sustainability

MDPI

Article

Personal Data Management in Smart Product-Service Systems: Preliminary Design Strategies to Avoid User Manipulation in Democratic Processes

Alessandra C. Canfield Petrecca [1,2,*], Carlo Vezzoli [1] and Fabrizio Ceschin [2]

[1] LeNSlab Polimi, Department of Design, Politecnico di Milano, 20158 Milan, Italy; carlo.vezzoli@polimi.it

[2] Design for Sustainability Research Group, Brunel Design School, College of Engineering, Design and Physical Sciences, Brunel University of London, London UB8 3PH, UK; fabrizio.ceschin@brunel.ac.uk

* Correspondence: alessandracaroline.canfield@polimi.it

Abstract: The use of digital technologies in Product Service Systems (PSSs) has increased in recent years. More and more smart devices are used in these models, collecting significant amounts of data to provide personalized and responsive products and services. However, data extraction has been causing disruptions in the social sphere, manipulating users, threatening democratic processes, and harming the social dimension of sustainability. To mitigate these problems associated with user data, some solutions on the market claim to take a more ethical approach. This article presents the preliminary results of a study aiming to understand what features in these solutions may favour the resilience of democratic processes and reduction in user manipulation due to personal data extraction and personalized activity. It also examines how designers can use them to develop smart PSSs that incorporate these elements and features in their process. Based on a literature review, three key elements relevant to personal data and democracy were assessed and applied to analyze 30 cases. The results provided a preliminary list of 46 features and 15 strategies for designers to embed these elements in the design of smart PSSs, as well as a conceptual framework. The study concludes with recommendations for future research.

Keywords: smart sustainable product-service systems design; personal data; user manipulation

check for updates

Citation: Canfield Petrecca, A.C.; Vezzoli, C.; Ceschin, F. Personal Data Management in Smart Product-Service Systems: Preliminary Design Strategies to Avoid User Manipulation in Democratic Processes. *Sustainability* **2024**, *16*, 10110. https://doi.org/10.3390/su162210110

Academic Editors: Dun Liu, Decui Liang and Yinfeng Du

Received: 16 September 2024
Revised: 29 October 2024
Accepted: 11 November 2024
Published: 20 November 2024

1. Introduction

Digital technologies mark the current age [1]. However, as they are considered disruptive, they affect fundamental areas of society such as economic and political systems [2–4]. The extraction of data from different devices and the variety of information about users can create a surveillance state that challenges freedom and private life [5]. Algorithms and predictive models are embedded with opinions from their design as pre-established rules by the developer, creating indented and unintended manipulations [6]. Not only do they interfere in everyday life but they can also cause societal systemic problems, replicating and affirming patterns of exclusion. Furthermore, users' data (or personal data) can give unprecedented power to the hands of large technology companies that centralize data and those that can pay for their services to maneuver their audiences [7]. The system works in such a way that the user produces data by interacting with digital solutions and training predictive models. At the same time, the users consume personalized and often sponsored information (advertisements, search results, news, etc.) produced by these models and algorithmic functions [8]. This can significantly increase the likelihood that users will take positive action, resulting in profits and influence for technology companies and those who advertise with them. The impact on society can be seen in the spread of misinformation, polarization, and exclusion affecting democratic processes, as highlighted in news stories from around the world, such as the Cambridge Analytica case [9]. This underscores the importance of ongoing discussions about the use of personal data.

In Product Service Systems (PSSs), digital technologies can potentially support different design strategies for sustainability. Potential benefits include improving workers' conditions, e.g., [10,11], favouring the inclusion of people who live in remote areas, and developing better services and products, e.g., [12,13]. The application of sensors and the Internet of Things (IoT) has become increasingly common to better understand user needs, leading to the enhancement and creation of innovative services and products [10,14]. Smart products and services have further evolved PSSs in connectivity and intelligence [15]. However, few articles cite concerns about the use of data and how it affects society [16].

It is essential to consider crucial issues such as data extraction, violations of privacy and surveillance, potential barriers to accessing information and user manipulation in products and services. To that end, it is necessary to ensure that digital technologies are designed to support democratic processes rather than reinforcing existing power imbalances [7,17]. Technology is not good or bad, nor neutral [18]. Even though the outcomes of the application of certain technology can be unpredictable, whether positive or negative, the design of a technological solution can still reflect the principles, morals and ethics of its creators [19]. Its design is shaped by people and, in turn, shapes societies [20]. Inspired by Democracy by Design (DbD), an approach that intends to incorporate democratic-related moral elements into the design process [19], this article presents an initial study that outlines a conceptual framework to be further explored in ongoing doctoral research on the design of Sustainable Product-Service Systems (S.PSSs) and digital technologies, focusing on the socio-ethical dimension of sustainability, in particular, the issue of mitigating the manipulation of users and citizens, in democratic processes, due to the extraction of personal data, favouring elements related to the resilience of democracy and personal data management in the design of these systems. Therefore, this study aims to answer the following research questions:

- What are the design features that can foster key democratic-related elements for personal data management in smart PSSs?
- How can these features be applied in the design of smart PSSs to mitigate user manipulation?

By analyzing existing solutions, this study aims to identify and systematize a set of preliminary design features and develop a conceptual framework to support the design knowledge base and know-how.

The paper is structured as follows: Section 2 presents the methodology, which includes a literature review to identify key elements related to democratic processes relevant to personal data and an exploratory analysis of digital solutions to assess their embodiment, leading to a set of preliminary strategies for designing Smart Product-Service Systems (smart PSSs). Section 3 discusses democratic-related elements and their relevance to personal data found in the literature: Privacy, Transparency, and Participation. Section 4 analyses thirty cases of digital solutions that deal with personal data, identifying forty-six features related to the elements, which were categorized into actionable strategies for smart PSS design. Finally, the Conclusions highlight the examples found and the strategies developed to integrate these elements into smart PSS design, aiming to enhance protection, awareness, control, and collaboration.

2. Method

Strategies and methods for designing PSSs for socio-ethical sustainability are scarce [21]. The existing ones, e.g., [21–23], do not directly and fully address the contemporary problems of digital technology in society [16]. In addition, the concept of Democracy by Design (DbD) is derived from Value Sensitive Design (VSD) [24], a design of technology approach that takes into account moral values during the design process [19]. However, the literature on DbD is also scarce and diverges in fields covering topics from computer engineering [24] to citizen education [25]. Nevertheless, VSD and DbD have been identified as promising concepts to tackle issues caused by digital technology for assisting democratic process resilience [17,26–28]. Friedman and Henry [19] affirm that the assumption of a specific set of moral elements for the VSD approach can risk favouring some over others, suggesting the definition of VSD as an activity in the project. Democracy is a complex concept that has many definitions and intertwined elements [29]. Therefore, a literature review was carried out to understand the existing knowledge on democracy and digital data and to establish an initial set of elements related to democracy and personal data. The intention was not to target publications addressing democracy in the context of the governance of a nation, such as decision-making processes, electoral systems, legislative bodies, etc. Instead, it intended to find elements, understood here as components connected with democracy, including instrumental factors that contribute to democratic systems and processes resilience. Complementary, pursue factors that could be favoured when designing solutions that deal with personal data to avoid user manipulation.

For the review, the terms democracy and data or digital were researched in the Scopus database (Table 1). The search was focused on articles published in the last 10 years, limited to English. The first result found 107 articles in total. The articles passed through three selection filters. First, the title, keywords and abstract were read (F1); then, the introduction and conclusion were read (F2); and finally, the full text was read (F3). After the filters, seven articles were considered relevant.

Table 1. Research string, result, and filters.

STRING	RESULT	F1	F2	F3
(TITLE (democracy) AND TITLE (data OR digital)) AND PUBYEAR > 2014 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE, “ar”)) AND (LIMIT-TO (LANGUAGE, “English”))	107	48	22	7

Publications were organized into an Excel (v.2410) spreadsheet, placing their basic information (author, year, abstract, keywords, and link for the document), a summary of the ideas on the article, and highlighted citations. Subsequently, the articles were grouped by similarity, and a keyword was assigned to each group, reflecting the saturation of the concepts identified. Due to the complexity of the subject, as a complementary resource and initial non-systematic literature review, grey literature, books, and reports were also considered. Three key elements emerged from these materials, Privacy, Transparency, and Participation, which are further presented in Section 3.

Subsequently, a qualitative exploratory analysis of cases of existing digital solutions was conducted. This aimed at understanding how the three elements identified in the literature were embedded in existing solutions. The decision to adopt an exploratory case analysis was made with the objective of maximizing breadth of observation rather than depth. This approach was selected with the intention of gaining insight into the implementation of democratic elements across a diverse range of existing solutions rather than focusing on the specifics of a limited number of solutions. While an alternative approach could have been considered (such as an in-depth case study), this would have resulted in a narrower scope for the framework. Therefore, it employs a sampling approach covering a wide range of cases, exploring their variety and aiming for a broader understanding of the phenomenon under investigation [30]. The observation of practises and their factors in relation to the established elements in real solutions [21] is applied to obtain information for a conceptual framework. For that, for each case, it was identified specific design features associated with the three key elements. These features were then clustered and systematized in a coherent framework and used to derive a preliminary set of design strategies. These strategies will be further validated in the future through other research methods, which will include the application of the strategies with experts and design practitioners.

The term ‘smart PSS’ can be defined as a smart, connected product that is integrated with e-services, with the objective of addressing consumer needs [12,14]. An example of this would be laundry machines with sensors and software that monitor and identify problems, integrated with a remote maintenance service. In a pilot, it was observed that the cases of smart devices exhibited features that could be interpreted as aligning with the elements. These features were either directly correlated to the product (e.g., a component as a removable battery or a cloud service) or indirectly correlated (e.g., a forum or policy of privacy by design). A review of these features in smart devices revealed a limited diversity identified. In addition, not many cases in the sector had a concern for data ethics. Furthermore, it should be noted that smart devices are connected solutions that collect and share data with other connected solutions, such as mobile phones, personal computers, smart TVs, and other devices or software. In fact, smart PSS can also be defined as "a platform service ecosystem, in which platform is made of smart products and smart services" [31]. It was thus decided that the scope of the cases should be expanded to encompass digital solutions that demonstrate a commitment to ethical practises regarding personal data (data ethics). This includes the provision of enhanced privacy, security, respect for local regulations, transparency, and other related considerations.

In order to find the cases, two lists of recommended digital products and services that aim for more ethical solutions towards data management available online were used: an independent project focused on digital and ethical solutions called privacytools.io and a non-profit independent organization on data ethics called dataethics.eu. From these two communities, a variety of cases involving personal data (such as browser, email, search engine, communication tool, etc.) were identified and considered. The solutions were subjected to a process of correlation with the elements, resulting in the extraction and listing of relevant features in an Excel spreadsheet accompanied by a brief description. Following the collection of several cases and the description of their features, it became evident that they were repeating, indicating that further cases were not needed since the theoretical saturation was achieved.

A process of coding for qualitative analysis was then carried out, merging and correlating features to form preliminary strategies. This reflective process allowed the iteration of the elements, features, and strategies (Figure 1). Initially, the extracted features were combined and condensed. For instance, particular forms of encryption were identified and merged into a single general description. During the first coding, the elements were used to group these generalized features, assisting in the understanding of the element's correlation to themselves, as the results presented in Section 4.2. Each feature was then coded with a verb relating to how they favour a more ethical approach to personal data in the solution for the reduction in manipulation of users aiming to extract possible strategies. For example, encryption was placed with the verb "alter" as it was described to alter data to not be understandable by outside viewers. After providing a code for each one of the generalized features they were then placed on a Miro board and grouped by similarity. This process of grouping provided a refinement of the definitions of features, and clusters emerged, indicating possible strategies, as presented in Section 4.3. The process of forming possible strategies led to iterations between the elements, features and strategies, as illustrated below and further presented in the results.

Overall, the methodology included a literature review to identify key democratic-related elements relevant to personal data. These elements were then used to analyze a set of existing digital solutions. In this analysis, specific features that embodied these elements were identified. Thirty cases were selected, resulting in the identification of forty-six distinct features, which were then grouped into fifteen clusters. Following the definition of these features and clusters, an initial set of strategies for the design of smart PSSs, grounded in the elements, were formed. These preliminary strategies aim for the integration of the elements into the design of Smart S.PSSs, inspired by the principles of Value Sensitive Design (VSD), aiming for more careful consideration of the ethical implications of digital technology [26].

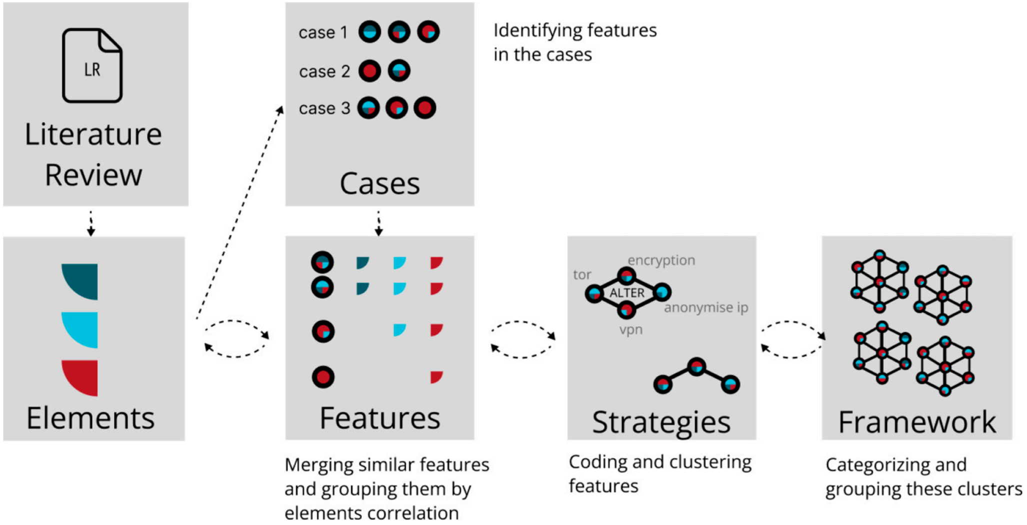

LR
Literature Review
Elements
case 1
case 2
case 3
Cases
Identifying features in the cases
Features
Merging similar features and grouping them by elements correlation
encryption
tor
ALTER
anonymise ip
vpn
Strategies
Coding and clustering features
Framework
Categorizing and grouping these clusters

Figure 1. Representation of the iterations in the methodology.

3. Democratic-Related Elements and Their Relevance to Personal Data

Debates about the meaning of democracy have generated a diversity of concepts ranging from the Greek dēmokratía to contemporary global democracy [22]. The epistemology of the term derives from Greek meaning "rule by the people" [32]. However, its definition is always striving for improvement [33]. The Cambridge dictionary describes it as an ethical ideal towards equality and freedom among people or a system of government based on this belief [34]. Since its origins, democracy as a set of ethical assets has been intrinsically linked to its form of government exchange and modifying each other [35]. Recognizing democracy's role as a set of political, ethical assets in peoples' lives, this research focuses on how democratic-related elements may contribute to a more ethical approach to personal data management in smart PSSs and to the resilience of democratic processes. Three key elements emerged from the literature review: Privacy, Transparency, and Participation.

3.1. Privacy

Privacy is a central theme in discussions about data, as most of the articles included in the literature review addressed the subject. Privacy, not only in relation to personal data, is vital for democracies, guaranteeing freedom of thought, individual choice and decision-making [35,36]. Personal data (or users' data) can be differentiated by three distinct sources. It can be volunteered, as provided directly by the user (e.g., name); observed, as captured by recording activities of users (e.g., GPS location); or inferred, as the results of data analysis and generation of new data (e.g., credit scores) [36]. Through digital technologies, information has been produced in unprecedented ways, and when accumulated in complex and voluminous sets, it is called big data. In acquiring intelligence from it, big data is analyzed, revealing patterns and correlations [37]. These technologies have been transforming how organizations and relations happen, being positive in many aspects. However, never before have public and private organizations had access to such "granular, immediate, varied, and detailed data" about their subjects [5]. Tracking and profiling users can be a powerful tool to influence behaviour and change outcomes [17,36]. Therefore, data have become a problem for people's privacy and democracies [35].

The rise of surveillance systems by governments creates a paradigm of democracy between control and freedom. Aradau and Mc Cluskey [38] affirm that this incoherence is due to a vision of collective uniformity that oversimplifies and generalizes security measures for control and overlooks minority issues, such as facial recognition technology and errors with people of colour. Saura García [39] explains that technology companies and their systems for data collection attract government support due to economic and political advantages, leading to digital expansionism and digital sovereignty strategies. Digital expansionism involves enhancing a nation's power over others or reducing rival influence, while digital sovereignty policies can lead to digital authoritarianism. Both forms of control and dominance over citizens can be achieved through improved user experience, convenience, and the incentivization of specific platforms, ultimately blurring the lines between cooperative and coercive control [39]. This secrecy and opacity can be seen as democracy erosion agents, making surveillance unacceptable [38]. These forms of control ignore that plurality and self-determination are often considered crucial to democratic systems, providing valuable criticism that prevents the concentration of power by institutions [38].

Digital privacy involves the protection of personal data and can thus become a key element that protects other democratic-related elements. Moreover, the concept of a data-owning democracy can be seen as complementary to privacy and data regulation [36]. While it does not fundamentally eliminate harmful data extraction mechanisms, it provides additional tools to empower citizens alongside existing privacy and antitrust measures [36]. Data protection is critical to a just digital economy, and perhaps integrating data flows into a political economy that extends beyond solutions can empower citizens [36]. Nevertheless, despite the efforts of governments to regulate issues of data extraction and appropriation of information, it is essential to continue developing strategies to strengthen democratic systems [39].

3.2. Transparency

Although data ownership can be linked to privacy, it is also linked to transparency, as it increases user knowledge of their data. Users are often unaware that they do not fully own their data, as many types of digital records are not owned by the individuals to whom they belong [36]. As Aradau and Mc Cluskey [38] affirm, "the right to an effective remedy is entirely meaningless if one is unaware of being subjected to surveillance". Better access to information regarding data source, storage and processing, as well as its compliance with regulations, is essential. Transparency is crucial for democratic systems to empower individuals, build knowledge, and promote accountability, deliberation, and participation [28,40]. It ensures privacy is not violated without justification and authorization and assures users that adequate policies are in place to prevent data misuse [28]. Transparency in the context of digital solutions, design, and sustainability involves the provision of clear, contextual, complete, consistent, and accurate information [41].

Robbins and Henschke [28] discuss the importance of transparency in addressing disruptions caused by digital solutions in democracies, noting that transparency can be an enabler and a detractor (e.g., threaten the security of digital systems). Nevertheless, the barrier to user's understanding of the technology behind digital solutions and the inherent opacity of algorithms used in the process of data, especially due to machine learning and AI (sometimes called black boxes) [28], make transparency necessary. Technology companies have a certain dominance over users and stakeholders in which, with algorithms, they can curate and narrow individual choices presented to users, supporting polarization affecting more deliberative or antagonistic actions, and consequently shaping the public sphere [42]. The content moderation practises conducted by social media companies, for example, are non-transparent and consequently unaccountable [42]. As argued by Aradau and Mc Cluskey [38], plurality is important for effective democratic control, and the public must be able to see proposals or measures that are not tailored for them and be prepared to organize in opposition. However, this plurality has been hindered by big tech corporations due to the use of curated content and algorithmic personalization [42]. Transparency can be amplified by providing options for the users to understand algorithmic rules and choose these rules in a manner that can contribute to more participative actions. Aytac [42] suggests opening choices for users presenting options of different types of algorithms, such as deliberative, antagonistic, or mixed output modes, to make systems more pluralistic.

3.3. Participation

Indeed, data extraction and decisions about what to do with this powerful resource should not be concentrated in the hands of a few companies or be an opaque process in solutions. Users should have a say in how their data are used, actively participating in the development of system structures, including algorithms and storage decisions. Movements of data openness, such as open source and open data, approach data as a communitarian resource and can be seen as a broader perspective of transparency towards participation. Baack [43] affirms that activists of open data believe in making available, along with the open-source code of digital solutions, the collected raw data so that others can process and make their own interpretation of it. For the authors, this could improve not only users' choices but also their agency towards deliberation for a critical examination of ideas and the development of new rationalities [43]. Democracy with digital technologies could be seen as the concept of collective intelligence, where the experience of participation is capable of being educative [44]. Collective intelligence aims to improve human intelligence with technology rather than making technology more intelligent than humans [44].

Democracy is based on the free will of people to decide their own system and their full participation in this decision over all aspects of their life [45]. Participation empowers communities to gain and exercise control in a collaborative process of defining problems, identifying and applying assets and finding solutions for their own community [46]. The participatory process involves deliberation, which allows issues to be debated, positions to be explained, and compromises and solutions to be found [35]. Participation, together with deliberation, can be linked to the inclusion of users and other stakeholders in collective debate and decisions about personal data in the system and the distribution of power that data can give. The term participation here is used as one of the elements relevant to discussions around personal data to avoid manipulation in the context of democratic systems. However, transparency and availability of data do not ensure participation, as many users lack awareness and understanding of digital solutions. Intermediates, such as specialists or government organizations, can play a crucial role in engaging users by identifying valuable data for the community and transforming it into meaningful information, thereby empowering users and encouraging collaborative participation [43]. Nevertheless, it is also important to critically examine and balance these ideas and ensure protection against data violation and manipulation [43].

3.4. Relations and Guiding Questions

Overall, the three elements presented are intrinsically interconnected. Transparency and participation are mutually reinforcing, as transparency involves openness of information about the system and its collection of data. This can amplify participation in decision-making processes over the development of the system, thereby distributing control to users over their data and proportionating knowledge building. Although these ideas appear opposite to privacy, the opaque intentions behind data use on solutions support increased transparency over solutions structures. Nevertheless, a balance between transparency and privacy may be essential since complete privacy would undermine the purpose of smart technologies. In contrast, complete transparency, especially concerning personal data, could impede individual freedom. To better orient the features analysis of the cases, the following guiding questions were formulated (Table 2):

Throughout the literature, privacy, transparency, and participation have emerged as relevant concepts for the relationship between personal data and democracy-related factors for the resilience of democratic systems and have therefore been defined here as elements relevant to personal data. However, following the understanding of Friedman and Henry [19], these principles are not fixed as they are also subject to iterations. These elements were used to analyze existing solutions and their features, as presented below.

Table 2. Guiding questions of the democratic-related elements for personal data.

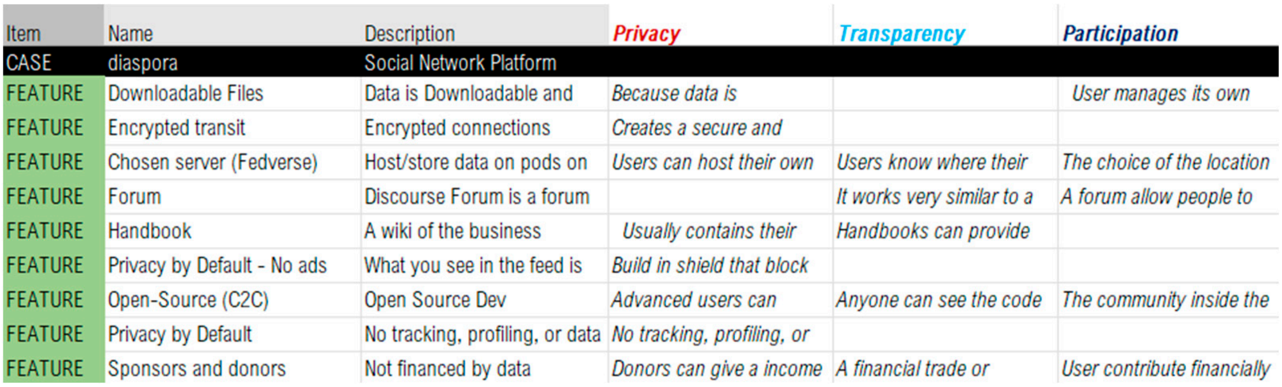
Element	Guiding Questions
● Privacy	Does the solution enhance users' privacy, reducing manipulation, or improving their self-determination and freedom over their data?
● Transparency	Does the solution provide accurate and clear information about how and what data are used and how they are regulated, ensuring awareness, knowledge building, and accountability?
● Participation	Does the solution encourage different stakeholders to come together, discuss, and exchange ideas about how their data are being used and their participation in the collaborative development and management of the system (rather than passive exploitation of data)?

4. Cases and Features Analysis

4.1. Sample of Cases

As presented in the methodology, the case analysis intended to explore practises of personal data management in alignment with the elements. Two lists of recommended digital products and services designed for more ethical data management solutions available online were used to identify the cases: dataethics.eu/tools and privacytools.io. The first is a nonprofit, independent organization that provides a list of solutions aligned with the European General Data Protection Regulation (GDPR). The second, Privacy Tools, is a community established after 2015 Snowden's publications of the NSA documents and aims to provide solutions against mass surveillance. In these websites, they present a list of tools separated by their main functionality. Selecting one from each category, it was possible to collect and make a list of cases considering different offers, such as browsers, search engines, communication tools, privacy knowledge management, web statistics tools, and others.

After an initial selection, the cases and their features were listed on a spreadsheet with a brief description and crossed with the elements, describing how they favour them. Figure 2 presents an extract from this spreadsheet for one of the cases, showing its list of the features, their description, and notes on each element.



Item	Name	Description	Privacy	Transparency	Participation
CASE	diaspora	Social Network Platform			
FEATURE	Downloadable Files	Data is Downloadable and	*Because data is*		*User manages its own*
FEATURE	Encrypted transit	Encrypted connections	*Creates a secure and*		
FEATURE	Chosen server (Fedverse)	Host/store data on pods on	*Users can host their own*	*Users know where their*	*The choice of the location*
FEATURE	Forum	Discourse Forum is a forum		*It works very similar to a*	*A forum allow people to*
FEATURE	Handbook	A wiki of the business	*Usually contains their*	*Handbooks can provide*	
FEATURE	Privacy by Default - No ads	What you see in the feed is	*Build in shield that block*		
FEATURE	Open-Source (C2C)	Open Source Dev	*Advanced users can*	*Anyone can see the code*	*The community inside the*
FEATURE	Privacy by Default	No tracking, profiling, or data	*No tracking, profiling, or*		
FEATURE	Sponsors and donors	Not financed by data	*Donors can give a income*	*A financial trade or*	*User contribute financially*

Figure 2. Image of the spreadsheet with Diaspora case and its features with descriptions.

The collection and analysis of cases stopped when the identified features started to repeat, and no new feature was found. This indicated that the theoretical saturation was achieved. Most of the cases had a main offer with other products and services related to it. The table below presents the final list of cases selected (Table 3).

A total of thirty cases were selected, representing a diverse range of commonly used digital solutions, including browsers, email tools, social media platforms, mobile phones, and operating systems. The collection also included cases focusing on more specialized tools, such as data analysis and management solutions. The diversity of cases assisted in the identification of distinct features related to the element under investigation.

Table 3. List of cases and their products and/or services offered.

Name	Offer
Librem 5	Mobile phone, sim card
Home Assistant	Central smart home system management app, cloud, hub
diaspora	Social media platform, distributed data management
Brave	Browser; search engine; virtual private network (VPN); ad-block; artificial intelligence (AI) chat
Signal	Communication app
Skiff	Email manager
GitLab	Development, security, and operations (DevSecOp) platform
ErnieApp	Privacy knowledge manager (PKM)
matomo	Web statistic tool
Whonix Project	Operational system
DeepL Translate	Translation
Obsidian	Digital Notepad
Qwant	Search engine; ad-block; maps
hCaptcha	Captcha
Cludo	Search engine
uBlock Origin	Ad-block
Whereby	Webinar app
TOR browser	Browser
LimeSurvey	Feedback tool
SupWiz	Chatbot
Vivaldi	Browser; e-mail; calendar; notepad; translator; contacts
Brevo	Newsletter tool
Varonis	Privacy knowledge manager (PKM)
Hetzner	Cloud
Xing	Social media
Open Street Map	Maps
Etracker	Web statistic tool
Clever Reach	Newsletter
DuckDuckGo	Browser; search engine; maps; e-mail
Nextcloud	Cloud; documents suite; chat; calendar

4.2. Features and Elements

Features in this study are understood as any part of the offer that could be correlated to the democratic-related elements associated with personal data management. They were part of the offer directly, such as components (e.g., ad-blocker and downloadable files) and embedded services (e.g., server choice and encryption), and indirectly, such as management factors of the institution (e.g., privacy by design policies) or more general services (e.g., forum or open-source community and its management).

Following an examination of the cases, it was found that some of the unique features were present in multiple denominations yet exhibited significant overlap. For instance, the terms 'privacy by default', 'privacy by design' and related privacy policies demonstrated similarities despite having distinct nomenclature. Subsequently, an iterative process was initiated to ascertain which features could be merged and which were part of a group that could provide the basis for a strategy. To this end, an online tool for a virtual whiteboard (Miro v.2024) was employed in parallel with the spreadsheet, facilitating the visualization of similarities. The features from the cases were transferred to the whiteboard as 'post-its' and rearranged into groups. One of the arrangements was to place them with the correspondent element, which helped to elucidate how the elements could be correlated to the features and between themselves. The final list of features is presented below, grouped by the democratic-related element/s they contribute to the following (Table 4):

Table 4. Features associated by their elements.

Features	Elements
Anonymise IP; Encryption; VPN; TOR; Crypto transactions; Decentralized storage; Matrix API	● Privacy
Alias domains; Explainable AI (XAI); Open Data; Handbook; Digital Literacy content; Open Changelog;	● Transparency
Opt-in ads and rewards; Opt-out tracking; Physical Kill Switches; AdBlock; Certifications; Law Compliance; Policies; Ethical behaviour reward; Ethical actions; Private server; Regional server; Disclosed server location; AI Automated Data Security; Attack resistance management; Compliance scan; Downloadable Files; Data Ownership; Downloadable Software; Self-hosted server; Open file format;	●● Transparency Privacy
Forum; External webchat channel; Open-Source; external parts; Open-Source; Community driven; Support C2C; Local Knowledge; Sponsors and donors; Financial Trade; Employee ownership;	●● Participation Transparency
Chosen server; Blocklist; DPO;	●●● Participation Transparency Privacy

● Participation; ● Transparency; ● Privacy.

From this analysis, it was observed that the elements of Transparency and Privacy are present in most of the features, which shows their strength in the current solutions. The least present element is participation, which can also be linked to more specialized features to facilitate the user's dialogue and interaction with the solution structure. Although each feature was initially directly related to one element, it was observed that they usually contribute to multiple elements. Overall, we can identify five different combinations:

- ● *Privacy*: The characteristics of this category are exclusively associated with the concept of privacy. They can be favoured independently of the user's awareness. For example, encryption can safeguard and enhance the user's interests without their knowledge. This illustrates that strategies related to privacy do not necessitate the user's awareness. Privacy can assist in the improvement of people's freedom and reduction in manipulation; however, without transparency and the inclusion of users in deliberations and collaboration about the development of solutions, privacy support to avoid manipulation is limited.
- ● *Transparency*: The Alias Domains, XAI, Open Changelog, and Open Data features offer users insights into the ways in which data are utilized. The Handbook and Digital Literacy content facilitate the development of knowledge among users. Although they assist users seeking accountability, they do not necessarily prevent data privacy from being violated.
- ●● *Privacy and Transparency*: The features here show the transparency and privacy possible relations. They provide higher privacy for users on their data and present them with information on what is happening, with the option to modify this information. For example, the "opt" functions indicate that data collection is occurring and allow users to enable or disable these functionalities within the solution. However, they lack a mechanism to enable users to provide feedback and participate in the development of the system structure.
- ●● *Participation and Transparency:* The features of this group provide a way for the user to be involved in the development of the solution structures. Although they may offer privacy to users who demand accountability, they do not guarantee or aim to do so. Thus, privacy enhancement through these features is not certain.
- ●●● *All elements*: The Blocklist, Chosen Server, and DPO features have shown that there are possibilities for having the three elements together. Transparency appears to

facilitate a connection between the elements of privacy and participation but does not automatically guarantee them.

● ● *Participation and Privacy:* None of the presented features demonstrated the combination of privacy and participation or only participation without transparency. Without the openness of information, people cannot learn about problems and participate in the changes.

Grouping the features according to the elements permitted an examination of the interrelationships between the elements. However, a more effective method of classification and reflection was clustering according to their functionality.

4.3. Clusters and Preliminary Strategies

The features were grouped into distinct clusters based on their functional characteristics, with attributions derived from their descriptions as presented in the case studies (see the list of features in Appendix A). These clusters were predominantly concerned with transparency and privacy. Participation involved only six of the features (Block, Locate, Monitor, Assemble, Contribute, Financial support), while Privacy involved seven (Alter, Block, Comply, Decentralize, Incentivize, Locate, Monitor) and Transparency fourteen (Block, Comply, Incentivize, Inform, Locate, Monitor, Own, Port, Switch, Assemble, Contribute, Support financially, Trace).

It was observed that within the same cluster, there were multiple connections to the elements. Three clusters were identified as exhibiting non-homogeneous characteristics. In the "Block" category, the Blocklist feature has been grouped with AdBlock. Although both are related to the concepts of privacy and transparency, Blocklist differs in that it allows user participation through external forums where users can suggest web addresses to be added to the list. This affords users the opportunity to exert direct influence over the web addresses that are blocked by the solution. In the "Monitor" category, the DPO allows users to provide feedback, while in the "Locate" category, the Chosen Server feature enables users to choose the server location or host it themselves. This results in greater participation compared to other features in the same category that only provide information. As the categorization through the elements was not homogeneous, the clusters were grouped into four larger categories: (a) User data protection, (b) User guidance, (c) User control, and (d) User collaboration. The compilation is presented below (Table 5).

Table 5. Clusters that support democratic-related elements based on the functionality of the features.

Cluster	Features	Elements
User data protection		
Alter	Anonymise IP; Encryption; VPN; TOR	●
Decentralize	Crypto transactions; Decentralized storage; Matrix API	
Block	AdBlock	●●
	Blocklist	●●●
User guidance		
Inform	Open Data; Handbook; Digital Literacy content; Open Changelog	●
Trace	Alias domains; XAI	
Incentivize	Ethical behaviour reward; Ethical actions	●●
Comply	Certifications; Law Compliance; Policies	
Monitor	AI Automated Data Security; Attack resistance management; Compliance scan	
	DPO	●●●

Table 5. *Cont.*

Cluster	Features	Elements
User control		
Own	Downloadable Files; Data Ownership; Downloadable Software; Self-hosted server	●●
Port	Open file format	
Switch	Opt-in ads and rewards; Opt-out tracking; Physical Kill Switches	
Locate	Private server; Regional server; Disclosed server location	
	Chosen server	●●●
User collaboration		
Assemble	Forum; External webchat channel	●●
Contribute	Open-Source external parts; Open-Source; Community driven; Support C2C; Local Knowledge	
Support financially	Sponsors and donors; Financial Trade; Employee ownership	

●; Participation; ● Transparency; ● Privacy.

These clusters constituted a draft version of the preliminary strategies. The objective of user data protection is to ensure the protection of personal data, whereas the purpose of the user guidance clusters is to provide educational resources. Clusters associated with user control relate to features that afford users a certain degree of control over the system, allowing them to become more active participants in its operation. Finally, user collaboration clusters permit direct collaboration between users and the solutions, thereby influencing its structure.

Furthermore, despite the lack of uniformity in the elements across the categories, there is a clear correlation between them and more specific ones. In the initial category, all nine features are related to privacy, whereas transparency and participation vary, with the latter being the least present. In the "User guidance" category, all eleven features are related to transparency. In the third category, "User control", the features are mostly related to transparency and privacy. In the final category, "User collaboration", all features are related to transparency and participation.

5. Preliminary Strategies

As presented above, the preliminary strategies were formulated to be used in the design of smart product-service systems embedding the elements. The found features that integrate each strategy can work as examples to be directly implemented in the design or as inspiration for new features.

In the realm of user data protection, and stronger on the element of privacy, three primary possible strategies have emerged:

- **Alter**: To alter or scramble personal data, making it unidentifiable to outsiders. Examples of features for this are IP anonymization, encryption, VPN and TOR.
- **Block**: To block the transmission of personal data to third-party applications, such as trackers and fingerprints. Examples of features are AdBlock and Blocklist.
- **Decentralize**: To use a type of decentralized personal data system to ensure that user data are not concentrated in a single organization. Examples of features include cryptocurrency transactions, decentralized storage, and matrix API.

In the category of user guidance, the strongest element is Transparency. The five possible strategies are as follows:

- **Comply**: To comply with personal data laws, regulations, and best practises and make them available and clear to the user. Examples of features include certifications, compliance disclosures and policy disclosures.

- **Incentivise**: To and its organization encourage data ethics actions, support research and development, and encourage users to refine their privacy standards and identify potential issues. Examples of features are rewarding ethical behaviour and ethical actions.
- **Inform**: To provide education and information to stakeholders and users about solution structures and data ethics. Examples of features include open data, manual, digital literacy content, and open changelog.
- **Monitor**: To continuously monitor and update its data ethics parameters and provide reports to users. Examples of features are AI automated data security, attack resistance management, compliance scan, and DPO.
- **Trace**: To provide a means for the user to trace the path or logic of their data process within the solution. Examples of features include alias domains and XAI.

For user control, the strongest elements are Privacy and Transparency. The five possible strategies are locate, own, port, and switch.

- **Own**: To allow users to own and manage their data. Examples of features include downloadable files, data ownership, downloadable software and self-hosted servers.
- **Switch**: To allow users to switch data collection on or off according to their needs. Examples of features include opt-in ads and rewards, opt-out tracking, and physical kill switches.
- **Locate**: To disclose to users the physical location where their data are stored and processed. Examples of features include private server, regional server, disclosed server location (with more precise location) and chosen server.
- **Own**: To allow users to own and manage their data. Examples of features include downloadable files, data ownership, downloadable software and self-hosted servers.
- **Port**: To allow users to port their data to other similar solutions, ensuring compatibility of data formats. An example of a feature is open file format.

Finally, in user collaboration, the elements are Transparency and Participation, and the three possible strategies are assemble, contribute, and support financially.

- **Assemble**: To provide a space for users to discuss data policies and processes. Examples of features include a forum on the main app or webpage of the solution and an external web chat channel.
- **Contribute**: To allow users to contribute to and change the structure and content of the solution. Examples of features are open-source external parts, open source, community-driven, support C2C, and local knowledge.
- **Support Financially**: To offer users the opportunity to financially support the solution for its economic sustainability, not based on data extraction. Examples of features are sponsors and donors, financial trading and employee ownership.

The four categories can be seen as a progressive engagement of users in a more active role in the decisions over their data, from features that support privacy by default to a deeper collaboration within the solutions aiming to mitigate/avoid user manipulation. Another point is that personal data can function as a private and shared resource to be defined individually and by the community of users. When collected and shared, it can benefit the individual since the system to be smart needs certain data to operate, but it also benefits the community by providing feedback on the product performance, resulting in updates. Furthermore, the preliminary strategies can trigger designers to consider the possible actions to be implemented in the design of smart PSSs with democratic-related elements and features provided as examples.

6. Conclusions

The study aimed to identify examples of personal data practises within existing solutions that favour democratic-related elements (Privacy, Transparency, and Participation) that can prevent user manipulation in smart PSSs. Then, it developed a set of preliminary strategies for incorporating these elements into the design of such PSSs.

A literature review on democracy and personal data revealed the importance of privacy, transparency, and participation. In the review, privacy was found to be vital for maintaining other democracy-related elements. The unprecedented collection and analysis of personal data through digital technologies pose significant privacy risks, with institutions now holding detailed data that can influence behaviour. Surveillance systems and digital sovereignty strategies by governments further threaten privacy, potentially eroding democratic systems. This element aimed to find features that enhanced users' privacy, reducing manipulation and improving their self-determination and freedom over their data. Complementary, transparency was found crucial for empowering individuals and promoting accountability in democratic systems. The inherent opacity of algorithms hinders plurality and effective control of users to avoid their manipulation. This element aimed to find features that provided accurate and clear information about how and what data are used and how it is regulated, ensuring awareness, knowledge building and accountability. Lastly, active user participation in processes regarding their data is fundamental for a robust democracy. Movements like open data and open-source software encourage viewing data as a communal resource, fostering critical examination and new rationales, contributing to the user's agency. However, balancing transparency and privacy is essential to protect individual freedom while ensuring the functionality of smart technologies. Collective intelligence believes that technology can enhance human capabilities and promote participatory and educative experiences. Participation, as an element, aimed to find features that encourage different stakeholders to come together, discuss, and exchange ideas about how their data are being used and their participation in the collaborative development and management of the system.

The identification of features and their subsequent clustering highlighted the interdependence of these elements, especially between transparency and participation, since the latter inherently depends on the former. Evaluating the elements within the four categories reveals that the combination of privacy and transparency is linked to user control over their own data since, without knowledge, control is not possible. Transparency and participation significantly influence the update and design of solutions, making users more active participants. Transparency without participation primarily serves an educational purpose; these features can subtly connect with privacy, as transparency fosters accountability and enhances privacy parameters within a solution. Conversely, privacy features tend to require less user involvement and function without active user engagement. This set of elements saturated concepts found in the literature related to personal data and democracy. Although the elements did not undergo radical changes in this study, they are not fixed and are subject to iterations beyond this article.

The existing features have demonstrated that the design of a smart PSS has the potential to incorporate democratic-related elements in the handling of personal data to avoid user manipulation. Democratic concerns over personal data are affected not only by technology but also by socio-political and regulatory contexts. Nevertheless, our research is conducted with a design perspective, focussing on the aspects that are subject to the direct influence of design(er). For this reason, the political and regulatory aspects are not fully taken into account.

These preliminary strategies are intended to be further iterated, with applications with design professionals and specialists for further validation. The material will be further elaborated to guide designers in developing smart PSSs with a higher level of social responsibility. With a particular focus on democratic-related elements, this approach seeks to address issues of manipulation through the extraction of data and the current deficit of research on ethical data approaches in smart PSSs.

Author Contributions: Conceptualization, A.C.C.P., C.V. and F.C.; Methodology, A.C.C.P., C.V. and F.C.; Formal analysis, A.C.C.P., C.V. and F.C.; Investigation, A.C.C.P., C.V. and F.C.; Writing—original draft, A.C.C.P. and F.C.; Writing—review and editing, A.C.C.P., C.V. and F.C.; Supervision, C.V. and F.C.; Project administration, A.C.C.P. and C.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Politecnico di Milano Scholarship of doctorate of the PNRR code 38-411-16-DOT1316795-1540.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Feature descriptions.

Feature	Description
Ad-Blocker	Block profiling, tracking, unwanted and illegal data collection.
AI Automated Data Security	AI-driven data security management tool that can map and correct problems such as sensitive data breach in real time.
Alias domains	Alternative email addresses to identify if it has been sold to third parties.
Anonymize IP	Scrambles IP addresses to protect user location data.
Attack resistance management	Inviting “ethical hackers” to find and report vulnerabilities.
Blocklist	List of malicious domains to block unwanted data collection.
Certifications	Certification and awards enforce rules over users’ data collection and expose protocols, especially when it involves external validation.
Chosen server	Hosting location options for user data.
Community driven	Collaborative development of the solution by users, professionals, and organizations.
Compliance scan	Automated scan tools for auditability and compliance.
Crypto transactions	Decentralized banking based on blockchain, independent of central authorities and with enhanced privacy.
Data Ownership	Users control their data, including deletion and storage choices.
Data Protection Officer (DPO)	GDPR-related function of an external consultant who guarantees data protection while having a communication channel with users.
Decentralized storage	Decentralized redundant storage, such as Torrent. It enhances data privacy and resilience.
Digital Literacy content	Informative material on digital literacy, data ethics, and cybersecurity.
Disclosed server location	Exact or approximate location of the personal data storage can reveal its commitment to comply with local data laws.
Downloadable Files	Data are downloadable and erasable, but not always transferable.
Downloadable Software	Software can be downloaded and modified, and users’ files stay on the device.
Employee ownership	Shared ownership between employees fostering decentralized control.
Encryption	Makes data unreadable for protection. It has different types, such as protecting data in transit, at rest or end-to-end.
Ethical actions	Support for research and policy development on data ethics.
Ethical behaviour reward	Users and other stakeholders’ rewards for ethical data practises.
Explainable AI (XAI)	Report of the algorithm path over its results for enhancing understanding and transparency.
External webchat channel	External communication channels for knowledge sharing, such as social media platforms.
Financial Trade	Offer of paid products and services to ensure economic sustainability independent of personal data.
Forum	Public discussion area in the solution about the solution.

Table A1. *Cont.*

Feature	Description
Handbook	Encyclopedic guide covering the solution structure, policies, and documentation for users, customers, and developers (in case of open source).
Law Compliance	Information about compliance with different laws and regulations (of different countries), enforcing basic rules over data collection.
Local Knowledge	Regional contributions of users, ensuring local expertise, accuracy and relevance.
Matrix API	Distributes data across volunteer nodes for enhanced communication privacy.
Open Changelog	Public record of the source code changes aiding accountability.
Open Data	Access to the source code and data for transparency and community use under credit attribution.
Open file format	Non-proprietary files ensuring data access outside the solution, freeing the user from dependency and preserving data for the long term.
Open-Source	Source-code availability enabling users and developers to view, modify, and collaborate. It has different types, from fully to partially open (closed core or extension).
Open-Source external parts	Use of open-source software in the solution, such as GNU and Linux.
Opt-in ads and rewards	Non-profiling ads with rewards for users' attention.
Opt-out tracking	Allows users to disable tracking, providing clear information when it is collection information.
Physical Kill Switches	Physical switches to disable transmissions and sensors.
Policies	Internal policies beyond legislation, such as privacy by design protocols, and involvement with NGOs following recommendations of specialists, such as Global Privacy Control.
Private server	Organization-owned servers ensure higher data security against third-party servers.
Regional server	Data allocated to the nearest region of the user and comply with local data laws.
Self-hosted server	Users store their data on their own devices.
Sponsors/donors	Independent funding by users can promote transparency.
Support C2C	Community-led project encouraging knowledge sharing, where more experienced users provide support to less experienced ones.
TOR	Anonymous communication through a global network of volunteer nodes.
VPN	Redirects IP address to a remote server, hiding users' online activity.

References

1. Floridi, L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* **2020**, *33*, 369–378. [CrossRef] [PubMed]
2. Morozov, E. 'Capitalism's New Clothes', The Baffler. Available online: https://thebaffler.com/latest/capitalisms-new-clothes-morozov (accessed on 22 April 2024).
3. Han, B. *Ecodesign—A Promising Approach to Sustainable Production and Consumption*; United Nations Environment Programme (UNEP): Paris, France, 1997. Available online: https://cir.nii.ac.jp/crid/1573105974909900160 (accessed on 27 September 2023).
4. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; First trade paperback edition; PublicAffairs: New York, NY, USA, 2020.
5. Ruppert, E.; Isin, E.; Bigo, D. Data politics. *Big Data Soc.* **2017**, *4*, 2053951717717749. [CrossRef]
6. O'Neil, C. *Weapons of Math Destruction*; Crown Publishing Group: New York, NY, USA, 2017. Available online: https://www.penguin.co.uk/books/304513/weapons-of-math-destruction-by-oneil-cathy/9780141985411 (accessed on 22 April 2024).
7. How to Win Elections in the 21st Century... and How to Save Democracy—European Parliament. 7 November 2018. Available online: https://www.youtube.com/watch?v=YUCxQv3xqso (accessed on 27 January 2024).
8. Delmastro, M.; Nicita, A. *Big Data: Come Stanno Cambiando il Nostro Mondo*; In Farsi Un'idea, No. 274; Il Mulino: Bologna, Italy, 2019.
9. Cadwalladr, C.; Graham-Harrison, E. Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach—Cambridge Analytica the Guardian. Available online: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (accessed on 2 April 2023).

10. Li, A.Q.; Found, P. Towards Sustainability: PSS, Digital Technology and Value Co-creation. *Procedia CIRP* **2017**, *64*, 79–84. [CrossRef]
11. Watanabe, K.; Kishita, Y.; Tsunetomo, K. Conceptual design framework for digital technology assisted service system. In Proceedings of the ServDes2020, Melbourne, Australia, 2–5 February 2021.
12. Zheng, P.; Wang, Z.; Chen, C.-H. Smart product-service systems: A novel transdisciplinary sociotechnical paradigm. In *Advances in Transdisciplinary Engineering*; Hiekata, W.N., Moser, B.K., Moser, B., Inoue, M., Stjepandic, J., Eds.; IOS Press BV: Amsterdam, The Netherlands, 2019; pp. 234–241. [CrossRef]
13. Li, A.Q.; Rich, N.; Found, P.; Kumar, M.; Brown, S. Exploring product–service systems in the digital era: A socio-technical systems perspective. *TQM J.* **2020**, *32*, 897–913. [CrossRef]
14. Valencia, A.; Mugge, R.; Schoormans, J.; Schifferstein, R. The Design of Smart Product-Service Systems (PSSs): An Exploration of Design Characteristics. *Int. J. Des.* **2015**, *9*, 13–28.
15. Zheng, P.; Lin, T.-J.; Chen, C.-H.; Xu, X. A systematic design approach for service innovation of smart product-service systems. *J. Clean. Prod.* **2018**, *201*, 657–667. [CrossRef]
16. Petrecca, A.C.C.; Vezzoli, C. The social influences of digital technologies in the Design of S.PSS and DE: A literature review. In *IASDR 2023: Life-Changing Design*; Design Research Society: Milan, Italy, 2023; pp. 1–16. [CrossRef]
17. Helbing, D.; Mahajan, S.; Fricker, R.H.; Musso, A.; Hausladen, C.I.; Carissimo, C.; Carpentras, D.; Stockinger, E.; Sanchez-Vaquerizo, J.A.; Yang, J.C.; et al. Democracy by Design: Perspectives for Digitally Assisted, Participatory Upgrades of Society. *J. Comput. Sci.* **2023**, *71*, 102061. [CrossRef]
18. Kranzberg, M. Technology and History: "Kranzberg's Laws". *Technol. Cult.* **1986**, *27*, 544–560. [CrossRef]
19. Friedman, B.; Hendry, D.F. *Value Sensitive Design: Shaping Technology with Moral Imagination*; The MIT Press: Cambridge, MA, USA; London, UK, 2019.
20. Winograd, T.; Flores, F. *Understanding Computers and Cognition: A New Foundation for Design*; 24th Printing; Addison-Wesley: Boston, MA, USA, 2008.
21. Vezzoli, C.A.; Macrì, L.; Takacs, B.; Yang, D. *System Design for Sustainability in Practice*, 1st ed.; Maggioli spa: Rimini, Italy, 2022. [CrossRef]
22. Clark, G.; Crul, M.R.M.; Diehl, J.C. *Design for Sustainability: A Practical Approach for Developing Economies*; United Nations Environment Programme (UNEP): Paris, France, 2006.
23. Tukker, A.; Tischner, U. (Eds.) *New Business for Old Europe: Product-Service Development, Competitiveness and Sustainability*; Greenleaf Publishing: Sheffield, UK, 2006.
24. Pitt, J.; Ober, J. Democracy by Design: Basic Democracy and the Self-Organisation of Collective Governance. In Proceedings of the 2018 IEEE 12th International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Trento, Italy, 3–7 September 2018; pp. 20–29. [CrossRef]
25. Thomas, N.L. Democracy by Design. *J. Public Delib.* **2014**, *10*, 17. Available online: https://www.publicdeliberation.net/jpd/vol10/iss1/art17 (accessed on 9 April 2024). [CrossRef]
26. van den Hoven, J. ICT and Value Sensitive Design. In *The Information Society: Innovation, Legitimacy, Ethics and Democracy In Honor of Professor Jacques Berleur s.j.*; Goujon, P., Lavelle, S., Duquenoy, P., Kimppa, K., Laurent, V., Eds.; Springer: Boston, MA, USA, 2007; pp. 67–72. [CrossRef]
27. Helbing, D.; Frey, B.S.; Gigerenzer, G.; Hafen, E.; Hagner, M.; Hofstetter, Y.; van den Hoven, J.; Zicari, R.V.; Zwitter, A. Will Democracy Survive Big Data and Artificial Intelligence? In *Essays on the Dark and Light Sides of the Digital Revolution*; Springer: Cham, Switzerland, 2019; pp. 73–98. [CrossRef]
28. Robbins, S.; Henschke, A. The Value of Transparency: Bulk Data and Authoritarianism. *Surveill. Soc.* **2017**, *15*, 582–589. [CrossRef]
29. Held, D. *Models of Democracy*, 3rd ed.; Stanford Univ. Press: Stanford, CA, USA, 2006.
30. Creswell, J.W. *Research Design*, 3rd ed.; SAGE: Los Angeles, CA, USA, 2009.
31. Liu, J.; Liu, Z.; Yang, Q.; Osmani, M.; Demian, P. A Conceptual Blockchain Enhanced Information Model of Product Service Systems Framework for Sustainable Furniture. *Buildings* **2022**, *13*, 85. [CrossRef]
32. Birch, A.H. *The Concepts and Theories of Modern Democracy*, 3rd ed.; Routledge: London, UK, 2007.
33. Keane, J. *The Life and Death of Democracy*; Pocket Books: London, UK; Sydney, Australia; New York, NY, USA; Toronto, ON, Canada, 2010.
34. Cambridge University. Cambridge Dictionary. Available online: https://dictionary.cambridge.org (accessed on 29 January 2024).
35. European Union. *Report of the High Level Group on European Democracy*; European Committee of the Regions: Brussels, Belgium, 2022. Available online: https://data.europa.eu/doi/10.2863/643553 (accessed on 15 September 2024).
36. Fischli, R. Data-owning democracy: Citizen empowerment through data ownership. *Eur. J. Political Theory* **2024**, *23*, 204–223. [CrossRef]
37. Mavriki, P.; Karyda, M. Big Data Analytics: From Threatening Privacy to Challenging Democracy. In *Communications in Computer and Information Science*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 1111, pp. 3–17. [CrossRef]
38. Aradau, C.; Cluskey, E.M. Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes. *Int. Political Sociol.* **2022**, *16*, olab024. [CrossRef]
39. García, C.S. Digital expansionism and big tech companies: Consequences in democracies of the European Union. *Humanit. Soc. Sci. Commun.* **2024**, *11*, 448. [CrossRef]

40. Schnell, S. Transparency in a "Post-Fact" World. *Perspect. Public Manag. Gov.* **2022**, *5*, 222–231. [CrossRef]
41. Nicastro, M.L.; Santos, A.D. Sustainability transparency: Scope for digital services: Transparência para sustentabilidade: Escopo em serviços digitais. *MIX Sustent* **2023**, *9*, 181–199. [CrossRef]
42. Aytac, U. Digital Domination: Social Media and Contestatory Democracy. *Political Stud.* **2024**, *72*, 6–25. [CrossRef]
43. Baack, S. Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data Soc.* **2015**, *2*. [CrossRef]
44. Peters, M.A.; Jandrić, P. Dewey's Democracy and Education in the age of digital reason: The global, ecological and digital turns. *Open Rev. Educ. Res.* **2017**, *4*, 205–218. [CrossRef]
45. United Nations. *Vienna Declaration and Programme of Action*; United Nations: Vienna, Austria, 1993. Available online: https://www.ohchr.org/en/about-democracy-and-human-rights (accessed on 15 September 2024).
46. Ruijer, E.; Dymanus, C.; van Kesteren, E.-J.; Boeschoten, L.; Meijer, A. Open data work for empowered deliberative democracy: Findings from a living lab study. *Gov. Inf. Q.* **2024**, *41*, 101902. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.