendations aimed at ensuring greater security and privacy, especially for IoT projects, highlighting the importance of thinking about these aspects from the beginning of the project, even in the design stage. However, design in this context goes far beyond designing a product, interface or providing a good user experience. Design in this case refers to the

design of the entire ecosystem involving the relationships between technologies and the interested parties (PADYAB; STÅHLBRÖST, 2018).

Homes are a growing trend that configure themselves as smart environments, but that need to be connected to smart services from third parties and technology providers, such as data storage in the cloud, big data and services that visualize and analyze sensitive information as a means to offer new insights to its customers, but that typically crosses the personal space or privacy boundaries of the smart environment (PORAMBAGE et al., 2016).

On the other hand, IoT services in the health area adopt several initiatives that aim to ensure data privacy; however, most are outdated and do not minimize violations. The analysis and comparison of 7 frameworks focused on privacy and applied in the healthcare area, resulted in the conclusion that PbD is essential for us to deliver the expected value for the area, as so far, we have failed to create an effective method to resolve issues of privacy. From this perspective, designers will need, in addition to respecting current legislation, to find the best approaches to implement data privacy techniques according to each area, segment, context and amplitude, which may require a greater number of researches, even impacting the budget of the projects (SEMANTHA et al., 2020).

Also, in studies on IoT-based therapeutic robots in the health area, a discussion about the ethics of data sharing with science can be found, predicting that studies with human beings will increasingly stop taking place in laboratories upon arrival of the IoT and will be carried out by companies directly in the users' environment. Sharing these data with science has enormous potential for advancing treatments and knowledge, especially for vulnerable individuals (SCHARTUM, 2016).

On the other hand, health and wellness services noted that users feel a much higher level of privacy using the data protection system with Blockchain technology, due to the high capacity of this system to track data transactions on the Internet, which is why it is used in financial transactions around the world (ROBLES et al., 2020).

Considering this ecosystem, it is worth reflecting on how much designers are really prepared or have a repertoire to work in front of this complexity of technologies and number of "actors". Based on this complexity, it is assumed that there is a need to form multidisciplinary teams to think about all aspects of an IoT-based product or service, including the legal aspects according to the legislation of each country (PADYAB; STÅHLBRÖST, 2018).

IoT applications for end users, within the design of healthcare companies' services and the prevalent concerns about the use of various IoT technologies, including wearables, which collect personal information to help visualize a person's health in their daily activities, have vulnerabilities in the servers of healthcare companies and data tampering. As an example, privacy issues associated with the use of Bluetooth and data integrity on portable health trackers, which can lead to location tracking, third party access to fitness data, sale of data to third parties, demographic data col-

lection, device access of sensitive user information and vulnerabilities to hackers (CHAUDHURI; CAVOUKIAN, 2018).

It was also seen the need for a holistic attention to the life cycle of products that use IoT from their design, being essential to consider the architecture and data privacy from design to discontinuation of use (EFRAIMIDIS et al., 2016).

Thus, the inclusion of requirements to protect people's privacy in data processing in companies can be done in the initial phases, when processes are being designed, generating higher levels of data protection and trust (ROMERO; HEREDERO, 2017).

However, when it comes to privacy studies on vulnerable individuals, such as the elderly, people with disabilities, etc., few practices are found. The basic ethical principles of the Belmont Report and its extensions have been adopted to formulate practices and recommendations considering this audience, which may have a greater degree of demand and rigor regarding the collection and use of data, an additional point of attention for the inclusive design that needs to verify the existence of extra legislation according to each country (SCHARTUM, 2016).

Considering that today humans are increasingly losing power and control to machines and even adults and traditional institutes have difficulty keeping up with the fast pace of technology, it becomes important to think beyond user-centric design and consider participatory design (ZAMAN, 2020).

From these elements, in the next topic, the best practices for Privacy by Design are set out.

Privacy By Design: Best practices

The fundamental principles of Privacy by Design, created in Canada in the 1990s and defended by Ann Cavoukian, presented in (Table 3) below (PORAMBAGE et al., 2016).

Table 3. The Seven Principles of Privacy by Design.
Source: Porambage et al. (2016).

Nº	**Principle**
1	Proactive not reactive, more preventive and not corrective;
2	Privacy by default;
3	Privacy built into the design;
4	Full functionality - positive sum, not zero sum;
5	End-to-End Security - Lifecycle Protection;
6	Visibility and Transparency;
7	Respect for user privacy.

The original principles bring some guidelines that can be adopted even in the project stage by designers, divided into 8 phases: 1) Define IoT

service project and operation plan; 2) Develop IoT data flows, application interfaces, infrastructure and network layouts based on interested parties; 3) Clarify, document and limit objective collection using personal data; 4) Identify all security and privacy risks; 5) Conduct privacy impact assessment of all IoT devices and data components; 6) Develop IoT privacy features; 7) Implement IoT security and privacy controls; 8) Continued review of the effectiveness of privacy controls and identify new privacy risks (BENDER et al., 2017).

Sedenberg, Chuang and Mulligan (2016), reinforcing the need to work on data privacy in a transparent manner since the beginning of the projects, 6 more recommendations were listed that can be adopted by any area as shown in (Table 4).

Table 4. The Six Principles of Privacy by Design.
Source: Schartum (2016).

Nº	Recommendations
1	Data Access and Review;
2	Presentation of user's privacy and consent policies;
3	General Privacy Controls;
4	Awareness of existing laws and potential use of data;
5	Responsible data sharing;
6	Anticipate new knowledge and unintended consequences.

In addition to the principles presented above, the 5 variables of the Unified Theory of Acceptance and Use of Technology (UTAUT), built on previous research on the acceptance of technologies. UTAUT explores the relationship between user factors with the intention of accepting new technologies or information systems as described in (Table 5) (BU et al., 2021).

Table 5. UTAUT Variables.
Source: Bu et al. (2021).

Nº	Variables
1	Behavioral intent to implement PbD;
2	Performance expectation regarding the PbD implementation;
3	Expectation of effort regarding the implementation of PbD;
4	Social influence on the implementation of PbD;
5	Enabling conditions for the use of PbD.

In order to facilitate the understanding of the parties involved in projects based on PbD, given this infinity of principles, recommendations and technologies, there is a proposal to use a schematic and unified graphic/visual language, capable of translating the conformity of a system with the law of data protection. Known as Petri nets, which has been in existence for over 50 years, it is accepted as an ISO standard and a way to make complex software issues visible and more readable for professionals, lawyers and scientists who are not technology specialists. The Petri

language is composed of symbols that represent the states (circles), transitions (rectangles) and the data processing flow with connections and arrows (HERNÁNDEZ-RAMOS; BERNABÉ; SKARMETA, 2016). In this proposal, design as a visual language plays an essential role in communication, legal and technical documentation of software and IoT devices.

Another study with usage of the Pythia application, which provides contextual suggestions for tourism, demonstrates that keeping data "on the user's side" and using data generalization techniques are less invasive practices that provide greater security when it comes to IoT (SEDENBERG; CHUANG; MULLIGAN, 2016). However, even with these friendly practices, it was identified that users did not feel comfortable knowing that the application collected personal data, causing some to not even want to install it. From this perspective, in addition to ensuring security and privacy, designers need to work to gain the trust of users so that products and/or services based on IoT manage to be successful.

In this regard, the analysis of 253 practices in the Chinese IT industry, which aim to implement systems based on Privacy by Design, also contributes. Placing Information Systems Engineers at the center of the discussion about privacy, especially as these professionals work directly with data collection through the use of technology. Still in this scenario, the implementation of PbD was identified as capable of positively influencing the behavior of engineers not only in the digital sphere, but also in the physical one (BU et al., 2021).

Physical/digital behavioral change is important to prevent data leaks or security breaches that could harm thousands of people. This new paradigm allows professionals a broad view of issues that were not considered or perceived before. However, there is a need to encourage these practices to realize a cultural change (BU et al., 2021).

From this perspective, the same can be applied to design professionals, who need to encourage PbD practices in the scope of service design and inclusive to the point of using them as competitive differentials without limiting the efficiency and capabilities of technologies (ROMANOU, 2018).

The regulation of the European Union (EU), through the General Data Protection Regulation (GDPR), also contributes to the analysis of this new context. It indicates that data controllers must ensure that only data necessary for each purpose are used and stored, and that the data is not made available to third parties, also pointing out the following principles (ROMANOU, 2018):

- Principle of legal processing;
- Specification principle and purpose limitation;
- Data quality principles (relevance, accuracy, and limited retention);
- Fair processing principle (transparency, establishment of trust);
- Principle of responsibility (implementation of measures to safeguard data protection, demonstration of compliance with protection rules).

Another possible way to achieve data privacy is linking access to data using biometric data, this way the information would be more protected, this encryption would make access by third parties more difficult (ROMANOU, 2018). Data minimization, encryption, anonymization, pseudonymization, regular impact assessments, risk assessments and other tools in combination with regulatory guidelines should support a more secure environment with fewer data breaches and privacy concerns (ROMANOU, 2018).

Through a broad approach that used a SWOT analysis matrix (strengths, weaknesses, opportunities and threats), the main aspects to be observed within a company about PbD were described according to different strategies (Table 6) (ROMERO; HEREDERO, 2017).

Table 6. Strategies to be observed about PbD.
Source: Romero and Heredero (2017).

Strategy	Observation
Offensive (strengths + opportunities)	Formalize the practice of PbD in business processes.
	Include processing process improvement routine considering privacy.
	Obtain, whenever possible, certifications in privacy and quality standards that prove the performance with privacy.
Defensive (strengths + threats)	Communicate to data owners about the privacy approach from the design adopted by the company and the benefits that this entails.
	Carry out marketing actions aimed at communicating the data processing that companies perform in terms of privacy protection.
	Standardize tasks that help manage privacy from the definition of the process and that impact as little as possible in terms of time and costs of management resources in companies.
Reorientation (weak points + opportunities)	Raise awareness among managers to consider privacy as part of all decisions involved in collecting and sharing personal data.
	Integrate privacy processing into the cycle steps process.
	Develop a culture of privacy awareness among employees.
	Conduct campaigns and training programs for employees in the process phases to raise awareness of the need to integrate privacy into the design process.

Survival (weak points + threats)	Promote and collaborate with consulting companies in the use of integrated privacy methods in defining of processes.
	Create work profiles oriented at organizational levels to support a culture of privacy.
	Incorporate privacy risks in the analysis and management of risks carried out in the company.

Another possible way to achieve data privacy is linking access to data using biometric data, this way the information would be more protected, this encryption would make access by third parties more difficult (ROMANOU, 2018). Data minimization, encryption, anonymization, pseudonymization, regular impact assessments, risk assessments and other tools in combination with regulatory guidelines should support a more secure environment with fewer data breaches and privacy concerns (ROMANOU, 2018).

- **Different degrees of decision-making power regarding the use of child-centred guidelines and participatory design research with young people;**
- **Wide range of approaches that fit the umbrella term of participatory design but differ in that they involve young people as consumers or citizens;**
- **Use participatory design with young people to serve empowerment rather than being a decoration.**

Final Considerations

As we have seen, this study sought to establish an overview of the state of art from a review of current literature, contributing to the design of services and inclusive design with practices appropriate to the context of product and service projects, based on the application of PbD guidelines, in order to comply with the new General Data Protection Law in Brazil (Law No. 13.709 of 2018) (BRASIL, 2018).

The research's guiding question can be answered based on a synthesis of recommendations, conducts and good practices related to data privacy and identified in the BRSR, as shown in (Table 7) below.

In it, 10 recommendations are pointed out that can be incorporated into the design of services and inclusive design for the design of products and services with an inclusive approach based on the IoT. These practices can be applied to other areas, such as the development of smart cities.

Table 7. Good practices for service design and inclusive design.
Source: The authors (2021).

Nº	Recommendation, conduct and/or good practice
1	Work with multidisciplinary teams (lawyers, programmers, suppliers, manufacturers and users);
2	Apply generalization and data storage techniques on the user side;
3	Find the appropriate framework for the project context to implement data privacy (field, segment, region, public and/or country), each area has its particularities regarding data privacy;
4	Working on the user experience in order to acquire the user's trust in addition to the processing of collected data;
5	Use visual languages to document and demonstrate to lay people how and where the collected data are used;
6	Encourage PbD practices in design processes in public and private spheres (companies, universities, entities);
7	Link data access using biometric data;
8	Use blockchain technology to track transaction and authenticate data;
9	In addition to being user-centered, the use of participatory design is recommended;
10	Consider sharing data with the scientific community to advance treatments and knowledge about vulnerable individuals.

Therefore, an initial exploratory study, and further studies should deepen in terms of a better definition or creation of methods that unify approaches centered on the user and PbD, making this practice less complex and more participatory. It was evident with this that there are few studies that demonstrate the application of inclusive design and privacy issues in IoT products and services, which was considered a worrisome gap given the importance of including people with disabilities, elderly and disadvantaged people.

Particularly, regarding the design of services, it was possible to identify a set of practices that can be adopted in user-centered design processes. However, the lack of a standard and the divergence of legislation between countries or certain areas, can become a greater challenge for designers.

Another issue that can be explored in further investigations concerns the creation of techniques or tools to assess the users' perception of data security, since many products and services, even after the application of PbD, made some users not feel comfortable with the collection of personal data.

References

ABDUL-GHANI, Hezam Akram; KONSTANTAS, Dimitri. A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. **Journal of Sensor and Actuator Networks**, v. 8, n. 2, p. 22, 2019.

BENDER, Jacqueline Lorene et al. Ethics and privacy implications of using the internet and social media to recruit participants for health research: A privacy-by-design framework for online recruitment. **Journal of Medical Internet Research**, v. 19, n. 4, p. e7029, 2017.

BRASIL. Lei 13.709 de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Diário Oficial da República Federativa do Brasil, 15 ago. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/ L13709.htm, last accessed 2019/20/10.

BU, Fei et al. Motivating information system engineers' acceptance of Privacy by Design in China: An extended UTAUT model. **International Journal of Information Management**, v. 60, p. 102358, 2021.

CAVOUKIAN, Ann. Privacy by design [leading edge]. **IEEE Technology and Society Magazine**, v. 31, n. 4, p. 18-19, 2012.

CHAUDHURI, Abhik; CAVOUKIAN, Ann. The proactive and preventive privacy (3P) framework for IoT privacy by design. **Edpacs**, v. 57, n. 1, p. 1-16, 2018.

CONFORTO, Edivandro Carlos; AMARAL, Daniel Capaldo; SILVA, SL da. Roteiro para revisão bibliográfica sistemática: aplicação no desenvolvimento de produtos e gerenciamento de projetos. In **VIII Congresso Brasileiro de Gestão de Desenvolvimento de Produto**. Porto Alegre, RS, Brasil, v. 8, 2011.

DIVER, Laurence; SCHAFER, Burkhard. Opening the black box: Petri nets and Privacy by Design. **International Review of Law, Computers & Technology**, v. 31, n. 1, p. 68-90, 2017.

EFRAIMIDIS, Pavlos S. et al. A privacy-by-design contextual suggestion system for tourism. **Journal of Sensor and Actuator Networks**, v. 5, n. 2, p. 10, 2016.

FRANCELIN, Marivalde Moacir. Fichamento como método de documentação e estudo. **SILVA, JFM**, 2016.

GEA, Tomas et al. Smart cities as an application of internet of things: Experiences and lessons learnt in barcelona. In: **2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing**. IEEE, 2013. p. 552-557.

GOMES, D.; QUARESMA, M. **Introdução ao design inclusivo**. Appris, Curitiba, 2018.

HERNANDEZ-RAMOS, Jose L.; BERNABÉ, Jorge Bernal; SKARMETA, Antonio. ARMY: architec-

ture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. **IEEE Communications Magazine**, v. 54, n. 9, p. 28-35, 2016.

LOWDERMILK, Travis. **Design Centrado no Usuário**. Novatec, São Paulo, 2013.

MATTOS, P. D. C. **Tipos de Revisão de Literatura**. Unesp, Botucatu, 2015. https://www.fca.unesp.br/Home/Biblioteca/tipos-de-evisao-de-literatura.pdf, last accessed 2021/05/10.

DE OLIVEIRA, Nairobi et al. Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). **Revista Eletrônica de Iniciação Científica em Computação**, v. 17, n. 4, 2019.

PADYAB, Ali; STÅHLBRÖST, Anna. Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. **Digital Policy, Regulation and Governance**, 2018.

PERERA, Charith et al. Privacy-by-design framework for assessing internet of things applications and platforms. In: **Proceedings of the 6th International Conference on the Internet of Things**. 2016. p. 83-92.

PORAMBAGE, Pawani et al. The quest for privacy in the internet of things. **IEEE Cloud Computing**, v. 3, n. 2, p. 36-45, 2016.

ROGERS, Yvonne; SHARP, Helen; PREECE, Jennifer. **Design de interação**. Bookman Editora, 2013.

PREUVENEERS, Davy; JOOSEN, Wouter. Security and privacy controls for streaming data in extended intelligent environments. **Journal of Ambient Intelligence and Smart Environments**, v. 8, n. 4, p. 467-483, 2016.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico.** 2ª Edição. Editora Feevale, 2013.

ROBLES, Tomás et al. Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design. **International Journal of Distributed Sensor Networks**, v. 16, n. 5, p. 1550147720912110, 2020.

ROMANOU, Anna. 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.

ROMERO, Santiago Martín-Romo; DE-PABLOS-HEREDERO, Carmen. Contribution of Privacy by Design (of the Processes). **Harvard Deusto Business Research**, v. 6, n. 3, p. 176-191, 2017.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO M. D. P. B. **Metodologia de Pesquisa**. 5. Ed. Porto Alegre: Editora Penso, 2013.

SCAVONI, G. dos S., & BÜHRING, M. A. Uma ótica sobre cidades inteligentes. **RJLB**, Ano 7, nº 4, p. 655-701, 2021.

SCHARTUM, Dag Wiese. Making privacy by design operative. **International Journal of Law and Information Technology**, v. 24, n. 2, p. 151-175, 2016.

SEDENBERG, Elaine; CHUANG, John; MULLIGAN, Deirdre. Designing commercial therapeutic robots for privacy preserving systems and ethical research practices within the home. **International Journal of Social Robotics**, v. 8, n. 4, p. 575-587, 2016.

SEMANTHA, Farida Habib et al. A systematic literature review on privacy by design in the healthcare sector. **Electronics**, v. 9, n. 3, p. 452, 2020.

AN, Seyun; KIM, Sungwhan; KIM, Soyeon. Necessity of the Needs Map in the Service Design for Smart Cities. **Frontiers in Psychology**, v. 11, p. 202, 2020.

STICKDORN, Marc; SCHNEIDER, Jakob. **Isto é design thinking de serviços: fundamentos, ferramentas, casos**. Bookman Editora, 2014.

WAHLSTROM, Kirsten et al. Privacy by design. **Australasian Journal of Information Systems**, v. 24, 2020.

ZAMAN, Bieke. Designing technologies with and for youth: Traps of privacy by design. **Media and Communication**, v. 8, n. 4, p. 229-238, 2020.

Recebido: 10 de fevereiro de 2022.

Aprovado: 11 de fevereiro de 2022.