



UvA-DARE (Digital Academic Repository)

A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies

Del-Real, C.; De Busser, E.; van den Berg, B.

DOI

[10.1080/13600869.2025.2457227](https://doi.org/10.1080/13600869.2025.2457227)

Publication date

2025

Document Version

Final published version

Published in

International Review of Law Computers & Technology

License

CC BY

[Link to publication](#)

Citation for published version (APA):

Del-Real, C., De Busser, E., & van den Berg, B. (2025). A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. *International Review of Law Computers & Technology*, 39(3), 374–405. <https://doi.org/10.1080/13600869.2025.2457227>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)

A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies

Cristina Del-Real ^a, Els De Busser ^b and Bibi van den Berg ^a

^aInstitute of Security and Global Affairs, Leiden University, The Hague, The Netherlands; ^bInstitute of Information Law, University of Amsterdam, Amsterdam, The Netherlands

ABSTRACT

This paper offers a comparative systematic literature review of the key principles, norms, and strategies associated with Security by Design (SbD) and Privacy by Design (PbD). Both frameworks are grounded in the idea that security and privacy should be integral components of digital technologies from the very beginning of the design process. Following PRISMA guidelines, we reviewed 82 documents sourced from databases such as the ACM Digital Library, EBSCO Library, IEEE Xplore, ProQuest, Scopus, and Web of Science. Our analysis reveals that SbD and PbD share four fundamental principles: prevention/proactiveness, embeddedness, user-centricity, and transparency. The review also highlights the solid regulatory foundation of PbD, particularly under the General Data Protection Regulation (GDPR), compared to the emerging regulatory context for SbD. Additionally, we explore a range of strategies, from organizational cultural changes to technical interventions, that illustrate the nuanced approaches taken to implement these paradigms. We conclude by discussing the broader implications of these findings and suggesting directions for future research, aiming to contribute to the development of technologies that are both secure and respectful of privacy, while also advocating for integrated frameworks that enhance digital trust.

ARTICLE HISTORY



Received 10 April 2024
Accepted 20 January 2025


KEYWORDS

Software security; Systems development; Software design

1. Introduction

In 2009, Ann Cavoukian published her report entitled ‘Privacy by Design: The 7 Foundational Principles’ (Cavoukian 2009). Little could she anticipate the significant impact her principles would have on technology development in the ensuing decade. Cavoukian’s work has been extensively acknowledged by scholars as fundamental to the Privacy by Design (PbD) approach, inspiring subsequent works that translated her

CONTACT Cristina Del-Real  c.de.real@fgga.leidenuniv.nl  Institute of Security and Global Affairs, Leiden University, Turfmarkt 99, The Hague 2511 DC, The Netherlands

 Supplemental data for this article can be accessed online at <https://doi.org/10.1080/13600869.2025.2457227>.

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

principles into strategies (Hoepman 2014), organizational practices (see for a scoping review Iwaya et al. 2022), design approaches (e.g. Degeling et al. 2016), tools and technologies (e.g. Y. Liu and Simpson 2016). The primary objective of PbD is to ensure that privacy is taken into account from the outset of digital technology development and becomes the default mode of operation for organizations. Despite criticism by scholars and practitioners on the challenges of implementation (Spiekermann 2012), adoption (Rubinstein and Good 2012), scalability (van Dijk et al. 2018), and vagueness (van Rest et al. 2014) – among others – the PbD literature continues to position Ann Cavoukian’s principles as the foundation of the approach.

The relevance of Cavoukian’s foundational principles of PbD is evident in the numerous policies that have been developed and approved, integrating this approach. These policies include regulations such as the European General Data Protection Regulation (GDPR) (European Parliament and Council of Europe 2016) and the California Consumer Privacy Act (CCPA) (Legislature 2018), policy documents such as ‘Privacy, Trust and Innovation – Building Canada’s Digital Advantage’ by the Office of the Privacy Commissioner of Canada (2010), ‘Protecting Consumer Privacy in an Era of Rapid Change’ by the US Federal Trade Commission (2012), and ‘Privacy and Data Protection by Design – From Policy to Engineering’ by the European Union Agency for Network and Information Security (ENISA) (Domingo-Ferrer et al. 2014), which emphasize the importance of PbD. Finally, international standards such as Consumer Protection: Privacy by Design for Consumer Goods and Services (ISO/DIS 31700) (International Organization for Standardization 2023) also support the implementation of PbD principles.

In the years that followed, PbD was used as an example to formulate other design principles for the design and development of digital technologies. Security by design (SbD) is the most prominent of these. However, the principles that underpin the SbD approach, are not as extensively consolidated by any reference author as is the case with PbD. SbD is similar to PbD, in the sense that it focuses on integrating security considerations into the development process of technologies from an early stage. This concept has prompted the creation of numerous technical models and software design methodologies (e.g. Casola et al. 2020), which embed security considerations in software architecture. Its evolution can be traced along a trajectory of convergences and discontinuities from computer science, with significant advances being made by companies. For instance, Microsoft’s Security Development Lifecycle (SDL) is one of the most renowned, containing twelve practices aimed at improving the security of their products (Microsoft 2022).

Standards and policies that have embraced SbD can also be found, albeit to a lesser extent than those for PbD. For instance, there is the technical specification ‘Cyber Security for Consumer Internet of Things’ (ETSI TS 103 645) by the European Telecommunications Standards Institute (ETSI) (2019), the ISO/IEC 27000-series, and more recently, the ‘Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020’ (Cyber Resilience Act 2022).

The aim of this article is to synthesize the contributions of existing literature on the principles, norms, and strategies in SbD and PbD, and to provide a comparative analysis. Previous systematic literature reviews have not offered a comparative overview and analysis of the principles, norms, and strategies associated with SbD and PbD. Existing reviews on similar topics tend to focus either on the technical aspects of SbD or PbD

approaches (e.g. see Andrade et al. 2023 for a SLR of the application of PbD to software engineering), on specific sectors (e.g. Samantha et al. 2020 in the healthcare sector), or on particular technologies (e.g. Macedo et al. 2019 about IoT). Prior research related to this project has explored the conceptual definitions of both SbD and PbD, but without delving into their principles, norms, and strategies (Del-Real, De Busser, and van den Berg 2024). To the best of our knowledge, this systematic literature review contributes in an innovative way to the field by providing a comprehensive overview and analysis of the principles, norms, and strategies that define SbD and PbD. This research further clarifies the fundamental propositions underlying both concepts and their respective levels of development. The findings of this study contribute to a better understanding of the normative aspects of SbD and PbD, which will be valuable for future research on the integration of technical, normative and social factors in the design of secure software systems.

The review follows the PRISMA guidelines, including the selection of appropriate databases, search terms, and inclusion criteria. The article is structured in the following manner. The first section presents the debate regarding the definitions of software security and privacy, along with the significance of principles, norms, and strategies for these two approaches. The section 2 outlines the methodology adopted for this systematic review, including the literature search, eligibility criteria, study selection, and data extraction and presentation. In section 3, the results of the review are presented, while section 4 delves into a discussion of the findings, their implications for research and practice, and proposes future research avenues.

1.1. Software privacy and security

One of the challenges faced by the PbD and SbD approaches is the absence of a consensus definition regarding software privacy and security. This lack of agreement not only impacts the work within singular disciplines (e.g. computer science) but also adds complexity when we extend the scope of the review to other disciplines, such as law, governance, safety science, or criminology, among others. The notion of privacy has been the subject of extensive academic debate (e.g. Thomson 1975). The aim was always to keep the concept of privacy as flexible as possible to stand the test of time – and the advancement of technology – and to be interpreted by judges and administrative authorities in concrete circumstances. Legislators therefore have refrained from squeezing the right to privacy in a legal definition which would be too restrictive to make it work in practice. This lack of a clear definition has however also led to the right to privacy become mixed up with the right to data protection.

With the increasing penetration of technology in our daily lives, the risks of privacy violations have risen due to the ability to collect and store vast amounts of data (e.g. Finn, Wright, and Friedewald 2013). Regarding software design, privacy has mostly been defined as synonymous with the protection of personal data and information against unauthorized access, use, and disclosure (e.g. Hartzog 2018). The blending of privacy and data protection is confusing but also understandable for the following reasons.

First, we cannot deny the relevance of data for both rights. The way that data are collected and processed can breach the right to privacy and the right to data protection at the same time. Second, where the protection of personal data refers exclusively to data that identify or enable to identify an individual, privacy can encompass those parts of an

individual's life that are not necessarily specific enough to single out the individual from a population but are considered belonging to the personal sphere and in need of protection for that reason, for example religion. Vice versa, data that identify or enable to identify an individual can also not be considered part of the private sphere, such as name or email address. The right to privacy and the right to data protection can overlap but do not necessarily do so.

Third, since 2009, both are recognized as independent rights in accordance with the EU Charter of Fundamental Rights and Freedoms. This is however not the case in the rest of the world. For example, in the European Convention on Human Rights (ECHR) only the right to a private life is recognized as a fundamental right. This means that the European Court of Human Rights has adjudicated on cases where personal data were unlawfully processed, such as cases regarding national surveillance laws or practices, by referring to Article 8 of the Convention on the right to a private life. Even though the Council of Europe has a specific legal instrument on data protection – known as Convention 108 from 1981 and its modernized version Convention 108+ from 2018 – it will still rely on the right to privacy from the ECHR to rule on the matter due to the limited mandate of its Court.

To further operationalize privacy, it has been divided into distinct properties: confidentiality, unlinkability, intervenability, integrity, availability, and transparency of information (Rost and Bock 2011). The GDPR solidified the link between privacy (by design) and the protection of personal data in its Article 25 (e.g. Ayalon and Toch 2021). This article mandates data controllers to implement organizational and technical measures that uphold data protection principles, thereby safeguarding the rights of data subjects. Scholars have analysed this article in the literature as an application of privacy. Conversely, other authors define privacy by grounding it in specific rights, such as the respect for private and family life, personal data (Aljeraisy et al. 2022b; Porcedda 2018), and the right to be let alone (Warren and Brandeis 1890).

The concept of security has also been the subject of considerable scientific debate. For several decades, the definition of security in the realm of digital technologies was defined with a focus on the notions of confidentiality, integrity, and availability (commonly known as the 'CIA-model') (e.g. Bygrave 2022b). In recent times, the predominant focus on the technical aspect of security has faced criticism, as digital technologies are now perceived not merely as data vessels but also as new spaces for social interaction (Dodge and Kitchin 2001). Consequently, there appears to be a shift from merely securing information to ensuring people's and organizations' digital life security. Researchers now also focus on human behavior and the ways in which digital technologies are used, both for intended and for unintended purposes.

Privacy and security share an important characteristic. Both are known to not have a clear definition. Instead, both privacy and security are characterized by imprecision allowing for interpretations in accordance with time and location (Zedner 2003). One particular characteristic sets privacy and security apart though: where privacy is recognized universally as a fundamental right embedded in legal instruments, security is not.

1.2. Principles, norms, and strategies

This paper adopts a normative approach, concentrating on the principles, norms, and strategies associated with SbD and PbD. The study aims to synthesize the various

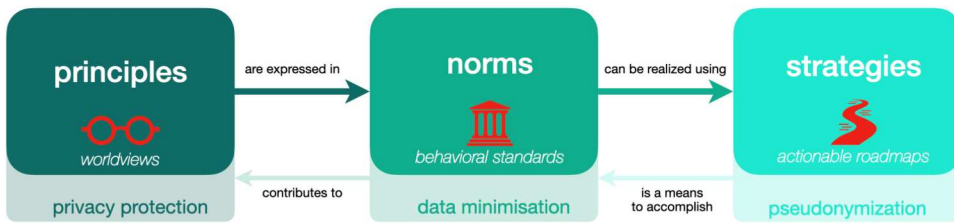


Figure 1. Principles, norms and strategies.

efforts in the literature that describe principles, analyze standards, and propose strategies necessary for achieving SbD or PbD. To accomplish this, it is essential to first define the concepts of *principles*, *norms*, and *strategies* (see Figure 1).

Principles encompass a broad perspective on a particular issue and outline philosophical approaches for addressing these challenges. In Bygrave's words (2022b, 139), '[principles] tend to depict norms with a higher level of generality, abstraction, open-endedness, persistence and explicit value-embodiment than rules, and they often help ground and justify the latter.'

Norms refer to standards of behavior, which may or may not be codified in specific laws or regulations. A norm embodies one or more underlying principles. For example, if data protection is a key principle in our worldview, we might establish a norm that dictates data minimization as a crucial behavioral standard for all entities engaged in data collection and processing. Data minimization entails limiting the collection of personal data to what is directly relevant and necessary to achieve a specific purpose. This principle is formally articulated in the GDPR, specifically in Article 25. In the context of this paper, norms refer to the concrete formalizations of principles within legal instruments. A significant implication of this is that norms become binding once they are enshrined in legal provisions. When enforcement measures such as fines or orders to cease data processing activities are added, these norms, for the purposes of this paper, are considered only at the level of binding legal obligations.

Strategies, finally, function as actionable roadmaps designed to achieve specific objectives. A strategy translates a norm, along with its underlying principle(s), into a set of actions that lead to a desired outcome. By implementing a strategy, the underlying principles can be actualized, and the norm can be adhered to. For instance, considering the principle of privacy and the norm of data minimization, one strategy to uphold this principle and implement the norm could be the use of 'pseudonymization.' This process manages personal information in such a way that it prevents the direct identification of the data subject without the need for additional details. Thus, pseudonymization as a strategy exemplifies the norm of data minimization, which in turn embodies the principle of privacy protection.

2. Methods

2.1. Protocol and registration

The protocol for this study was pre-registered in the Open Science Framework (OSF) Registries (<https://doi.org/10.17605/OSF.IO/WQ98H>). Initially, our aim was to conduct a

single systematic review on SbD definitions and principles. However, as we advanced in our research, we observed that SbD is closely linked to PbD. Therefore, we examined both concepts in conjunction to provide for a more nuanced understanding of SbD, expanding our original protocol. This article presents the findings of the second part of our systematic review.

We focused specifically on the comparison of SbD with PbD – and not other concepts such as ‘data protection by design (and by default)’ or ‘security of processing’ – for three reasons. First, PbD precedes data protection by design (and by default) in terminology and in the scholarly and policy discourse. We found literature that argues that the GDPR’s legal obligations articulated as ‘data protection by design’ and ‘data protection by default’ in Article 25 are rooted in PbD (Buttarelli 2018). Second, literature discussing security and privacy is more extensive (e.g. Cavoukian and Dixon 2013; Haber and Tamò-Larrieux 2020) than that on security and data protection.¹ The third reason for our approach is our desire to analyse SbD in relation to a concept that, while rooted in computer science, also extends into various scholarly disciplines and policy discussions. In contrast, data protection is more heavily anchored in the legal domain (Bygrave 1998) and does not resonate as strongly within disciplines such as computer science and science and technology studies. As we aim to connect computer science with broader social studies, we believe focusing on privacy provides a more comprehensive framework to examine against security than other concepts, including data protection.

2.2. Literature search

We followed the Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) guidelines, particularly the extension for scoping reviews (PRISMA-ScR) which is ideal for broad research questions (Tricco et al. 2018). As there is a vast range of principles, norms and strategies in the literature on SbD and PbD, an interdisciplinary review is necessary to map and integrate the existing definitions. Following the PRISMA guidelines, we conducted a search for thematically relevant studies published in English, using specialized databases. No temporal restrictions were imposed as the foundations of the SbD paradigm, which emerged in the early twenty-first century, are still relevant today. In this review, we considered peer-reviewed manuscripts, technical papers, and doctoral theses. Three methods were used to identify eligible documents, including searching electronic databases, Google Scholar, and reaching out to authors.

We searched selected databases that were relevant to our field of study. These databases included the ACM Digital Library, EBSCO Library, IEEE Xplore, ProQuest, Scopus, and Web of Science. We gained access to these databases through Leiden University and the Delft University of Technology. The search strategy for our systematic review comprised of three steps. First, we formulated search terms by identifying the three key concepts of our study: the objective (i.e. security or privacy), the method (i.e. design), and the subject (i.e. digital technology). We developed our query by finding synonyms of the keywords and utilizing wildcards to include word stem variations (e.g. secur*) as well as Boolean operators. We checked the terms in the selected databases to determine the most effective search string for the purpose of this paper. The search strategy was assisted by two librarians from Leiden University, specializing in Sciences and Political Science, Public Administration, and Security and Global Affairs

(see supplementary file 1 for a list of search queries utilized per database). The search was conducted on 8th July 2024.

Second, we used the Publish or Perish software to perform the Google Scholar search and download the results. We used the following query: (secur* OR privacy) AND ('by design*' OR 'through design*' OR 'development lifecycle' OR 'development life cycle') AND (software OR 'operating system' OR 'computer program' OR digital* OR electronic* OR technolog*). Third, we contacted the authors of eligible studies and asked if they had conducted or were aware of other relevant documents to our research objectives.

2.3. Eligibility criteria and study selection

In the first stage of study selection, we employed ASReview LAB, an open-source software that uses machine learning models to facilitate systematic reviews (ASReview LAB Developers 2022; van de Schoot et al. 2021). The software prioritizes potentially eligible studies based on previous screening decisions, streamlining the screening process. Next, we conducted full-text screening of the selected studies. To ensure consistency in our screening process, we developed screening tools for both abstract and full-text screening, following established best practices guidelines for screening (see supplementary file 2 for details) (Polanin et al. 2019).

Eligibility criteria for study selection included the following: (1) open access or available through institutional access or provided by contacted researchers; (2) written in English; (3) peer-reviewed publication, book, book chapter, conference/proceeding paper, government or company document, technical report, or doctoral thesis; (4) not a correction, erratum or retracted article; (5) abstract specifically mentioned security or privacy by design (thematic relevance); (6) primary topic of the research was security of digital technology (focus); and (7) answered at least one of the research questions. We did not impose any restrictions on study design as the disciplines that have contributed to SbD and PbD vary extensively.

To evaluate the level of agreement among researchers, a preliminary test was performed, and the screening tool proposed in the protocol was modified based on the results. To conduct this test, we randomly selected 50 abstracts and assessed them based on the screening tool, which involved evaluating both the inclusion and exclusion criteria. The documents were classified as 'include,' 'exclude,' or 'undecided.' The level of agreement during the first pilot was calculated using a statistical measure known as Fleiss' kappa (Fleiss 1971), which ranges from -1 (no agreement) to $+1$ (full agreement), with values near 0 indicating that the agreement is no better than chance. Unfortunately, an insufficient level of agreement was obtained ($\kappa = 0.06$) (Landis and Koch 1977). After a research team meeting, the screening tool was updated, and a new sample of 20 abstracts was selected. This time, a substantial level of agreement was obtained ($\kappa = 0.782$, 95% agreement), and the first author performed the full title and abstract screening (van de Schoot et al. 2021). The updated screening tool is presented in supplementary file 3.

2.4. Data extraction and synthesis of results

We used Atlas.Ti (version 8) and a data spreadsheet to extract information from the selected documents, which included descriptive data such as the author(s), title of the publication, year of publication, journal, type of publication, discipline, and topic.

The final literature selection was imported into Atlas.Ti (version 8) for systematic coding of definitions. The coding of the definitions was initially performed by one researcher, followed by a thematic analysis by the research team. We presented the findings of this study as a narrative synthesis, which is the most suitable approach when research is heterogeneous (Popay et al. 2006). The results are structured according to the three elements: principles, norms, and strategies.

3. Results

3.1. Study selection and characteristics

We employed search queries within databases and Google Scholar, and direct communication with authors. We identified a total of 3918 distinct titles and abstracts (see Figure 2). Through the abstract screening we identified 186 studies that exhibit potential relevance to our research. Subsequently, we examined the full text of these studies and assessed 149 for their eligibility. We excluded records based on six criteria: (1) principles, norms and strategies were not addressed, (2) the paper was exclusively technical, (3) SbD or PbD was not addressed, (4) the paper was not about digital technology, (5) the paper was in a language not spoken by the authors, (6) it was not the type of document we were looking for, or (7) the paper was a previous published output of the project. The screening process resulted in 71 documents. Through contact with authors, we identified 10 more eligible papers. The final sample of this systematic review is composed of 82 unique documents (see Figure 2). Table 1 presents the list of studies included in the systematic review and a summary of the studies topic.

Table 1. Summary topic description of studies included in the systematic literature review.

	Reference	Topic of study
1	(Alam, Basit, and Arif 2023)	Comparison of PbD principles on blockchain platforms.
2	(Aljeraisy et al. 2022a)	Cross-country systematic analysis of data protection laws.
3	(Aljeraisy et al. 2022b)	PbD regulations for IoT and recommendations for developers.
4	(Alshammari 2019)	Proposal of a principled approach for engineering PbD.
5	(Alshammari and Simpson 2017)	Identification of privacy requirements engineering methods that derive in criteria that aid in identifying data-processing activities that may lead to privacy violations and harms.
6	(Ardo, Bass, and Gaber 2022)	Proposal of a practice-based model combined with Agile.
7	(Arizon-Peretz, Hadar, and Luria 2022)	Proactive security behavior among software developers.
8	(Austin and Slane 2023)	Analysis of Canada's constitutional framework for lawful access, and proposal of shifts to better address privacy and rights concerns in the digital age by focusing on the entire data life cycle and the context of its use.
9	(Ayalon and Toch 2021)	Examination of the consequences of the way privacy questions are framed.
10	(Balboni and Macenaite 2013)	FIUs technology compliance with privacy by design.
11	(Barth, Ionita, and Hartel 2022)	Review of privacy attributes.
12	(Batalla 2022)	Analysis of limitations and problems of implementation of privacy-enhancing technologies.
13	(Blythe, Sombatruang, and Johnson 2019)	Analysis of IoT devices user manuals compliance with SbD.
14	(Bu et al. 2020)	Influencing factors in PbD adoption by IT engineers.
15	(Bu et al. 2021)	IS engineers' acceptance of PbD.
16	(Bygrave 2022a)	Debate over prioritizing 'cyber resilience' versus 'cybersecurity' as public policy goals, examining their conceptual differences, legal implications, and the potential for integrating resilience within existing cybersecurity frameworks.

(Continued)

Table 1. Continued.

	Reference	Topic of study
17	(Bygrave 2022b)	Analysis of the SbD discourse and its utility as a regulatory principle.
18	(Caire et al. 2016)	PbD issues for Ambient Assisted Living.
19	(Cali et al. 2023)	Proposal of a digital energy platform architecture based on the principles of SbD and PbD.
20	(Carboni et al. 2023)	Analysis of PbD in systems for assisted living, personalized care, and well-being, focusing on how stakeholder involvement impacts privacy protection.
21	(Casola et al. 2020)	Proposal of a SbD methodology based on Security Service Level Agreements (SLAs).
22	(Cavoukian 2009)	Proposal of seven foundational principles of PbD.
23	(Cavoukian 2012)	Description of best practices to implement PbD successfully.
24	(Cavoukian and Dixon 2013)	Discussion about SbD principles and proposal of an enterprise architecture approach.
25	(Chaudhuri and Cavoukian 2018)	Proposal of the Proactive and Preventative Privacy (3P) Framework.
26	(Craggs 2019)	Proposal of the just culture to handle user error.
27	(CSA Singapore 2017)	Proposal of a framework to guide organizations in building security into their SDLC.
28	(de la Cámara et al. 2015)	Summary and gaps of SbD frameworks for software design.
29	(de la Cámara et al. 2016)	SbD practices, activities and control objectives for IT projects in SMEs.
30	(Department for Digital, Culture Media & Sport of the United Kingdom 2018)	Review of SbD practices applied to IoT.
31	(Federal Trade Commission 2012)	Proposal of PbD framework for business dealing with data.
32	(Fernandez et al. 2022)	Description of abstract security patterns and its relationship with other security features.
33	(Fluchs et al. 2023)	Proposal a method for making traceable security-by-design decisions in CPSs by using function-based diagrams and security libraries.
34	(Fockel, Merschjohann, and Fazal-Baqaie 2018)	Threat analysis for SbD-based software lifecycle.
35	(Freitas, Araújo, and Magalhães 2023)	Proposal of a process to integrate privacy and personal data protection into software development.
36	(Glasauer 2023)	Human and organizational factors that facilitate the development of secure by design robotic systems.
37	(Gupta 2022)	Proposal of a framework for DevSecOps adoption in organizations.
38	(Hadar et al. 2018)	Developers' perceptions, interpretations and practices of PbD.
39	(Hamon et al. 2024)	AI cybersecurity practices and gaps in security conformity assessment for AI systems.
40	(Hartzog 2018)	Proposal of a theoretical underpinnings of privacy law responsive to the way people perceive and use digital technologies.
41	(Hartzog and Stutzman 2013)	Obscurity by design as model for design-based privacy solutions for social technologies.
42	(Hoepman 2021)	Discussion on how to build privacy into the design of systems
43	(Humayun et al. 2023)	Analysis of practitioners' opinions on secure software practices.
44	(Jagarlamudi et al. 2023)	Analysis of privacy measures in FL, focusing on their effectiveness in safeguarding sensitive data during AI and ML model training.
45	(Janca 2021)	Explanation of the principles and practices of designing software with security in mind, and the importance of incorporating security measures early in the development process to prevent vulnerabilities and reduce the cost of fixing issues later.
46	(Kang and Kim 2022)	Proposal of a methodology that specifies the level of Secure SDLC desired by enterprises.
47	(Kapitonova et al. 2022)	Proposal of a framework to preserve privacy and cybersecurity in BCI applications by integrating privacy-by-design strategies throughout the BCI development process.
48	(Khan et al. 2024)	Identification of secure software development practices and dimensions.
49	(Khurshid et al. 2022)	Analysis of the challenges and prospects of incorporating IoT devices into cybersecurity certification frameworks, particularly under the EU Cybersecurity Act, and proposal of a template for an EU-specific IoT certification scheme.

(Continued)

Table 1. Continued.

	Reference	Topic of study
50	(Klitou 2014)	Analysis of regulations design and development of privacy-involving technologies.
51	(Koops and Leenes 2014)	Examination of PbD provision in data protection law, specifically the GDPR. Argument against the feasibility of hardcoding legal requirements into system designs, advocating instead for fostering PbD mindset.
52	(Koops, Hoepman, and Leenes 2013)	Critical analysis of the PbD provision in the GDPR.
53	(Malina et al. 2019)	Proposal of a framework of privacy-preserving procedures for Intelligence Infrastructures and IoT applications.
54	(Moganedi and Dlamini 2021)	Application of resilience thinking into SbD.
55	(Mouraditis 2010)	Establishment of a secure by design philosophy of secure information systems development.
56	(Perera et al. 2016)	Proposal of a privacy-by-design framework offering guidelines to evaluate the privacy strengths and weaknesses of current IoT applications and their supporting middleware.
57	(Perera et al. 2020)	Utility of PbD framework for IoT applications design process.
58	(Ping et al. 2023)	Discussion of current trends in secure software development and suggestions for improvements.
59	(Piras et al. 2021)	Proposal of a Data Scope Management service to support organizations' compliance with GDPR through PbD analysis.
60	(Porcedda 2018)	Alignment between technical understanding of PbD and the EU law.
61	(Prybylo et al. 2024)	Empirical analysis of software development teams' members' perceptions of privacy.
62	(Rachovitsa 2016)	The case for understanding privacy as a fundamental technical property for the well-functioning of Internet.
63	(Radunovic, Gratz-Hoffmann, and Maciel 2021)	Good corporate practices increasing security of digital products.
64	(Restuccia, D'Oro, and Melodia 2018)	Roadmap of research challenges related to the application of ML and SDN to address IoT security threats.
65	(Romanou 2018)	Case for the implementation of PbD in biometrics, e-health and video-surveillance.
66	(Rost and Bock 2011)	Proposal of unifying PbD and protection goals.
67	(Saltarella et al. 2023)	Systematic literature review of the translation of PbD principles into security requirements and integration in the human-centered design process.
68	(Saunders 2021)	Solutions for smart home security challenges using SbD framework.
69	(Semantha et al. 2020)	Systematic literature review on PbD for healthcare software systems.
70	(Shaabany and Anderl 2018)	Proposal to design secure an Industry 4.0 capable machine.
71	(Shirtz et al. 2024)	Description of security requirements for the implementation of SbD practices in ICS.
72	(Slesinger et al. 2023)	Empirical analysis of digital security communities of practices and proposal of participatory SbD.
73	(Slesinger, Panteli, and Coles-Kemp 2024)	Analysis of stakeholders' perceptions on regulation of digital security design.
74	(Sokolovska and Kocarev 2018)	Integration of legal and technical concepts of privacy.
75	(Tjondronegoro et al. 2022)	Proposal of a theoretical framework for responsible AI implementation.
76	(Ulhaq and Burmeister 2020)	PbD framework for federated learning systems.
77	(Umeugo, Lowrey, and Pandya 2023)	Analysis of factors affecting adoption of secure software practices in small and medium-sized companies.
78	(Valdés-Rodríguez et al. 2023)	Literature review of methods and models for integrating security in the software development lifecycle.
79	(Waldman 2020)	Critical analysis of Article 25(1) of GDPR in relation to the concept of PbD.
80	(Wilkinson et al. 2017)	Proposal of user-tailored PbD combining privacy features into a single intelligent user interface.
81	(Wohlgemuth 2014)	Proposal of PbD framework for IT systems' users' views on information exchange and IT support with different security interests.
82	(Zhao 2023)	Design of a privacy-focused framework to protect financial consumer information throughout its entire life cycle.

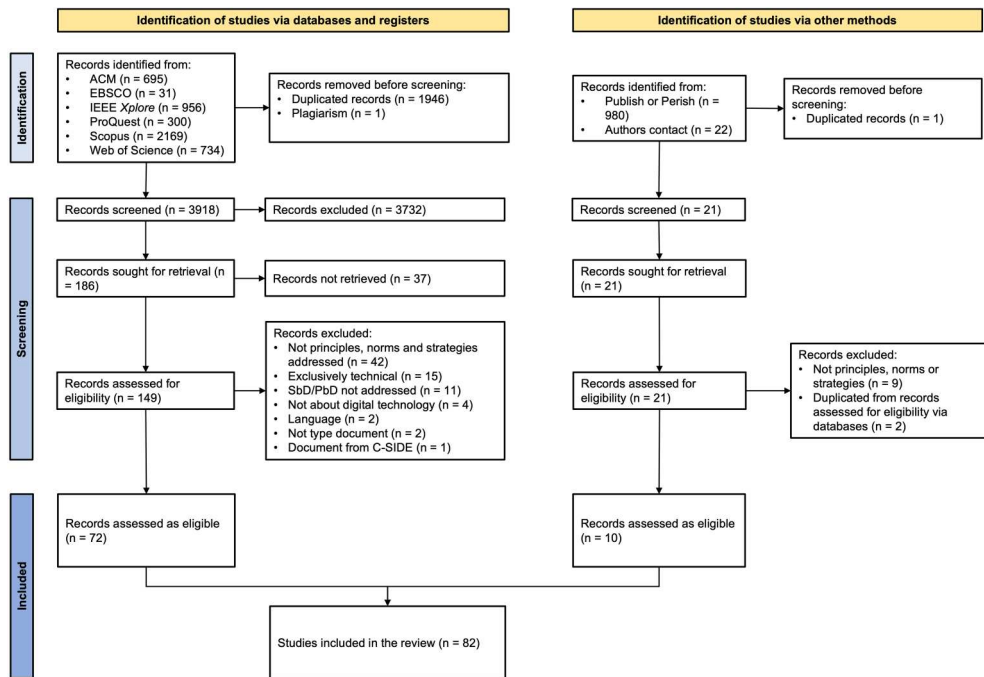


Figure 2. Adapted PRISMA Flow chart of search.

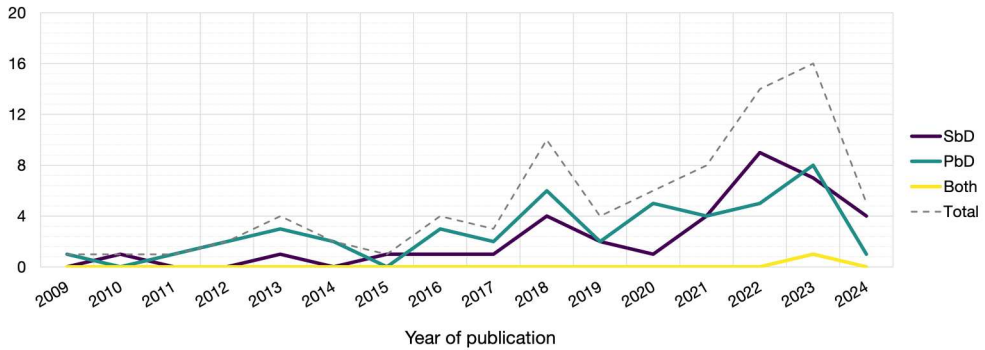
Figure 3 presents the descriptive characteristics of the final sample of 82 documents. We observe a growing trend in published articles on both SbD (n = 36) and PbD (n = 45), with a slight decline in 2024 due to the search being conducted only until July of that year. The majority of these documents focus on digital technologies, IoT devices, and software (systems). While some categories in **Figure 3** we chose to categorize the technologies based on the exact terminology used by the authors. Most documents originate from the fields of Computer Science, followed by Law and Science and Technology Studies. **Figure 3C** further highlights a trend in SbD and PbD studies: they either concentrate on specific technical applications and developments of these paradigms or explore their regulatory aspects.

3.2. Principles

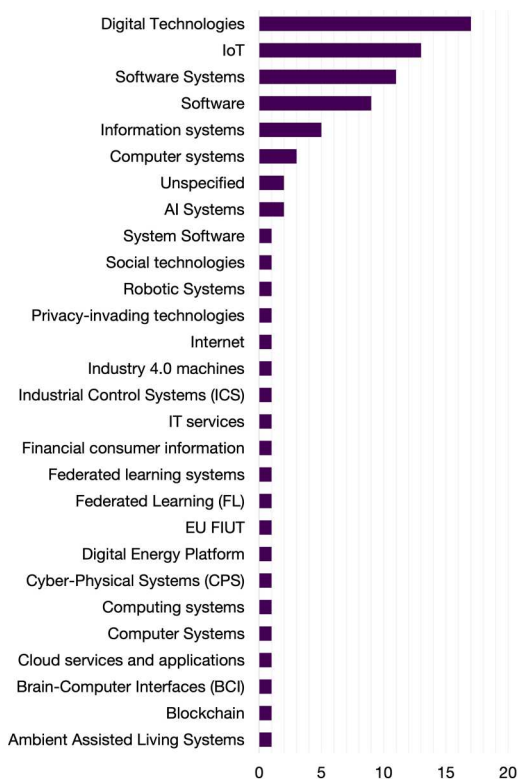
3.2.1. Security by design

To delineate a concept as a principle within our research scope, we employed a dual-method approach: on the one hand, we considered whether the concept was explicitly characterized as a ‘principle’ by the authors themselves. For example, Saunders (2021, 44) posits that ‘manufacturers and developers should leverage the principle of ‘least privilege’ as a benchmark in their security by design strategies’. On the other hand, we examined the literature for instances where authors articulate concepts in a prescriptive manner – i.e. they used imperatives such as ‘must’ or ‘should.’ An illustrative case is articulated by Fockel, Merschjohann, and Fazal-Baqaie (2018, 2), who assert that ‘In order to systematically develop secure products and services, security must be emphasized

A) Studies included in the systematic literature review (n = 82)



B) Technology



C) Discipline

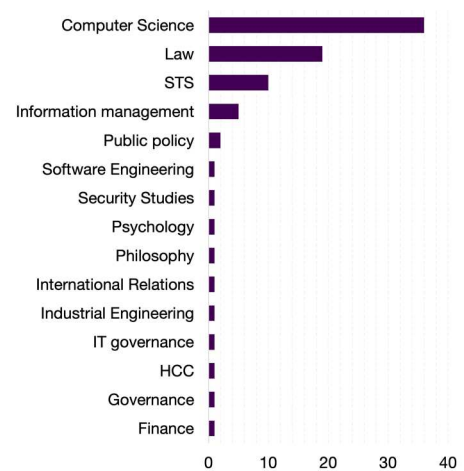


Figure 3. Studies included in the systematic literature review by (A) year of publication, (B) technology, and (C) discipline.

Note: Acronyms used mean the following. IoT = Internet of Things; EU FIUT = European Union financial intelligence units technology; STS = Science & Technology Studies; HCC = Human-Centered Computing.

throughout the whole software lifecycle, such that the results are secure by design.’ These two steps allowed us to identify 25 distinct principles related to SbD. The list with these principles, including the number of documents that mention them and the references, is systematically cataloged in [Table 2](#). The definition of all the principles can be found in supplementary file 4.

The two most common principles of SbD are *embedded nature* ($n = 13$) and *enabled in product lifecycle/design* ($n = 11$). These two principles are frequently intertwined, being the 'embeddedness' often pertaining to the product design process.² SbD seems to need the integration of security considerations and mechanisms within the technology development process (e.g. Radunovic, Gratz-Hoffmann, and Maciel 2021). A less common but significant perspective posits that security should be ingrained within the final product to ensure it is inherently secure (e.g. Fockel, Merschjohann, and Fazal-Baqaie 2018). Related to these two principles, the concept of *proactivity* advocates for security to be a foundational consideration, incorporated from the outset and during the technological design process, rather than as a retrospective addition. The proactivity principle is related to the culture and the strategic view of the organization (e.g. Chaudhuri and Cavoukian 2018; Valdés-Rodríguez et al. 2023).

To a lesser extent, we have discerned an association drawn by authors between the SbD approach and enhanced *resilience*. This principle entails the design of technologies that are not only more secure against threats (Ardo, Bass, and Gaber 2022; Fernandez et al. 2022; Hamon et al. 2024; Humayun et al. 2023; Janca 2021; Khan et al. 2024; Khurshid et al. 2022; Shirtz et al. 2024; Valdés-Rodríguez et al. 2023), but also capable of swiftly reverting to their normal operational state in the event of a cyber incident. Moreover, the processes through which the security of digital technologies is fashioned ought to be *transparent* and place the *user at the centre* of the design paradigm. This latter principle encompasses the need for security controls to be designed in an accessible manner, thereby augmenting user acceptance (Shaabany and Anderl 2018), as well as the incorporation of their security-related needs (Chaudhuri and Cavoukian 2018).

The remainder of the principles are referenced by merely one or two documents (see Table 2). It is observed that those principles which align with PbD principles are often connected with the work of Cavoukian in an effort to transpose PbD principles to SbD (e.g. principles such as *by default*, *transparency*, and *user-centric*, among others).

3.2.2.. *Privacy by design*

We identified 38 principles of PbD. At first glance, it is not only apparent that PbD encompasses a broader array of principles compared to SbD but also, upon examination of Table 2, there is discernible evidence of a more substantial consensus within the literature regarding these PbD principles. Indeed, 19 principles have been cited in at least five documents, and nine have been referenced in 10 or more documents. Amongst these principles receiving greater consensus in the literature, the *user-centric* principle is the most frequently reiterated ($n = 24$). This principle is often referred to the one by Cavoukian *respect for user privacy – keep it user-centric* (Cavoukian 2009). It includes considering users' privacy decision making and giving them the option to consent and choice in a way that it is appropriate for them.

The second most mentioned principle are *transparency*, identified in 22 documents. *Transparency* relates to the idea that users need to be informed in all circumstances about actions taken and technologies used. It is considered to be a key principle to achieve accountability (Alshammari and Simpson 2017; Austin and Slane 2023). *By default* ($n = 22$) and *embedded nature* ($n = 18$) share with SbD the position of being amongst the most prevalent principles cited in the documents. In this case, the *by*

Table 2. Principles of security and privacy by design.

Principle	Concept	
	Security by design	Privacy by design
Ability to intervene		Rost and Bock 2011
Access control		Aljeraisy et al. 2022a; Barth, Ionita, and Hartel 2022; Carboni et al. 2023; Jagarlamudi et al. 2023; Prybylo et al. 2024
Access protection		Hadar et al. 2018; Hartzog and Stutzman 2013; Shaabany and Anderl 2018
Accountability		Aljeraisy et al. 2022a; Alshammari and Simpson 2017; Barth, Ionita, and Hartel 2022; Batalla 2022; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Perera et al. 2020; Romanou 2018; Wohlgemuth 2014
Anonymity		Aljeraisy et al. 2022a; Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Caire et al. 2016; Carboni et al. 2023; Hadar et al. 2018; Hartzog and Stutzman 2013; Koops, Hoepman, and Leenes 2013; Perera et al. 2020; Porcedda 2018; Tjondronegoro et al. 2022
Back-to-front end		Ayalon and Toch 2021; Hartzog and Stutzman 2013
By default	Cavoukian and Dixon 2013; Freitas, Araújo, and Magalhães 2023	Alshammari 2019; Alshammari and Simpson 2017; Austin and Slane 2023; Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Bu et al. 2020; Bygrave 2022a; Caire et al. 2016; Carboni et al. 2023; Cavoukian 2009; 2012; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Koops, Hoepman, and Leenes 2013; Perera et al. 2016; Perera et al. 2020; Prybylo et al. 2024; Romanou 2018; Rost and Bock 2011; Saltarella et al. 2023; Samantha et al. 2020; Sokolovska and Kocarev 2018; Zhao 2023
Collection limitation		Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Hadar et al. 2018; Romanou 2018
Compliance with norms		Alshammari and Simpson 2017; Carboni et al. 2023; Koops, Hoepman, and Leenes 2013; Perera et al. 2016; 2020; Prybylo et al. 2024; Rachovitsa 2016; Saltarella et al. 2023
Conceptual integration	Mouraditis 2010	
Confidentiality		Hartzog and Stutzman 2013; Jagarlamudi et al. 2023; Kapitonova et al. 2022; Koops, Hoepman, and Leenes 2013; Perera et al. 2020; Porcedda 2018; Romanou 2018; Rost and Bock 2011; Saltarella et al. 2023; Zhao 2023
Control		Barth, Ionita, and Hartel 2022
Correctness		Aljeraisy et al. 2022a; Barth, Ionita, and Hartel 2022; Jagarlamudi et al. 2023
Data minimization		Aljeraisy et al. 2022a; Alshammari and Simpson 2017; Barth, Ionita, and Hartel 2022; Cavoukian 2012; Piras et al. 2021; Romanou 2018

(Continued)

Table 2. Continued.

Principle	Concept	
	Security by design	Privacy by design
Deletion/retention terms		Aljeraisy et al. 2022a; Barth, Ionita, and Hartel 2022; Saltarella et al. 2023
Disclosure		Aljeraisy et al. 2022a; Barth, Ionita, and Hartel 2022
Embedded nature	Ardo, Bass, and Gaber 2022; Bygrave 2022a; Cavoukian and Dixon 2013; Craggs 2019; Fernandez et al. 2022; Fockel, Merschjohann, and Fazal-Baqaie 2018; Gupta 2022; Khurshid et al. 2022; Mouraditis 2010; Ping et al. 2023; Radunovic, Gratz-Hoffmann, and Maciel 2021; Restuccia, D’Oro, and Melodia 2018; Saunders 2021	Alshammari 2019; Alshammari and Simpson 2017; Barth, Ionita, and Hartel 2022; Bu et al. 2020; 2021; Caire et al. 2016; Cavoukian 2009; 2012; Chaudhuri and Cavoukian 2018; Klitou 2014; Perera et al. 2016; Perera et al. 2020; Romanou 2018; Rost and Bock 2011; Semantha et al. 2020; Sokolovska and Kocarev 2018; Tjondronegoro et al. 2022; Zhao 2023
Enabled in product lifecycle/design end-to-end security	Cali et al. 2023; Cavoukian and Dixon 2013; de la Cámara et al. 2015; Fernandez et al. 2022; Fluchs et al. 2023; Fockel, Merschjohann, and Fazal-Baqaie 2018; Moganedi and Dlamini 2021; Mouraditis 2010; Radunovic, Gratz-Hoffmann, and Maciel 2021; Saunders 2021; Valdés-Rodríguez et al. 2023	Alshammari 2019; Alshammari and Simpson 2017; Barth, Ionita, and Hartel 2022; Bu et al. 2020; 2021; Caire et al. 2016; Carboni et al. 2023; Cavoukian 2009; 2012; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Klitou 2014; Perera et al. 2016; 2020; Romanou 2018; Rost and Bock 2011; Semantha et al. 2020; Sokolovska and Kocarev 2018; Tjondronegoro et al. 2022; Zhao 2023
Encouragement of pro-secure behavior	Craggs 2019	
External validation	Craggs 2019	
Facilitating dialogue	Department for Digital, Culture Media & Sport of the United Kingdom 2018	
Full functionality – win-win	Cali et al. 2023; Cavoukian and Dixon 2013; Hamon et al. 2024	Alshammari 2019; Alshammari and Simpson 2017; Austin and Slane 2023; Barth, Ionita, and Hartel 2022; Bu et al. 2020; 2021; Caire et al. 2016; Cavoukian 2009; 2012; Chaudhuri and Cavoukian 2018; Hartzog and Stutzman 2013; Perera et al. 2020; Romanou 2018; Rost and Bock 2011; Saltarella et al. 2023; Semantha et al. 2020; Sokolovska and Kocarev 2018; Zhao 2023
Holistic process in organizations	Glasauer 2023; Ping et al. 2023; Radunovic, Gratz-Hoffmann, and Maciel 2021; Zhao 2023	
Implemented in supply chain	Hamon et al. 2024; Khurshid et al. 2022; Radunovic, Gratz-Hoffmann, and Maciel 2021	
Integrated in the organization		Batalla 2022; Federal Trade Commission 2012; Hartzog and Stutzman 2013; Hoepman 2021; Kooops and Leenes 2014
Integrity of data		Carboni et al. 2023; Jagarlamudi et al. 2023; Porcedda 2018; Rost and Bock 2011
Interoperability	Saunders 2021	
Intervenability		Alshammari 2019; Porcedda 2018
Invisibility		Hartzog and Stutzman 2013
Lawful processing		Aljeraisy et al. 2022a; Romanou 2018
Least privilege	Saunders 2021	
Measurability	Department for Digital, Culture Media & Sport of the United Kingdom 2018; Gupta 2022	
Modularity		Tjondronegoro et al. 2022
Non-alignment	Craggs 2019	

(Continued)

Table 2. Continued.

Principle	Concept	
	Security by design	Privacy by design
Obscurity		Hartzog and Stutzman 2013
Plausible deniability		Porcedda 2018
Privacy-utility trade-off		Alam, Basit, and Arif 2023; Tjondronegoro et al. 2022
Proactive – Preventative	Arizon-Peretz, Hadar, and Luria 2022; Cali et al. 2023; Cavoukian and Dixon 2013; Craggs 2019; Restuccia, D'Oro, and Melodia 2018; Shaabany and Anderl 2018	Alam, Basit, and Arif 2023; Alshammari and Simpson 2017; Alshammari and Simpson 2017; Barth, Ionita, and Hartel 2022; Batalla 2022; Bu et al. 2020; 2021; Caire et al. 2016; Cavoukian 2009; 2012; Chaudhuri and Cavoukian 2018; Perera et al. 2020; Prybylo et al. 2024; Romanou 2018; Rost and Bock 2011; Saltarella et al. 2023; Samantha et al. 2020; Sokolovska and Kocarev 2018; Zhao 2023
Pseudonymity	Freitas, Araújo, and Magalhães 2023	Aljeraisy et al. 2022a; 2022b; Barth, Ionita, and Hartel 2022; Batalla 2022; Carboni et al. 2023; Hartzog and Stutzman 2013; Porcedda 2018
Purpose specification		Aljeraisy et al. 2022a; Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Carboni et al. 2023; Federal Trade Commission 2012; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Romanou 2018
Quantifiable		Tjondronegoro et al. 2022
Reducing burden	Department for Digital, Culture Media & Sport of the United Kingdom 2018	
Reliability	Restuccia, D'Oro, and Melodia 2018; Saunders 2021	
Resiliency	Bygrave 2022b; Department for Digital, Culture Media & Sport of the United Kingdom 2018; Moganedi and Dlamini 2021; Shirtz et al. 2024	
Revocable		Koops, Hoepman, and Leenes 2013; Romanou 2018
Scalability	Restuccia, D'Oro, and Melodia 2018; Saunders 2021	Tjondronegoro et al. 2022
Security culture	Craggs 2019; Gupta 2022; Mouraditis 2010; Ping et al. 2023	
Transparency	Cali et al. 2023; Cavoukian and Dixon 2013; Department for Digital, Culture Media & Sport of the United Kingdom 2018; Radunovic, Gratz-Hoffmann, and Maciel 2021	Alam, Basit, and Arif 2023; Aljeraisy et al. 2022a; 2022b; Alshammari 2019; Alshammari and Simpson 2017; Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Bu et al. 2020; 2021; Caire et al. 2016; Cavoukian 2009; 2012; Kapitonova et al. 2022; Koops, Hoepman, and Leenes 2013; Perera et al. 2016; Porcedda 2018; Romanou 2018; Rost and Bock 2011; Samantha et al. 2020; Sokolovska and Kocarev 2018; Wilkinson et al. 2017; Zhao 2023
Trustworthiness	Radunovic, Gratz-Hoffmann, and Maciel 2021	Perera et al. 2016; Romanou 2018; Tjondronegoro et al. 2022; Zhao 2023
Unlinkability		Balboni and Macenaite 2013; Hartzog and Stutzman 2013; Kapitonova et al. 2022; Koops and Leenes 2014; Porcedda 2018; Rost and Bock 2011; Saltarella et al. 2023

(Continued)

Table 2. Continued.

Principle	Concept	
	Security by design	Privacy by design
Unobservability		Carboni et al. 2023; Kapitonova et al. 2022; Koops, Hoepman, and Leenes 2013; Porcedda 2018; Wohlgemuth 2014
User awareness	Mouraditis 2010	
User-centric	Blythe, Sombatrung, and Johnson 2019; Cali et al. 2023; Cavoukian and Dixon 2013; Shaabany and Anderl 2018; Slesinger et al. 2023	Alshammari 2019; Alshammari and Simpson 2017; Ayalon and Toch 2021; Barth, Ionita, and Hartel 2022; Bu et al. 2021; Caire et al. 2016; Cavoukian 2009; 2012; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Hadar et al. 2018; Hartzog and Stutzman 2013; Koops, Hoepman, and Leenes 2013; Perera et al. 2016; 2020; Rachovitsa 2016; Romanou 2018; Rost and Bock 2011; Saltarella et al. 2023; Samantha et al. 2020; Sokolovska and Kocarev 2018; Wilkinson et al. 2017; Wohlgemuth 2014; Zhao 2023

default principle implies that technologies should be developed with privacy as a default setting of the system. The *embedded nature* states that privacy needs to become an essential component of the core functionality of the technology. Similarly to SbD, PbD also espouses the principle that privacy considerations should be integrated throughout the entire *product lifecycle* ($n = 20$).

The literature also identifies proactivity as a principle of PbD. 18 documents refer to Ann Cavoukian's principle of *full functionality – win-win*, which posits that one should not have to choose between functionality and privacy; rather, both should be in harmony, accommodating all legitimate interests. Additionally, also derived from the principles set forth by Ann Cavoukian, 18 documents acknowledge the *proactive not reactive; preventative not remedial* principle. This principle argues that invasions of privacy should be anticipated and prevented.

In our review, we identified principles not only associated with the foundational principles proposed by Ann Cavoukian but also numerous PbD principles that stem from the Fair Information Practices Principles outlined by the United States Federal Trade Commission. Among these are principles such as *accountability*, *collection limitation*, and *purpose specification* (supplementary file 4).

Further analysis of the principles reveals that compared to SbD, PbD studies demonstrate a more intensive focus on the principles. We calculated the ratio of principles per study by dividing the total number of principles mentioned in SbD or PbD documents by the total number of documents for each design. The results show that SbD documents mention an average of 2.1 principles per study, while PbD documents mention about 5.9 principles. The co-occurrence analysis of principles also provides valuable insights. We identified 21 pairs of principles that co-occur in 15 or more documents (see Figure 4). The most common pair is 'enabled in product lifecycle' and 'embedded nature,' with 24 co-occurrences, followed by 'enabled in product lifecycle' and 'by default,' 'user-centric' and 'by default,' and 'user-centric' and 'win-win,' with 18 co-occurrences. All these pairs seem to be related to the foundational principles established by Ann Cavoukian.

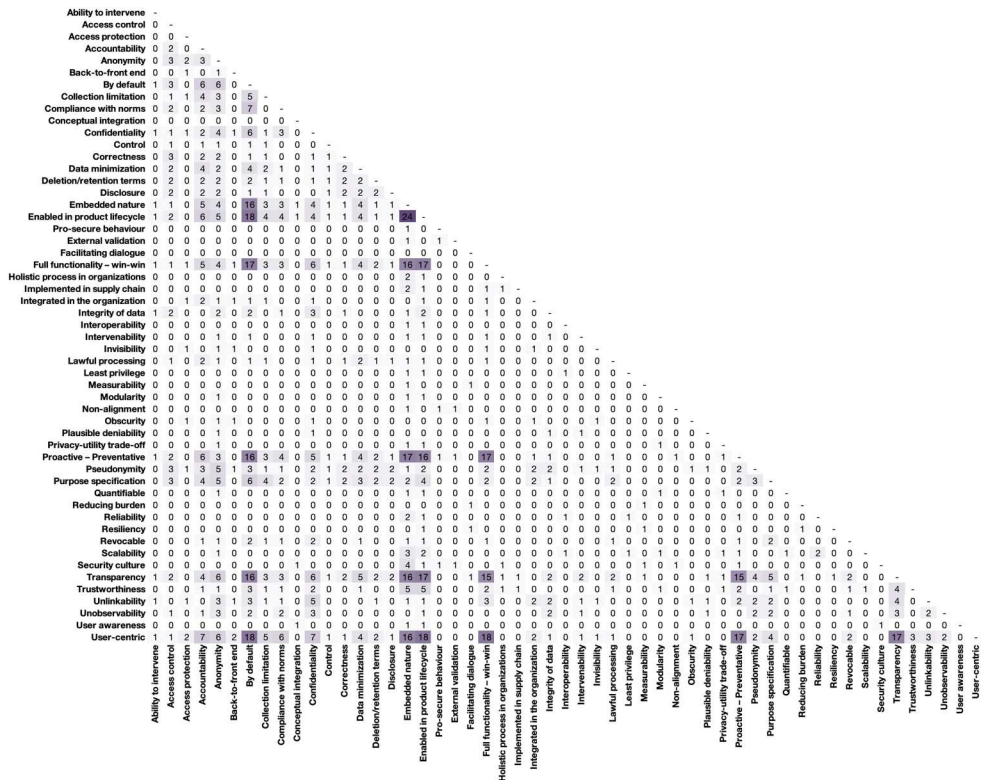


Figure 4. Co-occurrence matrix of Sbd and Pbd principles.

3.3. Norms

3.3.1. Security by design

We have identified as many as 15 norms, laws, and regulations pertinent to SbD in the documents reviewed. However, the sole normative cited by six documents is the GDPR (Bygrave 2022a; 2022b; Casola et al. 2020; Freitas, Araújo, and Magalhães 2023; Saunders 2021; Ulhaq and Burmeister 2020), followed by the NIS Directive with three documents (Bygrave 2022a; 2022b; Casola et al. 2020). The rest of the norms are mentioned by fewer authors: EU AI Act (Bygrave 2022b), California Civil Code (Bygrave 2022b), Charter of Fundamental Rights of the EU (Bygrave 2022a; 2022b), Data Act, Data Protection Directive (Bygrave 2022b), Digital Content Directive (Bygrave 2022b), Electronic Communications Code (Bygrave 2022a; 2022b), Electronic Identification, Authentication and Trust Services Regulation (Bygrave 2022b), EU Cybersecurity Act 2019 (Bygrave 2022a; 2022b; Khurshid et al. 2022), Financial Markets Directive (Bygrave 2022b), Medical Devices Regulation (Bygrave 2022a; 2022b), NIS2 Directive (Bygrave 2022a; 2022b), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Bygrave 2022a; 2022b). Merely five of the analysed documents refer to any form of regulation associated with SbD.

3.3.2. Privacy by design

PbD is unequivocally represented by the GDPR, as evidenced by 25 documents (Aljerisy et al. 2022a; Alshammari and Simpson 2017; Austin and Slane 2023; Ayalon and Toch

2021; Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Bu et al. 2020; Bygrave 2022b; Carboni et al. 2023; Hartzog 2018; Hoepman 2021; Jagarlamudi et al. 2023; Klitou 2014; Malina et al. 2019; Perera et al. 2020; Porcedda 2018; Prybylo et al. 2024; Rachovitsa 2016; Romanou 2018; Saltarella et al. 2023; Semantha et al. 2020; Sokolovska and Kocarev 2018; Tjondronegoro et al. 2022; Waldman 2020). Additional regulations identified include the Australian Privacy Principles (Aljeraisy et al. 2022b), the California Consumer Privacy Act (Aljeraisy et al. 2022b; Jagarlamudi et al. 2023; Prybylo et al. 2024), Enterprise Privacy Policies (Koops and Leenes 2014), New Zealand's Privacy Act (Aljeraisy et al. 2022b), and the Personal Information Protection and Electronic Documents Act (Aljeraisy et al. 2022b), PIPEDA (Austin and Slane 2023; Saltarella et al. 2023), Charter of Fundamental Rights of the EU (Austin and Slane 2023). In contrast with SbD, the legislative support for PbD is firmly established in Article 25 of the GDPR.

3.4. Strategies

3.4.1. Security by design

As with principles and regulations, we observed a lack of consensus on strategies. The strategies cited by a higher number of documents include the development of a security culture within the organization (Arizon-Peretz, Hadar, and Luria 2022; Bygrave 2022b; de la Cámara et al. 2015; 2016; Glasauer 2023; Janca 2021; Umeugo, Lowrey, and Pandya 2023), security training (Arizon-Peretz, Hadar, and Luria 2022; Kang and Kim 2022; Mouraditis 2010; Radunovic, Gratz-Hoffmann, and Maciel 2021; Shirtz et al. 2024; Valdés-Rodríguez et al. 2023), the implementation of multi-layered security (de la Cámara et al. 2015; 2016; Fernandez et al. 2022; Shaabany and Anderl 2018), validation (Humayun et al. 2023; Janca 2021; Fluchs et al. 2023; Shirtz et al. 2024), establishment of security requirements (Humayun et al. 2023; Janca 2021; Khan et al. 2024; Shirtz et al. 2024), designing the architecture (Cali et al. 2023; Cavoukian 2012; Fernandez et al. 2022; Shirtz et al. 2024), setting a vulnerability disclosure policy (Hamon et al. 2024; Khurshid et al. 2022; Ping et al. 2023; Valdés-Rodríguez et al. 2023), managing and testing security (Ardo, Bass, and Gaber 2022; Humayun et al. 2023; Shirtz et al. 2024; Valdés-Rodríguez et al. 2023), aligning security and functional requirements (Fluchs et al. 2023; Freitas, Araújo, and Magalhães 2023; Hamon et al. 2024), and software assurance processes (Casola et al. 2020; Saunders 2021; Shaabany and Anderl 2018). Additional strategies include secure data (Janca 2021; Khan et al. 2024; Shirtz et al. 2024), attack surface minimization (Department for Digital, Culture Media & Sport of the United Kingdom 2018; Fernandez et al. 2022), facilitate maintenance (Department for Digital, Culture Media & Sport of the United Kingdom 2018; Shirtz et al. 2024), ensuring software integrity (Department for Digital, Culture Media & Sport of the United Kingdom 2018; Freitas, Araújo, and Magalhães 2023), monitoring (Shirtz et al. 2024), minimize (Freitas, Araújo, and Magalhães 2023), managing organizational change (Humayun et al. 2023), managing security projects (Valdés-Rodríguez et al. 2023), and ensuring the security of the supply chain (Shirtz et al. 2024). The report from the Department for Digital, Culture Media and Sport of the United Kingdom (2018) on designing secure products also incorporates strategies such as avoiding default passwords, outages resiliency, protecting personal data, securing communications and data. The definition of all the strategies can be found in supplementary file 5.

3.4.2. Privacy by design

In contrast with SbD, there is a greater consensus among the PbD strategies identified. Ten of the strategies are referenced by at least six documents. These strategies are to minimize (Aljeraisay et al. 2022b; Alshammari and Simpson 2017; Ayalon and Toch 2021; Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Caire et al. 2016; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Hoepman 2021; Kapitonova et al. 2022; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Malina et al. 2019; Perera et al. 2016; 2020; Piras et al. 2021; Porcedda 2018; Prybylo et al. 2024; Romanou 2018; Saltarella et al. 2023; Samantha et al. 2020; Zhao 2023), control (Balboni and Macenaite 2013; Barth, Ionita, and Hartel 2022; Chaudhuri and Cavoukian 2018; Federal Trade Commission 2012; Hadar et al. 2018; Hartzog and Stutzman 2013; Hoepman 2021; Kapitonova et al. 2022; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Malina et al. 2019; Perera et al. 2016; 2020; Porcedda 2018; Prybylo et al. 2024; Romanou 2018; Saltarella et al. 2023; Samantha et al. 2020; Wilkinson et al. 2017; Zhao 2023), inform (Barth, Ionita, and Hartel 2022; Batalla 2022; Hoepman 2021; Kapitonova et al. 2022; Koops and Leenes 2014; Malina et al. 2019; Perera et al. 2016; 2020; Porcedda 2018; Prybylo et al. 2024; Saltarella et al. 2023; Samantha et al. 2020; Wilkinson et al. 2017), enforce (Alshammari and Simpson 2017; Barth, Ionita, and Hartel 2022; Batalla 2022; Hoepman 2021; Kapitonova et al. 2022; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Perera et al. 2016; 2020; Saltarella et al. 2023; Samantha et al. 2020), hide (Barth, Ionita, and Hartel 2022; Chaudhuri and Cavoukian 2018; Hoepman 2021; Koops, Hoepman, and Leenes 2013; Malina et al. 2019; Perera et al. 2016; 2020; Porcedda 2018; Prybylo et al. 2024; Samantha et al. 2020), separate (Aljeraisay et al. 2022b; Barth, Ionita, and Hartel 2022; Hoepman 2021; Jagarlamudi et al. 2023; Kapitonova et al. 2022; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Malina et al. 2019; Perera et al. 2016; Porcedda 2018; Saltarella et al. 2023; Samantha et al. 2020), aggregate (Barth, Ionita, and Hartel 2022; Hoepman 2021; Jagarlamudi et al. 2023; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Malina et al. 2019; Perera et al. 2020; Saltarella et al. 2023; Samantha et al. 2020), anonymize (Alshammari and Simpson 2017; Balboni and Macenaite 2013; Carboni et al. 2023; Chaudhuri and Cavoukian 2018; Hadar et al. 2018; Kapitonova et al. 2022; Koops and Leenes 2014; Malina et al. 2019; Romanou 2018; Saltarella et al. 2023; Zhao 2023), demonstrate (Barth, Ionita, and Hartel 2022; Hoepman 2021; Kapitonova et al. 2022; Koops and Leenes 2014; Koops, Hoepman, and Leenes 2013; Perera et al. 2016; 2020; Saltarella et al. 2023; Samantha et al. 2020), secure (Balboni and Macenaite 2013; Carboni et al. 2023; Federal Trade Commission 2012; Hadar et al. 2018; Koops and Leenes 2014; Malina et al. 2019; Perera et al. 2020; Prybylo et al. 2024), abstract (Hoepman 2021; Kapitonova et al. 2022; Saltarella et al. 2023), and limit access (Aljeraisay et al. 2022a; Zhao 2023). They coincide with the eight privacy design strategies proposed by Hoepman (2014).

Among the strategies also identified in the documents, yet with less consensus among the studies, are the following: ensuring accurate data (Aljeraisay et al. 2022a; Federal Trade Commission 2012; Jagarlamudi et al. 2023), intervening in user behavior (Hartzog and Stutzman 2013), intervening in corporate behavior (Hadar et al. 2018; Waldman 2020), certifying (Batalla 2022; Perera et al. 2016; Romanou 2018), complying (Hoepman 2021), measuring (Batalla 2022), limiting access (Hoepman 2021), overseeing (Austin and

Slane 2023; Federal Trade Commission 2012), implementing policy (Hadar et al. 2018; Hartzog and Stutzman 2013), promoting a privacy culture (Federal Trade Commission 2012; Hadar et al. 2018; Kapitonova et al. 2022), standardizing (Perera et al. 2016), designing the architecture (Jagarlamudi et al. 2023), training of employees (Carboni et al. 2023; Saltarella et al. 2023), and promoting user awareness (Federal Trade Commission 2012; Malina et al. 2019), encrypt, penetration testing, vulnerability scans, and change management (Carboni et al. 2023) (supplementary file 5).

4. Discussion

4.1. Discussion of findings

This systematic literature review aimed to synthesize the principles, norms, and strategies reported by the literature on SbD and PbD. The findings lead to the following conclusions. First and foremost, it is evident that the debate on PbD is older than that on SbD and, perhaps as a result, is more fully developed. There is generally greater consensus among scholars regarding the principles, norms, and strategies associated with PbD than there is with SbD. A more detailed comparison reveals additional insights, particularly when the discussion is divided into an analysis of the findings on principles, norms, and strategies, respectively.

The literature review on the *principles* that underpin SbD and PbD reveals that there are far more principles in the field of PbD than in that of SbD. However, when analysing the list of principles over which consensus emerges in the literature on both, it turns out that this list is similar in length. First, both for SbD and PbD, *prevention* or *proactiveness* are a central principle. By proactively making software secure or privacy-proof, negative outcomes for end users are prevented. SbD and PbD therefore are visions that focus on actively protecting the latter through particular measures and interventions. Proactive prevention is a guiding principle for the way in which the software ought to be designed. Second, *embeddedness* is a leading principle in both SbD and PbD. This is unsurprising, as the fundamental premise – that privacy and security should be integrated from the inception of the design or development process – necessitates that these values become an intrinsic part of the system, product, or service being created. The concept of embeddedness serves as a guiding principle, directing the specific approach and execution of the design process.

Finally, the last two principles that SbD and PbD share are those of *user-centricity* and *transparency*. User-centricity is central to both in the sense that both visions aim to implement interventions and mechanisms to increase protection for end users, with a primary focus on security in SbD, and on privacy in PbD. It is not surprising, therefore, that user-centricity appears as a guiding principle in the literature on both, with some authors going beyond the *centricity* aspect to propose forms of co-production of design with users – or participatory design (Slesinger et al. 2023).

The principle of transparency is more complicated. In debates on privacy and data protection there has been a long-standing call for (more) transparency towards end users with regard to the collection and processing of data. The principle of transparency expresses that call in the PbD literature. In SbD, however, the call for transparency likely aims not at end users, but at technology designers and providers. In contrast to

data collection and processing, whereby end users share something of themselves, end users do not want or need to be informed about (the exact constellation of) security measures in software, systems or networks – security must be provided ‘behind the screens’, without ‘getting in the way’ of what users want to do with them. Transparency about it is unnecessary and might even be considered an obstacle for use. However, modern-day software, systems and networks almost always consist of myriad subsystems that are not necessarily always custom-built from scratch. Code writers use existing libraries or scripts as part of their own designs. The principle of transparency is relevant for SbD in the sense that by being transparent about the quality and security of the code that is available in off-the-shelf libraries, scripts etc., code writers can warrant the security of their own products better.

There are also significant differences in the key principles of SbD and PbD. The most striking difference revolves around the principle of *resilience*. For SbD this is a key element. Systems must be able to withstand shocks, and should incidents arise, then it is helpful that they do not break completely, but fail only partially or gracefully or both. For PbD this principle is less apparent, because PbD does not focus on the continuous use of systems, but only on the ways in which personal data are gathered, stored, processed, shared and discarded. One key principle that is central to PbD but lacking in SbD is the notion of *full functionality*. One of the requirements of PbD is that end users can use software of systems to their full extent also when they choose not to share, or to only minimally share, their data. For SbD this interpretation of full functionality is less relevant. However, the principle of full functionality could be valuable to SbD in the sense that, sometimes, interventions to increase the security of systems are offset against their usability: because of security considerations, end users can no longer execute certain tasks. The principle of full functionality could restore some of the imbalance between designers’ desire to secure systems to the best of their abilities and end users’ desire to use software, systems and networks for a variety of (legitimate) purposes.

When analysing the translation of SbD and PbD into *norms*, laid down in laws and regulations, it is noteworthy that the translation and application of PbD is further along than that of SbD. PbD has a solid foundation and even its own article in the EU General Data Protection Regulation. While SbD lacks a similarly explicit presence, several authors reference the GDPR in relation to SbD. It is also noteworthy that SbD is connected to larger-scale and more impactful regulations than PbD, aside from the GDPR. SbD is discussed in connection to two of the most relevant regulatory frameworks for cybersecurity, the EU NIS-II directive and the EU Cyber Security Act. By contrast, PbD is connected to national legislation in countries such as New Zealand or in specific jurisdictions like the state of California.

Finally, analysing the literature on *strategies* for SbD and PbD is the most challenging. A significant number of strategies was found in the literature of each, only minor overlap. In each domain some strategies refer to larger sets of measures and interventions (‘data minimization,’ or ‘compliance,’ or ‘security testing’), whereas others are detailed and narrow (‘no default passwords’ or ‘access limitation’). Between articles in the literature on both PbD and SbD authors sometimes use different concepts for similar ideas. Going over the strategies in each body of literature, we clustered the strategies into more coherent sets. An analysis revealed that some strategies target *data, software and systems* (for instance ‘security testing’ or ‘data aggregation’), while others revolve

around *practices or processes or contexts* (for instance ‘promoting privacy/security culture’ or ‘ensuring compliance’), and yet others targeted *human behaviour* or human beings as *recipients* of protection (for instance ‘security training’ or ‘control over data’). Some strategies cover two categories: ‘multi-layered security’ has technical aspects but is also about the larger context in which systems or software is used. The same goes for ‘certification’. Strategies such as these have been placed in a joint category labeled *data and software in context*. We assigned the clusters of strategies for PbD and SbD to each of these four categories, thus ending up with the matrix presented in Table 3.

Upon examining this table, several observations become apparent. First, both literatures emphasize a range of similar strategies aimed at achieving security and privacy by design. Each framework imposes specific demands on organizations, categorized as ‘organizational change’ or ‘corporate behavior,’ and necessitates the cultivation of a conducive culture, referred to as ‘security culture’ or ‘privacy culture.’ Second, both frameworks outline steps to ensure that end users are adequately equipped to protect themselves, as evidenced by strategies such as security training, awareness, and behavioral change initiatives. Interestingly, one of the strategies in SbD is ‘protecting personal data,’ while one of the strategies in PbD is ‘securing data and systems.’

Significant differences also exist between the two approaches. These distinctions are, to some extent, expected, due to a different focus for SbD and PbD – the former prioritizing the security of software and systems, while the latter focuses on safeguarding the privacy of end users. The goals of both visions overlap partially – ultimately both aim to protect end users. But while PbD focuses mostly on the collection and exchange of data (of end users), SbD focuses on protecting systems, networks and data from attacks and failures. One could argue that in SbD protecting human beings is a *secondary* effect, which is realized through the protection of systems, data and networks, whereas PbD directly aims to protect individuals from privacy violations by ensuring more

Table 3. Summary of the results of the systematic literature review.

Theme	Concept	
	Security by design	Privacy by design
Data, software & systems	Software assurance Security testing, maintenance and validation Updating and minimizing attack surfaces Protecting integrity Protecting personal data No default passwords	Data minimization Hiding data/information Separating data/information Aggregating data/information Anonymizing data/information Securing data & systems Data accuracy Access limitation
Data and software in context	Multi-layered security Supply chain security Outage resiliency	Standardization Certification
Practices, processes & contexts	Organizational change and security culture Managing security project Having a vulnerability disclosure policy	Corporate behavior & privacy culture Enforcement & compliance Ability to demonstrate Policies & oversight
Human behavior & human beings as recipients of protection	Security training	Promoting user awareness & behavior Control for end users

robust guardianship of the data they share, store, and process. With this distinction in mind, it is understandable that the strategies under the 'data, software & systems' category within PbD focus predominantly on securing *software* and *systems* – with the notable exception of the broadly defined strategy of 'protecting personal data' – while all strategies under SbD aim to enhance privacy through a distinct approach to *data* management.

Two additional differences are particularly noteworthy. First, in SbD there appears to be a keen awareness that incidents may occur, even when security is implemented into software systems from the start. This awareness is reflected in strategies such as 'supply chain security' and 'outage resilience.' The first refers to the fact that digital systems are highly interconnected in our modern world, and the security of an interconnected system, therefore, is always as strong as its weakest link. The second refers to the fact that once systems are hit by incidents, it is efficient to have mechanisms in place to restore them as quickly as possible, and/or to minimize the impact of the incident. Interestingly, the literature on PbD lacks similar recovery or context-dependent strategies. It is unclear whether or not these strategies are, in fact, part of the implantation of PbD in particular design contexts, but the literature is silent on them. One might consider whether PbD could be further strengthened by incorporating strategies that address instances where privacy violations occur, even when systems are designed with privacy in mind.

Second, a similar omission can be observed within SbD. There, there is no mention of strategies such as certification and standardization as part of a gradual process of increasing security on a technical and a regulatory or organizational level. The literature on PbD does mention both explicitly. Standardization and certification are, in fact, high on the agenda of regulators and policy makers concerning cybersecurity. Therefore, it would be beneficial for these strategies to be incorporated into SbD as well.

4.2. Limitations of this review

This systematic literature review has limitations. First, it focuses exclusively on SbD and PbD while excluding related concepts like 'data protection by design.' This focus was chosen based on time constraints, relevance, and literature availability. Future studies could expand this comparison to include other concepts. The review's scope was also limited to certain databases, potentially overlooking non-scholarly works and articles that offer technical insights into SbD and PbD. Additionally, the review only included articles that explicitly mentioned SbD or PbD in their abstracts, possibly missing relevant studies. The screening and data extraction were conducted by a single researcher due to time constraints, despite efforts to ensure accuracy, leading to potential minor errors.

4.3. Research gaps and future research

An important area for future research originating from the analysis above is inspired by the significant differences between SbD and PbD under section 4.1. The conclusion that in SbD the protection of human beings is not a primary purpose but rather a secondary effect deserves more attention. From a previous systematic literature review it was already distinguished that SbD is often framed as an engineering approach (Del-Real, De Busser, and van den Berg 2024). Stakeholders with a software development

background indicated SbD transcending that concept and instead argued for viewing SbD as a *'holistic ecosystem encompassing diverse stakeholders, organizational practices, supportive leadership and policies, thereby necessitating the adoption of a security culture throughout the entire system producing digital technologies'* (Del-Real and De Busser 2023). This wider view on SbD clearly shows more attention to the organization and the human beings in it.

More research is needed to analyse (1) whether this expanded view on SbD resonates with a larger population of stakeholders working with SbD on a daily basis and (2) what that would look like in practice. If we take the aforementioned Microsoft's Security Development Life-cycle (SDL) as an example of a widely used secure software methodology, then we see that organizational aspects are included to some extent. Yet, the thinking about SbD as protecting human beings is academically underdeveloped. This is strongly related to the scope of the notion security which was earlier indicated as being imprecise. Whether and how to expand the understanding of the term security beyond the traditional CIA-focused meaning, possibly including personal safety and user protection, is still a debated question. It brings up the question, how much we can expect from developers?

Notes

1. When done, the concept of security is limited to 'information security'.
2. However, we decided to treat them as two separated principles because some authors place the 'embeddedness' of security in the product, and not in the process.

Acknowledgments

The authors want to thank Dr. Olga Gadyatskaya, Parto Mirzaei, Jasmijn Boeken, Jafar Akhondali, Arina Kudriavtseva (Leiden University), and Dr. Asier Moneva (Netherlands Institute for the Study of Crime and Law Enforcement, NSCR) for their valuable comments during the preparation of this paper. We also want to thank Rutger de Jong (subject librarian Science) and Majo Oldenhof (subject librarian Political Science, Public Administration and Security Affairs) for their help defining the key words for the systematic search.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was funded by NWO (the Dutch Research Council) (grant number NWA.1215.18.008) and is part of the Dutch Research Agenda 2018: Cyber security – towards a secure and reliable digital domain.

ORCID

Cristina Del-Real  <http://orcid.org/0000-0003-3069-4974>

Els De Busser  <http://orcid.org/0000-0002-7843-8833>

Bibi van den Berg  <http://orcid.org/0000-0002-4810-0460>

References

Papers marked with an asterisk (*) were included in the systematic review

- Alam, M. H., A. Basit, and F. Arif. 2023. "A Comparative Analysis of Implementation of Privacy by Design Principles on Different Blockchain Platforms." In *2023 International Conference on Communication Technologies (ComTech)*, 111–116. <https://doi.org/10.1109/ComTech57708.2023.10165248>. *
- Aljerais, Atheer, Masoud Barati, Omer Rana, and Charith Perera. 2022a. "Exploring the Relationships between Privacy by Design Schemes and Privacy Laws: A Comparative Analysis". arXiv.Org. <https://login.ezproxy.leidenuniv.nl/login?url=https://www.proquest.com/working-papers/exploring-relationships-between-privacy-design/docview/2723273547/se-2?accountid=12045>. *
- Aljerais, Atheer, Masoud Barati, Omer Rana, and Charith Perera. 2022b. "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective." *ACM Computing Surveys* 54 (5): 1–38. <https://doi.org/10.1145/3450965>.
- Alshammari, Majed, and Andrew Simpson. 2017. "Towards a Principled Approach for Engineering Privacy by Design." In *Privacy Technologies and Policy*, Edited by Erich Schweighofer, Herbert Leitold, Andreas Mitrakas, and Kai Rannenberg, 10518:161–77. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-67280-9_9. *
- Alshammari, Majed. 2019. "A Principled Approach for Engineering Privacy by Design". PhD diss., Oxford: University of Oxford. *
- Andrade, Vinícius Camargo, Rhodrigo Deda Gomes, Sheila Reinehr, Cinthia Obladen De Almendra Freitas, and Andreia Malucelli. 2023. "Privacy by Design and Software Engineering: A Systematic Literature Review." In *Proceedings of the XXI Brazilian Symposium on Software Quality. SBQS '22*. New York, NY: Association for Computing Machinery. <https://doi.org/10.1145/3571473.3571480>.
- Ardo, A. A., J. M. Bass, and T. Gaber. 2022. "Towards Secure Agile Software Development Process: A Practice-Based Model." In *2022 48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, edited by Gustavo M. Callico, Regina Hebig, and Andreas Wortmann, 149–156. Maspalomas, Gran Canaria, Spain: Conference Publishing Services. <https://doi.org/10.1109/SEAA56994.2022.00031>.
- Arizon-Peretz, Renana, Irit Hadar, and Gil Luria. 2022. "The Importance of Security Is in the Eye of the Beholder: Cultural, Organizational, and Personal Factors Affecting the Implementation of Security by Design." *IEEE Transactions on Software Engineering* 48 (11): 4433–4446. <https://doi.org/10.1109/TSE.2021.3119721>.
- ASReview LAB Developers. 2022. "ASReview LAB - A Tool for AI-Assisted Systematic Reviews". Zenodo. <https://doi.org/10.5281/ZENODO.7319063>.
- Austin, L. M., and A. Slane. 2023. "Digitally Rethinking Hunter v Southam." *Osgoode Hall Law Journal* 60 (2): 419–472. <https://doi.org/10.60082/2817-5069.3895>. *
- Ayalon, Oshrat, and Eran Toch. 2021. "User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes." *International Journal of Human-Computer Studies* 154 (October): 102641. <https://doi.org/10.1016/j.ijhcs.2021.102641>.
- Balboni, Paolo, and Milda Macenaite. 2013. "Privacy by Design and Anonymisation Techniques in Action: Case Study of Ma3tch Technology." *Computer Law & Security Review* 29 (4): 330–340. <https://doi.org/10.1016/j.clsr.2013.05.005>. *
- Barth, Susanne, Dan Ionita, and Pieter Hartel. 2022. "Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines." *ACM Computing Surveys* 55 (3): 1–37. <https://doi.org/10.1145/3502288>.
- Batalla, A. R. 2022. "The Limits of Privacy By Design." *Revista Catalana De Dret Public* 64 (June): 174–186. <https://doi.org/10.2436/rcdp.i64.2022.3717>. *
- Blythe, John M, Nissy Sombatruang, and Shane D Johnson. 2019. "What Security Features and Crime Prevention Advice Is Communicated in Consumer IoT Device Manuals and Support Pages?" *Journal of Cybersecurity* 5 (1): tyz005. <https://doi.org/10.1093/cybersec/tyz005>. *

- Bu, Fei, Nengmin Wang, Bin Jiang, and Huigang Liang. 2020. "Privacy by Design" Implementation: Information System Engineers' Perspective." *International Journal of Information Management* 53 (August): 102124. <https://doi.org/10.1016/j.ijinfomgt.2020.102124>
- Bu, Fei, Nengmin Wang, Bin Jiang, and Qi Jiang. 2021. "Motivating Information System Engineers' Acceptance of Privacy by Design in China: An Extended UTAUT Model." *International Journal of Information Management* 60 (October): 102358. <https://doi.org/10.1016/j.ijinfomgt.2021.102358>. *
- Buttarelli, Giovanni. 2018. "Preliminary Opinion on Privacy by Design". Opinion 5/2018. Brussels, Belgium: European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.
- Bygrave, L. A. 1998. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties." *International Journal of Law and Information Technology* 6 (3): 247–284. <https://doi.org/10.1093/ijlit/6.3.247>.
- Bygrave, L. A. 2022a. "Cyber Resilience Versus Cybersecurity as Legal Aspiration." In *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, 700:27–43. <https://doi.org/10.23919/CyCon55549.2022.9811084>. *
- Bygrave, L. A. 2022b. "Security by Design: Aspirations and Realities in a Regulatory Context." *Oslo Law Review* 8 (3): 126–177. <https://doi.org/10.18261/olr.8.3.2>.
- Caire, Patrice, Assaad Moawad, Vasilis Efthymiou, Antonis Bikakis, and Yves Le Traon. 2016. "Privacy Challenges in Ambient Intelligence Systems: Lessons Learned, Gaps and Perspectives from the AAL Domain and Applications." *Journal of Ambient Intelligence and Smart Environments* 8 (6): 619–644. <https://doi.org/10.3233/AIS-160405>. *
- Cali, Umit, Marthe Fogstad Dyngre, Ahmed Idries, Sambheet Mishra, Ivanko Dmytro, Naser Hashemipour, and Murat Kuzlu. 2023. "Digital Energy Platforms Considering Digital Privacy and Security by Design Principles." In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference, 167–73*. EICC '23. New York, NY: Association for Computing Machinery. <https://doi.org/10.1145/3590777.3591405>. *
- Cámara, Mercedes de la, Fco Javier Saenz, Jose Antonio Calvo-Manzano, and Magdalena Arcilla. 2015. "Security by Design Factors for Developing and Evaluating Secure Software." In *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. Aveiro, Portugal: IEEE. <https://doi.org/10.1109/CISTI.2015.7170500>. *
- Cámara, Mercedes de la, Javier Saenz-Marcilla, Magdalena Arcilla-Cobian, and Jose A. Calvo-Manzano. 2016. "Security by Design Practices for IT Projects Management in SMEs." In *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. Gran Canaria, Spain: IEEE. <https://doi.org/10.1109/CISTI.2016.7521485>. *
- Carboni, A., D. Russo, D. Moroni, and P. Barsocchi. 2023. "Privacy by Design in Systems for Assisted Living, Personalised Care, and Wellbeing: A Stakeholder Analysis." *Frontiers in Digital Health* 4 (February), <https://doi.org/10.3389/fgdth.2022.934609>.
- Casola, Valentina, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. 2020. "A Novel Security-by-Design Methodology: Modeling and Assessing Security by SLAs with a Quantitative Approach." *Journal of Systems and Software* 163 (May): 110537. <https://doi.org/10.1016/j.jss.2020.110537>. *
- Cavoukian, Ann, and Mark Dixon. 2013. *Privacy and Security by Design: An Enterprise Architecture Approach*. Ontario: Canadá: Information and Privacy Commissioner. *
- Cavoukian, Ann. 2009. *Privacy by Design: The 7 Foundational Principles*. Ontario: Canadá: Information and Privacy Commissioner. *
- Cavoukian, Ann. 2012. *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. Ontario: Canadá: Information and Privacy Commissioner. *
- Chaudhuri, Abhik, and Ann Cavoukian. 2018. "The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design." *EDPACS* 57 (1): 1–16. <https://doi.org/10.1080/07366981.2017.1343548>.
- Craggs, Barnaby. 2019. "A Just Culture Is Fundamental: Extending Security Ergonomics by Design." In *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, edited by Tomas Bures, Bradley Schmerl, John Fitzgerald, and Danny Weyns, 46–49. Montreal, QC: IEEE. <https://doi.org/10.1109/SEsCPS.2019.00015>. *

- Degeling, Martin, Christopher Lentzsch, Alexander Nolte, Thomas Herrmann, and Kai-Uwe Loser. 2016. "Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design." In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, edited by Randall Bilof, 502–505. Pittsburgh, PA: IEEE. <https://doi.org/10.1109/CIC.2016.077>.
- Del-Real, Cristina, and Els De Busser. 2023. *'Defining Security by Design: A Stakeholder's Perspective'*. The Hague: Leiden University. <https://scholarlypublications.universiteitleiden.nl/handle/1887/3715232>.
- Del-Real, Cristina, Els De Busser, and Bibi van den Berg. 2024. "Shielding Software Systems: A Comparison of Security by Design and Privacy by Design Based on a Systematic Literature Review." *Computer Law & Security Review* 52 (April): 105933. <https://doi.org/10.1016/j.clsr.2023.105933>.
- Department for Digital, Culture Media & Sport of the United Kingdom. 2018. *Secure by Design: Improving the Cyber Security of Consumer Internet of Things*. London: His Majesty's Government. *
- Dijk, N. van, A. Tanas, K. Rommetveit, and C. Raab. 2018. "Right Engineering? The Redesign of Privacy and Personal Data Protection." *International Review of Law, Computers & Technology* 32 (2–3): 230–256. <https://doi.org/10.1080/13600869.2018.1457002>.
- Dodge, Martin, and Rob Kitchin. 2001. *Mapping Cyberspace*. London: Routledge.
- Domingo-Ferrer, Josep, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, and George Danezis. 2014. *Privacy and Data Protection by Design - from Policy to Engineering*. Heraklion: ENISA.
- European Parliament and Council of Europe. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).
- European Parliament and Council. 2022. Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020. Vol. COM(2022) 454 final. <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.
- European Telecommunications Standards Institute. 2019. *ETSI TS 103 645 Cybersecurity for Consumer IoT (V1.1.1)*. Sophia-Antipolis, France: ETSI. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.
- Federal Trade Commission. 2012. *Protecting Consumer Privacy in an Era of Rapid Change*. Washington, DC: Federal Trade Commission.
- Fernandez, Eduardo B, Yoshioka Nobukazu, Washizaki Hironori, and Joseph Yoder. 2022. "Abstract Security Patterns and the Design of Secure Systems." *Cybersecurity* 5 (1): 1. <https://doi.org/10.1186/s42400-021-00103-8>.
- Finn, Rachel L., David Wright, and Michael Friedewald. 2013. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet, 3–32. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-5170-5_1.
- Fleiss, Joseph L. 1971. "Measuring Nominal Scale Agreement among Many Raters." *Psychological Bulletin* 76 (5): 378–382. <https://doi.org/10.1037/h0031619>.
- Fluchs, Sarah, Emre Taştan, Tobias Trumpf, Alexander Horch, Rainer Drath, and Alexander Fay. 2023. "Traceable Security-by-Design Decisions for Cyber-Physical Systems (CPSs) by Means of Function-Based Diagrams and Security Libraries." *Sensors* 23 (12): 5547. <https://doi.org/10.3390/s23125547>. *
- Fockel, Markus, Sven Merschjohann, and Masud Fazal-Baqaie. 2018. "Threat Analysis in Practice – Systematically Deriving Security Requirements." In *Product-Focused Software Process Improvement*, Edited by Marco Kuhmann, Kurt Schneider, Dietmar Pfahl, Sousuke Amasaki, Marcus Ciolkowski, Regina Hebig, Paolo Tell, Jil Klünder, and Steffen Küpper, 11271:355–58. Lecture Notes in Computer Science. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-03673-7_25. *
- Freitas, M. B., V. M. Araújo, and J. P. Magalhães. 2023. "Process SDLC-GDPR: Towards the Development of Secure and Compliant Applications." In *2023 1st International Conference on*

- Advanced Innovations in Smart Cities (ICAISC)*, 1–6. Jeddah, Saudi Arabia: Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/ICAISC56366.2023.10085308>.
- Glaser, C. 2023. "The PREVENT-Model: Human and Organizational Factors Fostering Engineering of Safe and Secure Robotic Systems." *Journal of Systems and Software* 195 (January), <https://doi.org/10.1016/j.jss.2022.111548>.
- Gupta, Akanksha. 2022. "An Integrated Framework for DevSecOps Adoption." *International Journal of Computer Trends and Technology* 70 (6): 19–23. <https://doi.org/10.14445/22312803/IJCTT-V70I6P102>. *
- Haber, Eldar, and Aurelia Tamò-Larrieux. 2020. "Privacy and Security by Design: Comparing the EU and Israeli Approaches to Embedding Privacy and Security." *Computer Law & Security Review* 37 (July): 105409. <https://doi.org/10.1016/j.clsr.2020.105409>.
- Hadar, Irit, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. "Privacy by Designers: Software Developers' Privacy Mindset." *Empirical Software Engineering* 23 (1): 259–289. <https://doi.org/10.1007/s10664-017-9517-1>. *
- Hamon, R., H. Junklewitz, J. S. Garrido, and I. Sanchez. 2024. "Three Challenges to Secure AI Systems in the Context of AI Regulations." *IEEE ACCESS* 12:61022–61035. <https://doi.org/10.1109/ACCESS.2024.3391021>. *
- Hartzog, Woodrow, and Frederic D Stutzman. 2013. "Obscurity by Design." *Washington Law Review* 88:385–418. *
- Hartzog, Woodrow. 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press. *
- Hoepman, Jaap-Henk. 2014. "Privacy Design Strategies." In *ICT Systems Security and Privacy Protection*, Edited by Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, and Thierry Sans, 428:446–59. FIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_38.
- Hoepman, Jaap-Henk. 2021. *Privacy Is Hard and Seven Other Myths: Achieving Privacy Through Careful Design*. Cambridge, MA: The MIT Press. *
- Humayun, M., M. Niazi, M. Assiri, and M. Haoues. 2023. "Secure Global Software Development: A Practitioners' Perspective." *Applied Sciences-Basel* 13:4. <https://doi.org/10.3390/app13042465>
- International Organization for Standardization. 2023. ISO/DIS 31700(En), Consumer Protection — Privacy by Design for Consumer Goods and Services. <https://www.iso.org/obp/ui/#iso:std:iso:31700:dis:ed-1:v1:en>.
- Iwaya, Leonardo Horn, Gabriel Horn Iwaya, Simone Fischer-Hubner, and Andrea Valeria Steil. 2022. "Organisational Privacy Culture and Climate: A Scoping Review." *IEEE Access* 10:73907–73930. <https://doi.org/10.1109/ACCESS.2022.3190373>.
- Jagarlamudi, G. K., A. Yazdinejad, R. M. Parizi, and S. Pouriyeh. 2023. "Exploring Privacy Measurement in Federated Learning." *Journal of Supercomputing*, <https://doi.org/10.1007/s11227-023-05846-4>. *
- Janca, Tanya. 2021. *Alice and Bob Learn Application Security*, 65–82. Wiley. <https://ieeexplore.ieee.org/document/9932263>.
- Kang, Sooyoung, and Seungjoo Kim. 2022. "CIA-Level Driven Secure SDLC Framework for Integrating Security Into SDLC Process." *Journal of Ambient Intelligence and Humanized Computing* 13 (10): 4601–4624. <https://doi.org/10.1007/s12652-021-03450-z>.
- Kapitonova, Maryna, Philipp Kellmeyer, Simon Vogt, and Tonio Ball. 2022. "A Framework for Preserving Privacy and Cybersecurity in Brain-Computer Interfacing Applications". arXiv.Org. <https://login.ezproxy.leidenuniv.nl/login?url=https://www.proquest.com/working-papers/framework-preserving-privacy-cybersecurity-brain/docview/2716400165/se-2?accountid=12045>. *
- Khan, Rafiq Ahmad, Muhammad Azeem Akbar, Saima Rafi, Alaa Omran Almagrabi, and Musaad Alzahrani. 2024. "Evaluation of Requirement Engineering Best Practices for Secure Software Development in GSD: An ISM Analysis." *Journal of Software: Evolution & Process* 36 (5): 1–19. *
- Khurshid, A., R. Alsaaidi, M. Aslam, and S. Raza. 2022. "EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme." *IEEE Access* 10:129932–48. <https://doi.org/10.1109/ACCESS.2022.3225973>.

- Klitou, Demetrius. 2014. *Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. Vol. 25. *Information Technology and Law Series*. The Hague: Asser Press. Springer. *.
- Koops, Bert-Jaap, and Ronald Leenes. 2014. "Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the "Privacy by Design" Provision in Data-Protection Law." *International Review of Law, Computers & Technology* 28 (2): 159–171. <https://doi.org/10.1080/13600869.2013.801589>. *.
- Koops, Bert-Jaap, Jaap-Henk Hoepman, and Ronald Leenes. 2013. "Open-Source Intelligence and Privacy by Design." *Computer Law & Security Review* 29 (6): 676–688. <https://doi.org/10.1016/j.clsr.2013.09.005>.
- Landis, J. Richard, and Gary G. Koch. 1977. "The Measurement of Observer Agreement for Categorical Data." *Biometrics* 33 (1): 159. <https://doi.org/10.2307/2529310>.
- Legislature, California State. 2018. "California Consumer Privacy Act of 2018." California Civil Code.
- Liu, Yang, and Andrew Simpson. 2016. "Privacy-Preserving Targeted Mobile Advertising: Requirements, Design and a Prototype Implementation: Privacy-Preserving Targeted Mobile Advertising: Requirements, Design and a Prototype Implementation." *Software: Practice and Experience* 46 (12): 1657–1684. <https://doi.org/10.1002/spe.2403>.
- Macedo, Evandro L. C., Egberto A. R. De Oliveira, Fabio H. Silva, Rui R. Mello, Felipe M. G. Franca, Flavia C. Delicato, Jose F. De Rezende, and Luis F. M. De Moraes. 2019. "On the Security Aspects of Internet of Things: A Systematic Literature Review." *Journal of Communications and Networks* 21 (5): 444–457. <https://doi.org/10.1109/JCN.2019.000048>.
- Malina, Lukas, Gautam Srivastava, Petr Dzurenda, Jan Hajny, and Sara Ricci. 2019. "A Privacy-Enhancing Framework for Internet of Things Services." In *Network and System Security. 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings, Edited by Joseph K. Liu and Xinyi Huang, 11928:77–97. Lecture Notes in Computer Science*. Springer Cham. *.
- Microsoft. 2022. "Microsoft Security Development Lifecycle". Company. 2022. <https://www.microsoft.com/en-us/securityengineering/sdl/>.
- Mogamedi, Sophia, and Sifiso Dlamini. 2021. "Security by Design: Rethinking Resilience of IoT in Healthcare". *.
- Mouraditis, Haralambos. 2010. "Secure by Design: Considering Security from the Early Stages of the Information Systems Development." In *Handbook of Electronic Security and Digital Forensics*, edited by Hamid Jahankhani, David Lilburn Watson, Gianluigi Me, and Frank Leonhardt, 115–132. Danvers: World Scientific. <https://doi.org/10.1142/7110>. *.
- Office of the Privacy Commissioner of Canada. 2010. "Privacy, Trust and Innovation – Building Canada's Digital Advantage." Submission to the Digital Economy Consultation. Canada. https://www.priv.gc.ca/media/1294/sub_de_201007_e.pdf.
- Perera, Charith, Ciaran McCormick, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms." In *Proceedings of the 6th International Conference on the Internet of Things*, edited by Albrecht Schmidt, Florian Michahelles, and Stefan Schneegass, 83–92. Stuttgart, Germany: ACM. <https://doi.org/10.1145/2991561.2991566>. *.
- Perera, Charith, Mahmoud Barhamgi, Arosha K. Bandara, Muhammad Ajmal, Blaine Price, and Bashar Nuseibeh. 2020. "Designing Privacy-Aware Internet of Things Applications." *Information Sciences* 512 (February): 238–257. <https://doi.org/10.1016/j.ins.2019.09.061>.
- Ping, Sam Wen, Jeffrey Cheok Jun Wah, Lee Wen Jie, Jeremy Bong Yong Han, and Saira Muzafar. 2023. "Secure Software Development: Issues and Challenges". arXiv.Org. <https://login.ezproxy.leidenuniv.nl/login?url=https://www.proquest.com/working-papers/secure-software-development-issues-challenges/docview/2894171522/se-2?accountid=12045>. *.
- Piras, Luca, Mohammed Ghazi Al-Obeidallah, Michalis Pavlidis, Haralambos Mouraditis, Aggeliki Tsohou, Emmanouil Magkos, and Andrea Praitano. 2021. "A Data Scope Management Service to Support Privacy by Design and GDPR Compliance." *Journal of Data Intelligence* 2 (2): 136–165. <https://doi.org/10.26421/JDI2.2-3>.
- Polanin, Joshua R., Terri D. Pigott, Dorothy L. Espelage, and Jennifer K. Grotzpetter. 2019. "Best Practice Guidelines for Abstract Screening Large-Evidence Systematic Reviews and Meta-Analyses." *Research Synthesis Methods* 10 (3): 330–342. <https://doi.org/10.1002/jrsm.1354>.

- Popay, Jennie, Helen Roberts, Amanda Sowden, Mark Petticrew, Lisa Arai, Mark Rodgers, Nicky Britten, Katrina Roen, and Steven Duffy. 2006. *Guidance on the Conduct of Narrative Synthesis in Systematic Reviews: A Product from the ESRC Methods Programme*. Lancaster: Lancaster University. <https://doi.org/10.13140/2.1.1018.4643>.
- Porcedda, Maria Grazia. 2018. "Privacy by Design" in EU Law: Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection." In *Privacy Technologies and Policy*, Edited by Manel Medina, Andreas Mitrikas, Kai Rannenber, Erich Schweighofer, and Nikolaos Tsouroulas, 11079:183–204. Lecture Notes in Computer Science. Cham: Springer International Publishing https://doi.org/10.1007/978-3-030-02547-2_11. *
- Prybylo, Maxwell, Sara Haghighi, Sai Teja Peddinti, and Sepideh Ghanavati. 2024. "Evaluating Privacy Perceptions, Experience, and Behavior of Software Development Teams". arXiv.Org. <https://login.ezproxy.leidenuniv.nl/login?url=https://www.proquest.com/working-papers/evaluating-privacy-perceptions-experience/docview/3030950628/se-2?accountid=12045>. *
- Rachovitsa, Adamantia. 2016. "Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue." *International Journal of Law and Information Technology* 24 (4): 374–399. <https://doi.org/10.1093/ijlit/eaw012>.
- Radunovic, Vladimir, Jonas Gratz-Hoffmann, and Marilia Maciel. 2021. "Impact of Good Corporate Practices for Security of Digital Products on Global Cyber Stability." In *2021 13th International Conference on Cyber Conflict (CyCon)*, edited by Taťána Jančárková, Lauri Lindström, Gábor Visky, and Philippe Zotz, 25–42. Tallinn, Estonia: IEEE. <https://doi.org/10.23919/CyCon51939.2021.9467805>. *
- Rest, Jeroen van, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen. 2014. "Designing Privacy-by-Design." In *Privacy Technologies and Policy*, Edited by Bart Preneel and Demosthenes Ikonoumou, 8319:55–72. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-54069-1_4.
- Restuccia, Francesco, Salvatore D'Oro, and Tommaso Melodia. 2018. "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking." *IEEE Internet of Things Journal* 5 (6): 4829–4842. <https://doi.org/10.1109/JIOT.2018.2846040>.
- Romanou, Anna. 2018. "The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise." *Computer Law & Security Review* 34 (1): 99–110. <https://doi.org/10.1016/j.clsr.2017.05.021>. *
- Rost, Martin, and Kirsten Bock. 2011. "Privacy by Design and New Protection Goals: Principles, Goals and Requirements." *European Privacy Seal*. *
- Rubinstein, Ira, and Nathan Good. 2012. "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents." *SSRN Electronic Journal*, <https://doi.org/10.2139/ssrn.2128146>.
- Saltarella, M., G. Desolda, R. Lanzillotti, and V. S. Barletta. 2023. "Translating Privacy Design Principles into Human-Centered Software Lifecycle: A Literature Review." *International Journal of Human-Computer Interaction*. <https://doi.org/10.1080/10447318.2023.2219964>
- Saunders, Tony I. 2021. "Cybersecurity Challenges of the IoT-Enabled Home Automation Technology: A Security by Design Perspective". PhD diss., Arlington, Virginia, US: Marymount University. *
- Schoot, Rens van de, Jonathan de Bruin, Raoul Schram, Parisa Zahedi, Jan de Boer, Felix Weijdem, Bianca Kramer, et al. 2021. "An Open Source Machine Learning Framework for Efficient and Transparent Systematic Reviews." *Nature Machine Intelligence* 3 (2): 125–133. <https://doi.org/10.1038/s42256-020-00287-7>.
- Semantha, Farida Habib, Sami Azam, Kheng Cher Yeo, and Bharanidharan Shanmugam. 2020. "A Systematic Literature Review on Privacy by Design in the Healthcare Sector." *Electronics* 9 (3): 452. <https://doi.org/10.3390/electronics9030452>.
- Shaabany, Ghaidaa, and Reiner Anderl. 2018. "Security by Design as an Approach to Design a Secure Industry 4.0-Capable Machine Enabling Online-Trading of Technology Data." In *2018 International Conference on System Science and Engineering (ICSSE)*, 1–5. New Taipei: IEEE. <https://doi.org/10.1109/ICSSE.2018.8520195>. *
- Shirtz, Dov, Inna Koberman, Aviad Elyashar, Rami Puzis, and Yuval Elovici. 2024. "Enhancing Energy Sector Resilience: Integrating Security by Design Principles". arXiv.Org. <https://login.ezproxy>.

- leidenuniv.nl/login?url = <https://www.proquest.com/working-papers/enhancing-energy-sector-resilience-integrating/docview/2928718752/se-2?accountid=12045>. *
- Singapore, C. S. A. 2017. 'Security-by-Design Framework Version 1.0'. Framework. Singapore: Cyber Security Agency of Singapore. *
- Slesinger, Ian, Lizzie Coles-Kemp, Niki Panteli, and Rene Rydhof Hansen. 2023. "Designing Through The Stack: The Case for a Participatory Digital Security By Design." In *Proceedings of the 2022 New Security Paradigms Workshop*, 45–59. NSPW '22. New York, NY: Association for Computing Machinery. <https://doi.org/10.1145/3584318.3584322>. *
- Slesinger, Ian, Niki Panteli, and Lizzie Coles-Kemp. 2024. "Regulating Digital Security by Design? Implications of the Perspectives from DSbD Programme Stakeholders." INFORMATION AND COMPUTER SECURITY. <https://doi.org/10.1108/ICS-01-2023-0010>.
- Sokolovska, Ana, and Ljupco Kocarev. 2018. "Integrating Technical and Legal Concepts of Privacy." *IEEE Access* 6:26543–26557. <https://doi.org/10.1109/ACCESS.2018.2836184>.
- Spiekermann, Sarah. 2012. "The Challenges of Privacy by Design." *Communications of the ACM* 55 (7): 38–40. <https://doi.org/10.1145/2209249.2209263>. *
- Thomson, Judith J. 1975. "The Right to Privacy." *Philosophy & Public Affairs* 4 (4): 295–314.
- Tjondronegoro, Dian, Elizabeth Yuwono, Brent Rischards, Damian Green, and Siiri Hatakka. 2022. "Responsible AI Implementation: A Human-Centered Framework for Accelerating the Innovation Process". arXiv.Org. <https://login.ezproxy.leidenuniv.nl/login?url=https://www.proquest.com/working-papers/responsible-ai-implementation-human-centered/docview/2714977168/se-2?accountid=12045>. *
- Tricco, Andrea C., Erin Lillie, Wasifa Zarin, Kelly K. O'Brien, Heather Colquhoun, Danielle Levac, David Moher, et al. 2018. "PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation." *Annals of Internal Medicine* 169 (7): 467–473. <https://doi.org/10.7326/M18-0850>.
- Ulhaq, Anwaar, and Oliver Burmeister. 2020. "COVID-19 Imaging Data Privacy by Federated Learning Design: A Theoretical Framework". arXiv. <http://arxiv.org/abs/2010.06177>. *
- Umeugo, Wisdom, Kimberly Lowrey, and Shardul Pandya. 2023. "Factors Affecting the Adoption of Secure Software Practices in Small and Medium Enterprises That Build Software In-House." *International Journal of Advanced Research in Computer Science* 14 (2): 1–7. <https://doi.org/10.26483/ijarcs.v14i2.6955>.
- Valdés-Rodríguez, Yolanda, Jorge Hochstetter-Diez, Jaime Díaz-Arancibia, and Rodrigo Cadena-Martínez. 2023. "Towards the Integration of Security Practices in Agile Software Development: A Systematic Mapping Review." *Applied Sciences* 13 (7): 4578. <https://doi.org/10.3390/app13074578>. *
- Waldman, Ari Ezra. 2020. "Data Protection by Design? A Critique of Article 25 of the GDPR." *Cornell International Law Journal* 53:147–167. *
- Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* IV 5 (5): 193–220. <https://doi.org/10.2307/1321160>.
- Wilkinson, Darcia, Saadhika Sivakumar, David Cherry, Bart P. Knijnenburg, Elaine Raybourn, Pamela Wisniewski, and Henry Sloan. 2017. "(Work in Progress) User-Tailored Privacy by Design." In *Proceedings 2017 Workshop on Usable Security*. San Diego, CA: Internet Society. <https://doi.org/10.14722/usec.2017.23007>. *
- Wohlgemuth, Sven. 2014. "Adaptive User-Centered Security." In *Advanced Information Systems Engineering*, Edited by Camille Salinesi, Moira C. Norrie, and Óscar Pastor, 7908:94–109. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-319-10975-6_7. *
- Zedner, L. 2003. "The Concept of Security: A Comparative Analysis." *Legal Studies* 23 (1): 153–176.
- Zhao, J. 2023. "Design of Whole Life Cycle Protection Framework for Financial Consumer Information." In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 01–05.
- Raichur, India: IEEE. <https://doi.org/10.1109/ICICACS57338.2023.10099862>.