Requirements Engineering (2022) 27:545–567
https://doi.org/10.1007/s00766-022-00391-7

ORIGINAL ARTICLE

Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation

Edna Dias Canedo[1] · Angelica Toffano Seidel Calazans[2] · Ian Nery Bandeira[1] · Pedro Henrique Teixeira Costa[1] · Eloisa Toffano Seidel Masson[2]

Received: 21 January 2022 / Accepted: 7 October 2022 / Published online: 4 November 2022

Abstract

The Brazilian General Data Protection Law (LGPD) implementation has impacted activities carried out by the software development teams. Due to it, developers had to become aware of the existing techniques and tools to carry out privacy requirements elicitation. Extending our previous work, we have investigated the actions taken by organizations regarding the LGPD, specifically in software development, considering the perception of agile development teams after two years of the LGPD implementation. In addition, we also investigated the perception of an agile team regarding the practices, techniques, and tools previously cited by practitioners as potential solutions for use in this context, along with techniques already in use in the current context. We have conducted a systematic literature review (SLR) and selected 36 primary studies. Furthermore, we have conducted a survey with 53 IT practitioners and semi-structured interviews with ten practitioners. The LGPD principles are known by most agile teams and are being implemented by the organizations, although the existing tools to support privacy requirements elicitation are still underused by agile teams. Moreover, agile teams consider that software requirements and software construction are the most impacted areas of knowledge by the LGPD, and most of them use user stories in privacy requirements elicitation. Our findings reveal that agile teams and Brazilian organizations are more concerned with user data privacy issues after the LGPD became effective. However, agile teams still face challenges in privacy requirements elicitation.

Keywords Privacy requirements elicitation · Agile teams · Techniques · Perception · LGPD

1 Introduction

Data privacy has become a major concern in software development, mainly due to the requirements of data protection laws, such as the General Data Protection Regulation 2016/679 (GDPR) [1] and the Brazilian General Data Protection Law (LGPD) [2]. Data privacy violations can be prevented if privacy requirements are set correctly during the early stages of the software development process [3]. According to Thomas and Blaine [4], privacy can be regarded as a non-functional requirement because it focuses on obtaining and processing large amounts of users' personal data.

Several research studies have identified that software developers lack knowledge of software privacy and do not have the technical knowledge necessary to develop systems that work with sensitive data [5]. In addition, software developers do not know the principles of data privacy, and when building software, they make ad hoc decisions and do not worry about the best practices developed by the academy to facilitate requirements elicitation and ensure data privacy of users. This behavior probably occurs due to the lack of knowledge of the existing techniques and methodologies [6].

All phases of a system development life cycle need to incorporate privacy components to achieve comprehensive

✉ Edna Dias Canedo
ednacanedo@unb.br

Angelica Toffano Seidel Calazans
angelica.toffano@gmail.com

Ian Nery Bandeira
iannerybandeira@gmail.com

Pedro Henrique Teixeira Costa
phtcosta@gmail.com

Eloisa Toffano Seidel Masson
eloisa.masson@ceub.edu.br

[1] Computer Science Department, University of Brasília (UnB), P.O. Box 4466 Brasília, DF, Brazil

[2] University center – UniCEUB, Brasília, DF, Brazil

privacy protection [7]. Designers and software developers often treat privacy as a secondary concern or a problem for future exploration [7], which leads to the construction of systems that fail to provide adequate information privacy [8]. Therefore, privacy issues are a necessary concern in all phases of Requirements Engineering, i.e., the specification of functional and non-functional requirements [9–11].

In requirements elicitation, agile teams work with stakeholders to understand the application domain, operational constraints, functional and non-functional requirements [12]. Agile methodologies recognize that requirements constantly change, evolve over time, and are discovered throughout the software development process [13]. Agile software development has several benefits, such as improved user satisfaction, changing requirements definition during any phase of the development process, frequent software delivery, and close stakeholder interaction [14]. According to Wagner et al. [15], non-functional requirements elicitation in agile software development is still neglected during its definition and documentation. Li et al. [16] reinforced this statement, mentioning that some startups change their processes quickly to meet market needs, which may lead them to neglect non-functional requirements during this process.

In our previous work [17], we carried out a systematic literature review (SLR) to identify the techniques, methodologies, and tools used in the literature to perform privacy requirements elicitation in the context of Agile Software Development (ASD). We also conducted an online survey to investigate the perception of agile teams regarding the impact that the Brazilian General Data Protection Law (LGPD) had had on their activities during software development. Furthermore, we investigated whether agile teams correctly interpret privacy principles and implement these concepts and principles during software development, along with what actions could have been taken to reduce the impact of needing to implement systems according to data privacy laws by agile development teams.

Other previous works have investigated the evolution of Brazilian organizations and practitioners in this context. Serasa Experian [18] conducted a survey in March 2020 and obtained 513 respondents. The results showed that 71% of Brazilian organizations and practitioners have a medium and high level of knowledge regarding the LGPD principles. In 2019, this percentage was 66%. The National Association of Data Privacy Professionals (ANPPD) [19] identified that 99% of organizations are motivated to adopt or are already implementing LGPD regulations into their organizational environment. The ANPPD identified that 86% of practitioners in organizations have knowledge regarding the principles of the LGPD, and approximately 48% of organizations have trained or are training their practitioners regarding the LGPD.

Canedo et al. [20] conducted a survey with ICT practitioners from software development organizations to get an overview of how these professionals were implementing data privacy concepts during software design. The authors also performed a systematic literature review to identify related works with software privacy and privacy requirements and what methodologies and techniques were used to specify them. The findings revealed that the practitioners lacked knowledge about software privacy, privacy requirements, and LGPD. Moreover, the survey participants stated that they could not work with data privacy laws and guidelines.

In this paper, we expand our previous work [17] towards investigating the actions adopted by organizations and specifically the actions in software development, considering the perception of agile development teams two years after the implementation of LGPD in Brazil. Thus, we investigate the current level of knowledge of agile teams regarding the LGPD and its principles, what privacy solutions the teams are adopting, and the techniques and tools used by agile development teams after the LGPD came into effect. In addition, we will identify what modifications have been made by organizations in their software development process during this period to become LGPD compliant, as well as what other alternatives are being used and implemented by organizations due to the LGPD principles.

The main contribution of our work is to understand the perception of agile teams regarding the actions and changes adopted by the organizations after the LGPD became effective, as well as to identify which organizational procedures were adopted concerning user data privacy and the changes made in how the teams work to ensure LGPD compliance.

Our findings reveal that agile teams and organizations are more concerned about user data privacy issues. Moreover, agile teams are more familiar with the principles of the LGPD and currently work with and implement all the principles of the law during the software development process.

2 Background and related works

2.1 Brazilian general data protection law (LGPD)

In August 2020, Law No. 13,709 - Brazilian General Data Protection Law (LGPD) [2], which foresees personal data protection, came into force. The LGPD was published in August 2018, but did not go into effect until August 2020. This Law applies to organizations in Brazil and organizations that are not physically located in Brazil but offer goods and services or process personal data in Brazil, and its primary purpose is the processing of individuals' personal data, i.e., information related to an identified natural person, such as name, age, marital status, and documents, performed by controllers and processors [2]. Regarding data privacy, several models were proposed with principles similar to LGPD [21, 22], among them ISO/IEC 29100 – Information technology — Security techniques — Privacy framework [23] and the General Data Protection Regulation – GDPR [1, 24]. GDPR started effect in the European Union (EU) on May 25, 2018, through the Regulation EU 2016/679 [1].

According to the Data Guidance by OneTrust [25], LGPD and GPDR have many similarities with a few disagreements regarding individuals' personal data processing. LGPD provides ten principles while GDPR provides seven [26]. It must be highlighted that ISO/IEC 29100 [23] has twelve principles, and most of them are similar to GDPR [1, 24] and LGPD principles [2], and the other principles are referred to as "individual rights" or "legal bases". For example, Consent and Choice is a principle in ISO/IEC 29100 [23]; however, it is considered a legal basis/individual right in LGPD and GDPR.

Ayala-Rivera and Pasquale [24], and Otto and Anton [27] mention that regulations are usually vaguely formulated and may contain ambiguities, cross-references, and domain-specific definitions, making it difficult for IT professionals to extract and operationalize privacy requirements. Regardless of the model adopted by the country or organization, several authors identify the need to study the views of information and communication technology (ICT) practitioners on privacy and the organization's position on privacy, among other aspects [5, 28].

Following the implementation of the LGPD in 2020, several proposals and studies have been carried out within the scope of the LGPD, including the work of Martins et al. [29], which proposed an automatic manner to apply formal concept analysis (FCA) to elicit key insights to support software development or re-design in compliance with LGPD. FCA is a conceptual modeling technique that can capture how objects (concepts) can be hierarchically clustered based on the attributes they have in common. Bax et al. [30] conducted preliminary research that examines enabling elements for the semantic integration of a consent mechanism under the General Data Protection Law with legacy systems. The authors intend to create an ontology and a systemic approach to support this integration.

Araujo et al. [31] proposed a process to assist organizations in implementing LGPD, named the LGPD4BP (LGPD for Business Process) Method, along with a catalog of modeling patterns using the Business Process Modeling Notation (BPMN). LGPD4BP was applied in a case study, whereas the setting was the enrollment process of a Laboratory School of the Federal University of Pernambuco. According to the authors, LGPD4BP can be used as a reference for modeling LGPD compliant business processes. Canedo et al. [17] also proposed a process to support the implementation of LGPD using the BPMN. The proposed process was applied in a Brazilian Federal Public Administration (FPA) Agency, and the results showed that the process could be applied in any FPA agency and in the industry.

Ribeiro et al. [32] proposed a model to select best practices for implementing personal data security criteria at the University of Brasília (UnB). The authors utilized the Multiple Criteria Decision Analysis (MCDA) process with the Preference Ranking Organization Method for Enriched Evaluation (PROMETHEE) II method to select the best to worst alternatives, according to the criteria selected in the MCDA process using the method Analytic Hierarchy Process (AHP). According to the authors, using the MCDA and PROMETHEE II helped prioritize and identify the key initiative the University needed to take to implement personal data security in its various LGPD-compliant systems.

In an inspection context, Mendes et al. [33] proposed um inspection checklist to evaluate software systems regarding their adherence to the LGPD. The final evaluation checklist contains 52 attributes distributed in evaluation categories, such as transparency, legal rights, security, contentment, and responsibility. The authors applied the checklist to evaluate a government web application. The initial results indicated that the current version of the checklist allowed the identification of problems regarding the adherence of software systems to the LGPD.

Within the context of maturity models, Muncinelli et al. [34] analyzed the major areas of contribution to the process capability assessment for the digital transformation of cybersecurity in the context of personal data, according to the principles of the LGPD. The authors cataloged the main components for a capability model, their functionalities, and the underlying flows within the LGPD context.

Sakamoto et al. [35] investigated professionals' awareness in Brazilian organizations regarding the LGPD. The authors found that 99% of organizations were motivated to adopt or were already implementing the LGPD principles in their organizational environment, and 86% of survey participants said they were familiar with the LGPD principles.

Aiming to gather the perception of agile software development team members from different organizations regarding the impact that LGPD will have on the activities of the software development process, Canedo et al. [17] investigated said context and identified, among other findings, that agile teams know the concepts related to data privacy legislation. However, they do not use the techniques proposed in the literature to perform privacy requirements elicitation and stakeholders' lack of knowledge regarding data privacy. It is worth noting the work done by Alhazmi et al. [36], despite not focusing on the LGPD, explored, through an experimental survey, the problems that programmers encounter when implementing the privacy that concerns all GDPR principles. Among the authors' findings, they identified that participants lacked resources and online materials for reference and guidance when implementing data privacy, and the implementation of GDPR, when developing privacy-preserving software systems, is affected by organizations or the customer.

2.2 Privacy versus Agile methodologies

Privacy is a dynamic concept, contingent upon changing social norms and technology [5]. Smith et al. [37] identified four constructs related to the concept of privacy, namely: 1) Control – the selective control of access to the self; 2) State – state of limited access to a person; 3) Right – general privacy as a right; and 4) Commodity – privacy is subject to the economic principles of cost–benefit analysis and trade-off. According to Kalloniatis et al. [38], privacy is the ability and the right of an individual to control of access their own information.

Privacy violations can be prevented if privacy requirements are properly identified/elicited during the initial stages of software development at the requirements specification stage. Thus, privacy becomes increasingly important in the way users rely on software to perform their daily activities [38]. Several authors have recognized the increased interest in privacy and requirements in recent years [39, 40]. Privacy Engineering, according to Gurses and Álamo [39], encompasses the following aspects: privacy engineering methods, privacy engineering techniques, and privacy engineering tools.

Regarding the concepts of privacy, requirements elicitation, and agile methodologies, a considerable amount of work covering the aspect of privacy engineering methods and requirements [41–43] can be found in the literature. However, a small amount of work focused on privacy techniques – which relate to procedures, prescribed language or notation, for performing privacy engineering tasks or activities – and requirements, especially when these techniques are related to agile methodologies and specifically to user story and use case.

User stories and use cases are popular techniques in requirements engineering. A use case describes the interaction between a user and the system from the user's perspective to achieve a particular goal [44]. Agile methodologies use user stories to capture software requirements [45]. They are comprised of short sentences written in natural language expressing units of functionality for the to-be system [44]. User stories can be written in different layers of detail and can cover a wide range of features, called Epics, which are usually broken down into several smaller user stories before being implemented. In some instances, user stories are further detailed by adding satisfaction conditions, i.e., a high-level description of the requirement. User stories are the predominant technique to capture requirements in agile software development [46]. User stories can also be employed as a requirement documentation technique due to their simplicity, comprehensibility, and popularity in agile development [46]. They are easy to learn and can also be applied by stakeholders without any notation or modeling skills. Furthermore, user stories stimulate collaboration and facilitate requirements elicitation, specification, planning, estimation, and prioritization [47].

Using user story and use case techniques, Bartolini et al. [48], in order to be compliant with GDPR principles, suggest the creation of Access Control Policies (ACPs) aligned with the principles of GDPR and the user stories. The work presented by Rygge et al. [49] suggests the use of Threat Poker to help identify security and/or privacy risks during agile software development.

3 Method

In our previous work [17], we have conducted a systematic literature review (SLR), according to the guidelines proposed by Kitchenham et al. [50] to identify the methodologies and techniques used for privacy requirements elicitation during the agile software development process. We have identified several methodologies and techniques used in the literature and the industry.

In this work, we have conducted an online survey with several agile software development teams practitioners. In addition, we have conducted ten semi-structured interviews with practitioners of agile teams to understand what their organizations have modified in the software development process to address privacy requirements after the LGPD came into effect, in order to prevent fines and sanctions by law enforcement agencies on organizations that do not comply with LGPD as of August 2021.

We have used triangulation to perform data analysis. The data triangulation aims to cover the breadth in the description, explanation and understanding of the study under analysis [51]. Data triangulation uses different data sources, including different times for data collection, different locations for data collection, and different people who may be involved in the study. The starting point is to explicitly and systematically involve people and study groups, local and temporal configurations in the study [52]. We performed data analysis through triangulation using 3 sources: (1) systematic literature review, (2) survey and (3) semi-structured interviews. Figure 1 presents the details of data triangulation adopted in this research.

We conducted the semi-structured interviews in order to validate or refute the results obtained in the survey. As research concerns pertain to values, beliefs, motivations, person-environment interactions, human behavior, and meanings, a quantitative approach alone is inadequate [53]. Thus, the qualitative approach was used to explore

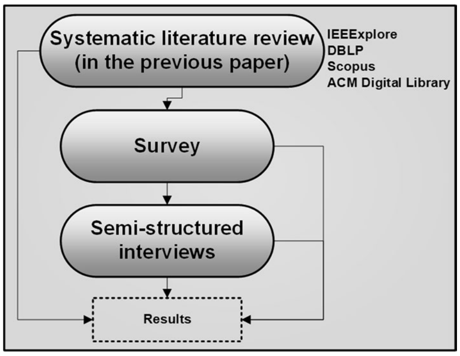

Systematic literature review (in the previous paper)
IEEExplore
DBLP
Scopus
ACM Digital Library
Survey
Semi-structured interviews
Results

Fig. 1 Adopted data triangulation scheme [17]

these issues from the perspectives of the study participants themselves.

3.1 Systematic literature review

We updated the systematic literature review (SLR) performed in the previous work [17] using the same defined protocol. The execution phase involves the search, selection, and evaluation of primary studies following the inclusion and exclusion criteria defined in the protocol [50]. Once the studies have been selected, data from the included primary studies can be extracted and synthesized during the results analysis phase.

3.1.1 Research questions

We have defined the following research questions to conduct this research:

RQ.1 What practices/techniques, and tools are used by agile teams to elicit privacy requirements that comply with the Brazilian General Data Protection Law?

RQ.2 What actions/changes have Brazilian organizations taken to develop LGPD-compliant software?

3.1.2 Search strategy

We proposed a protocol to specify the steps and criteria involved in carrying out the SLR. A review protocol includes details of how different types of studies are to be found, evaluated, and synthesized [54]. In the protocol were defined the research questions, the search strategies adopted to identify the relevant primary studies, the search string to use in the databases, the exclusion/inclusion criteria, and the quality assessment criteria. In addition, the data extraction and analysis process were determined.

The strategy for collecting the studies contained the following steps: (i) automatic search of electronic databases, (ii) manual search of journals, conferences, and workshops, (iii) analysis of the reference lists of other secondary studies in privacy requirements elicitation, known as snowballing.

We used the following digital bases for automatic search: ACM Digital Library, IEEE Xplore Digital Library, Scopus and dblp computer science bibliography. The search strings adopted were: TITLE-ABS-KEY ((“requirements engineering” OR “requirements approach” OR “requirements methodology” OR “requirements process” AND (“elicitation” OR “requirements elicitation” OR “requirements specification” OR “requirements gathering” OR “requirements capture”) AND (“technique” OR “method” OR “tool”) AND (“agile software development” OR “agile development”) AND (“privacy” or “security”) or “ Brazilian General Data Protection Law” or “LGPD”)).

3.1.3 Selection criteria (inclusion and exclusion)

We have defined the following selection criteria for the selection of primary studies: 1. The work must be available in the digital databases previously defined. 2. The year of publication of the studies must be between 2005 and 2021. However, classic sources with definitions (books with classic concepts or pioneering papers) can also be considered. 3. The work must be related to the context of privacy requirements elicitation. 4. The study should propose or use/evaluate existing methods, methodologies, techniques or tools to perform privacy requirements elicitation in the context of agile software development.

As a criteria for exclusion from studies, we consider the non-fulfillment of any of the inclusion criteria, as well as: 1. Works published as short paper; 2. Works that do not present enough information to extract the expected data, thus impairing its the quality or relevance.

3.1.4 Quality criteria

The evaluation of the quality of the studies identified by the search strategy execution made it possible to select the most relevant papers to compose the SLR that was executed using the four selection steps of studies [54]: 1. Search strategy execution involving automatic and manual searches. After that, a preliminary list of studies was generated, and with the help of StArt tool it was possible to discard duplicates immediately; 2. Identification of potentially relevant studies, based on reading the title and abstract. In this step, it was possible to discard studies that were clearly irrelevant to the research. In case of doubt about the permanence of any study in SLR, the next step helped to decide; 3. Reading of the introduction, methodology and conclusion of the pre-selected works, applying again the inclusion and exclusion criteria; 4. The works selected in step 3 were read in full and the volume

Table 1 Selected primary studies in systematic literature review

ID	Title	Reference
S1	Privacy requirements engineering in Agile software development: a specification method	[55]
S2	PCM tool: privacy requirements specification in agile software development	[41]
S3	Requirements engineering: a systematic mapping study in agile software development	[56]
S4	A requirements engineering techniques review in Agile software development methods	[57]
S5	Privacy by design in Agile software development	[58]
S6	Security and privacy as hygiene factors of developer behavior in small and Agile teams	[59]
S7	Metrics to meet security - privacy requirements with Agile software development methods in a regulated environment	[60]
S8	Empathy and criativity in privacy requirements elicitation: systematic literature review	[61]
S9	Experiences in the development and usage of a privacy requirements framework	[62]
S10	Security, compliance, and Agile deployment of personal identifiable information solutions on a public cloud	[63]
S11	The Odyssey: modeling privacy threats in a brave new world	[64]
S12	Aligning security objectives with Agile software development	[65]
S13	An empirical perspective on security challenges in large-scale Agile software development	[66]
S14	Towards a secure SCRUM process for Agile web application development	[67]
S15	GDPR-based user stories in the access control perspective	[48]
S16	Identifying how the Brazilian software industry specifies legal requirements	[68]
S17	Perceptions of ICT poractitioners regarding software privacy	[26]
S18	Information security in Agile software development projects: a critical success factor perspective	[69]
S19	The security intention meeting series as a way to increase visibility of software security decisions in agile development projects	[70]
S20	Towards risk-driven security requirements management in Agile software development	[71]
S21	Collaborative security risk estimation in agile software development	[72]
S22	Threat modelling and agile software development: identified practice in four Norwegian organisations	[73]
S23	Using the design thinking empathy phase as a facilitator in privacy requirements elicitation	[20]
S24	Are my business process models compliant with LGPD? The LGPD4BP method to evaluate and to model LGPD aware business processes	[31]
S25	Components of the preliminary conceptual model for process capability in LGPD (Brazilian data protection regulation) context	[34]
S26	Developing an lnspection checklist for the adequacy assessment of software systems to quality attributes of the Brazilian general data protection law: an initial proposal	[33]
S27	LGPD: a formal concept analysis and its evaluation	[29]
S28	Proposal of an implementation process for the Brazilian general data protection law (LGPD)	[22]
S29	Proposta de mecanismo de consentimento na Lei geral de proteção a dados - LGPD	[30]
S30	Software optimization for LGPD compliance using paraconsistent evidential annotated logic Eτ	[35]
S31	Using MCDA for selecting criteria of LGPD compliant personal data security	[32]
S32	Agile Teams' perception in privacy requirements elicitation: LGPD's compliance in Brazil	[17]
S33	I'm all ears! listening to software developers on putting GDPR principles into software development practice	[36]
S34	Effects and projections of the Brazilian general data protection law (LGPD) application and the role of the DPO	[74]
S35	Brazil's data protection law: putting brazil on the map of data privacy frameworks	[75]
S36	After Brazil's general data protection law: authorization in decentralized web applications	[76]

of studies resulting in this step (36 primary studies) was used to compose the SLR and support the answers to the research questions.

3.1.5 Systematic literature review results

The automatic search on digital databases resulted in 40 studies, and the manual search performed in the Annals of Conferences and Journals resulted in a total of 13 studies (53 pre-selected papers). After applying all the steps of the paper selection strategy, 36 primary studies to be used in data extraction were identified. Table 1 shows the primary studies used in the SLR.

3.2 Survey

We designed a survey to investigate and understand how software development teams using agile methodologies are performing the elicitation of privacy requirements after the LGPD came into effect. The survey was divided into three parts and contained 36 questions, as presented in Supplementary Material Table 1, available at Zenodo (https://zenodo.org/record/6989476). The first part contained the questions related to the participants' demographic information. Most of the questions in the second part of the survey were close-ended questions, mainly using the Likert scale [77] as possible answers: Strongly Disagree; Disagree; Neutral; Agree; Strongly Agree. 7 questions in this stage were open-ended, and their goal was to understand the impact of the LGPD on agile software development in aspects not covered by the close-ended questions. The survey questions and their corresponding answer choices are available in the "2-Survey_Questions.pdf" file in the Supplementary Material at Zenodo (https://zenodo.org/record/6989476).

The third and last part of the survey aimed at identifying possible candidates interested in providing us with an interview. In this step, we asked the participants if they were interested in participating in an interview about data privacy and LGPD in agile projects, if so, what was the contact for the interview (phone and email), and what was the best time for us to contact them.

We asked for participation on mailing lists and within our personal contacts. The survey was available for approximately two months. Participation was voluntary, and all the participants allowed the researcher to use and disclose the information provided while conducting the research. The survey contained 36 questions and the estimated time to complete the survey was 14–18 min. 53 IT practitioners answered all questions of our questionnaire.

3.3 Semi-structured interviews

To complement the survey's answers, we conducted semi-structured interviews with some practitioners from different Brazilian organizations. The interview participants were contacted based on the information they provided in the survey. All the practitioners who informed that they would like to participate in an interview were contacted. In total, we had 10 practitioners interviewed. During the interviews, we adhered the questions provided in Section 2 of the Supplementary Material available at Zenodo (https://zenodo.org/record/6989476).

We have employed Grounded Theory (GT) to analyze the data obtained from the open-ended survey and interview questions. GT was originally proposed by Glaser and Strauss [78]. GT is an approach to hypothesize through qualitative analysis procedures, in contrast to approaches that use statistical methods to confirm or refute pre-established hypotheses [79]. Furthermore, Grounded Theory is an approach suitable for answering research questions that aim to characterize scenarios from a personal perspective of those interested in an issue or activity [80]. Furthermore, Grounded Theory is useful when we want to learn how people manage their lives in the context of a problematic situation and is useful for learning the process of how people understand and deal with what is happening to them through time and changing circumstances [81]. This is the scenario presented in this research, as we aimed to investigate agile teams' perceptions of LGPD implementation during the software development process. We used the version of Grounded Theory proposed by Glaser [82]. Glaser keeps his attention focused on the data and asks, "what do we have here?" [83].

We performed the data analysis using the guideline on how to conduct a GT survey [81]. The guideline organizes a GT investigation in a) Open coding data collection; b) Selective coding data analysis; and c) Theoretical coding. The first two authors performed the survey and interview responses coding, and the third author performed a review of the results.

4 Results

4.1 SLR results

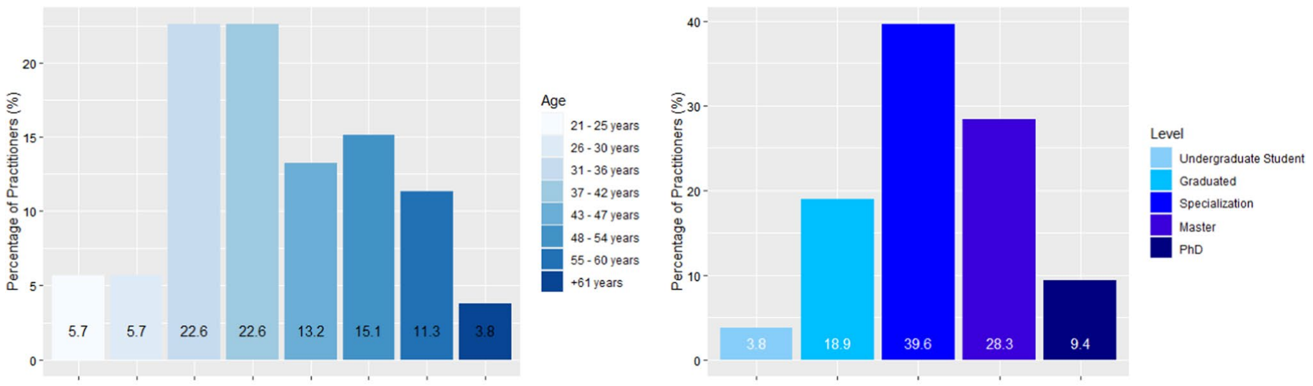
Most selected primary studies proposed a technique, method, or tool to address privacy or security in agile software development [41, 48, 55, 60, 62, 63, 67, 70–72]. Regarding the specific context of the LGPD, some selected papers proposed a process, protocol, method, framework, or checklist [22, 29, 31, 32, 76].

Other selected works were Requirements Engineering reviews; although they do not deal specifically with privacy, these studies show some results related to data privacy [56, 57].

Other works identified challenges and opportunities in the context of agile teams, privacy and privacy by design, and security [20, 58, 61, 64–66, 68, 69, 73].

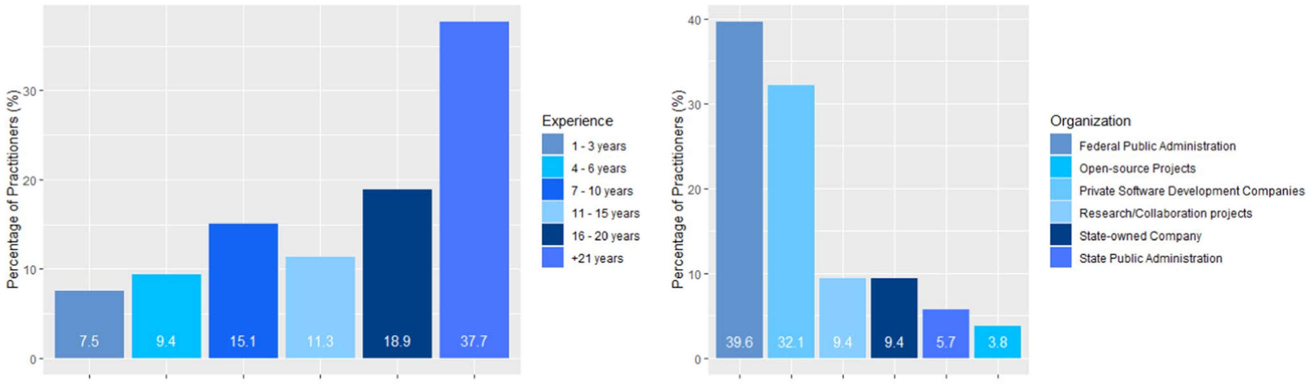
Some studies have analyzed the behavior and perceptions of ICT practitioners concerning privacy [36, 59]. Focusing exclusively on the LGPD and analyzing the perception of ICT practitioners, we identified the works of [17, 26, 35].

Bax et al. [30] have proposed an ontology to implement user consent regarding their personal data in the context of the LGPD, Muncinelli et al. [34] proposed a maturity model in accordance with the LGPD, and Mendes et al. [33] developed an inspection checklist for the adequacy of LGPD. Palhares [75] analyzed the history of Brazilian laws that contain privacy and data protection clauses to compare them with the LGPD. Pessoa et al. [74] analyzed the impact of LGPD's application on routine organizational business and the role of a Data Protection Officer in organizations.



(a) **(b)**

Fig. 2 Figure **a** shows the agile teams' practitioners' age (P2 of Supplementary Material Table 1), while **b** shows their education degree (P3 of Supplementary Material Table 1)



(a) **(b)**

Fig. 3 Figure **a** shows the experience length of the agile teams' practitioners (P4 of Supplementary Material Table 1), while **b** shows their workplace (P5 of Supplementary Material Table 1)

4.2 Survey results

The survey was answered by 53 ICT practitioners geographically distributed in several regions of Brazil. 5.7% of survey participants are between 21 and 30 years old, 22.6% are between 31 and 42 years old, 13.2% are between 43 and 47 years old, 15.1% are between 48 and 54 years old, 11.3% are between 55 and 60 years old, and 3.8% are over 61 years old, as shown in Fig. 2 (a). 39.6% of survey participants have a specialization degree, 28.3% are masters, 18.9% are graduated, 9.4% are Ph.D., and 3.8% of the survey participants are undergraduate students, as shown in Fig. 2 (b).

Regarding the experience length of the survey participants, 37.7% of agile teams stated to have over 21 years of experience in software development, 18.9% have between 16 and 20 years, 15.1% have between 7 and 10 years, 11.3% have between 11 and 15 years, 9.4% have between 4 and 6 years, and 7.5% of agile teams practitioners have between 1 and 3 years, as shown in Fig. 3a.

Regarding the type of organization that agile teams work in, 39.6% of them work in Federal Public Administration agencies, 32.1% work in private software development companies, 9.4% work in state-owned company, 9.4% work in research/collaboration projects, 5.7% work in State Public Administration agencies, and 3.8% work in open source software projects, as shown in Fig. 3b.

Regarding the primary function that ICT practitioners perform in a software development project, 50.9% claimed to be Programmers/Developers, 45.4% are Requirements Analysts, 43.3% are Project Managers, 37.8% are Software Engineers, 35.9% do Data Modeling, 24.7% are Software Testers, 17% are Designers, and 7.6% are Human-Computer Interaction specialists, as presented in Fig. 4a. 75.5% of the agile teams' practitioners stated that they work on the

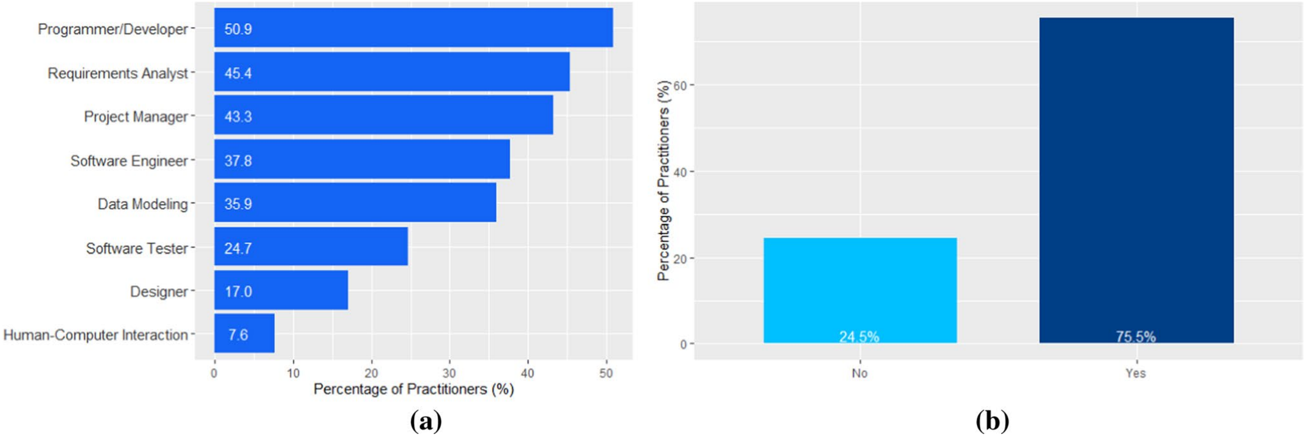


Fig. 4 Figure **a** shows the role of the agile teams' practitioners (P7 of Supplementary Material Table 1), while **b** shows the percentage of respondents that work on developing features with data privacy concerns (P8 of Supplementary Material Table 1)

development of software functionalities with data privacy concerns, as presented in Fig. 4b. This finding is interesting, because we can infer that most of the respondents are experienced in requirements elicitation and software development activities.

Summary: The results found allow us to infer that most agile team practitioners who responded to the survey possess the degree of specialist, work in Federal Public Administration agencies or private software development companies.In addition, more than 65% of the respondents have more than 11 years of experience, i.e., they are experienced practitioners in the area of software development

4.2.1 RQ.1. What practices/techniques, and tools are used by agile teams to elicit privacy requirements that comply with the Brazilian general data protection law?

To answer RQ.1, we asked the practitioners from the agile teams if the organization they work for has implemented or is implementing changes due to LGPD. 78% of these practitioners stated that the organization is implementing changes in its software development process, 16% were neutral, and 6% disagree and strongly disagree that the organization is changing its development process, as presented in P9 of Fig. 5. This finding ratifies the findings of Sakamoto et al. [35], in which the authors identified that 99% of employees in the analyzed organizations were motivated to implement LGPD in their organizational processes.

This result also shows an evolution compared to our previous work [17], which allows us to infer that this increase in changes made by the organizations, in the perception of agile teams, resulted from the need to implement measures to meet the principles of the LGPD.

In addition, we investigated whether the agile teams' practitioners have sufficient knowledge about the Brazilian General Data Protection Law (LGPD), which was implemented in 2020, to conduct their activities in the projects they are participating in. 56% of the agile teams' practitioners stated that they have enough knowledge to perform their functions, 21% were neutral, and 23% stated that they do not have the necessary knowledge to perform their functions in software development teams, as presented in P10 of Fig. 5. This finding also shows an increase of 11% from our previous study [17], which allows us to infer that the knowledge of agile teams has increased since the LGPD implementation and that the LGPD deployment has led organizations to capacitate their employees. This finding ratifies the results of Sakamoto et al. [35], who investigated developers' perceptions of LGPD concepts, and the authors identified that 86% of them claimed to know the LGPD.

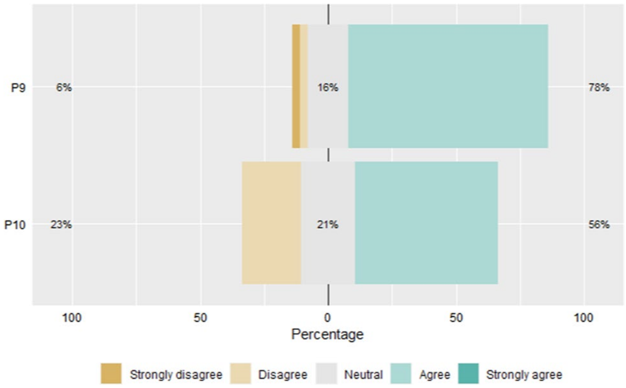


Fig. 5 Changes implemented by organizations and knowledge of the LGPD by agile teams' practitioners (P9 and P10 Supplementary Material Table 1)

Table 2 LGPD principles known by agile teams and used by organizations they work for (P11 and P12 of Supplementary Material Table 1)

LGPD principles	% Known principle	% Used principle
1. Security	81.1%	90.6%
2. Open access	67.9%	43.2%
3. Data quality	66%	54.7%
4. Prevention	66%	56.6%
5. Purpose	60.4%	56.6%
6. Transparency	60.4%	58.5%
7. Needs	56.6%	43.4%
8. Non-discrimination	56.6%	32.1%
9. Adequacy	54.7%	45.3%
10. Accountability and legal reporting	52.8%	34%

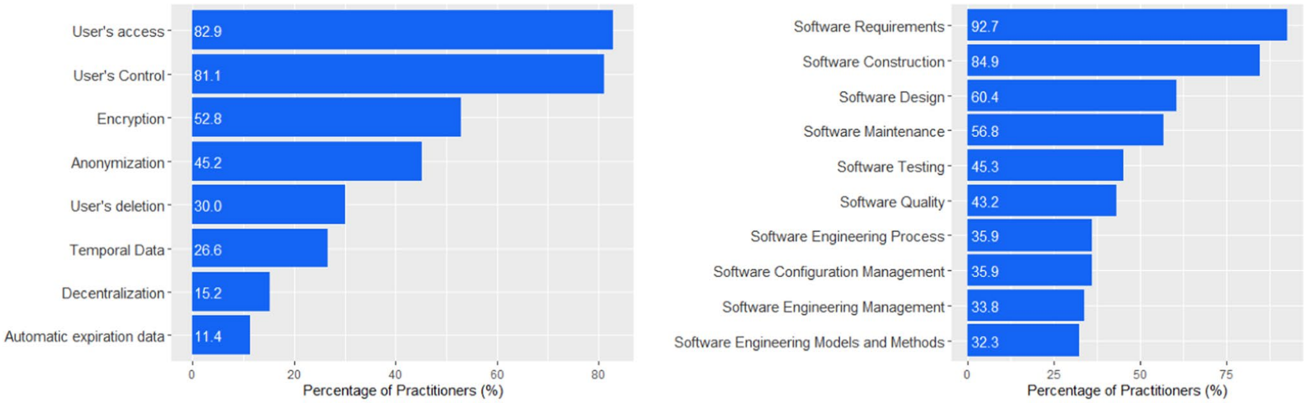
Regarding which of the General Data Protection Law principles agile teams' practitioners know and which of the LGPD principles the organization they work with uses in their agile projects, the Security principle is the most known by agile teams (81.1%) and the most used by the organizations they work with (90.6%), as presented in Table 2. In questions 11 and 12 of the Supplementary Material ("2-Survey_Questions.pdf" file) we used the 10 principles of the LGPD, with their corresponding description [84, 25].

This scenario differs from our previous results, in which the LGPD principle most known by agile teams was transparency, followed by security and needs [17]. Moreover, the Security principle is known by more than 81% of the survey participants, whereas in the previous study, it was known by only 46.2% of the participants.

The current scenario has not changed much from the previous study regarding the LGPD principles most used by the organizations where the agile teams work. The Security principle was the most used principle by organizations. Currently, the 5 LGPD principles most used by organizations are: Security (used by 90.6%), Transparency (used by 58.5%), Prevention (used by 56.6%), Purpose (used by 56.6%), and Data Quality (used by 54.7%), as presented in Table 2. Although the principles have not changed much compared to our previous study, the percentages of those principles have increased, which leads us to believe that organizations are more concerned about the LGPD principles.

Regarding which data privacy solutions the agile teams have worked on or are currently working on, 82.9% of the agile teams work with User's control, 81.1% with User's Access, 52.8% work with Encryption, 45.2% with Data Anonymization, 30% with User's Deletion, 26.6% with Temporal Data, 15.2% with Decentralization, and 11.4% of the agile teams work with Automatic Expiration Data. It can be seen in Fig. 6a that all solutions are used by the agile teams and the two most used solutions are also the same as the previous results of Canedo et al. [17, 26].

Concerning the knowledge areas of the software development process the changes proposed by the LGPD will impact (considering the knowledge areas proposed in the SWEBOK [85]), the changes proposed by the LGPD will impact the activities of the agile teams. 92.7% of the agile teams affirmed that the changes impact the knowledge area of Software Requirements, 84.9% affirmed that they impact Software Construction, 60.4% in Software Design, 56.8% in Software Maintenance, 45.3% in Software Testing, 43.2% in Software Quality, 35.9% in Software Engineering Process and Software Configuration Management, respectively. 33.8% in Software Engineering Management and 32.3% of the agile teams said it would be in the Software Engineering Models and Methods knowledge area, as presented in Fig. 6b. This finding echoes



(a) **(b)**

Fig. 6 Figure **a** shows the data privacy solutions that agile teams work with (P13 of Supplementary Material Table 1), while **b** shows which knowledge areas of the software development process will be affected by the LGPD (P14 of Supplementary Material Table 1)

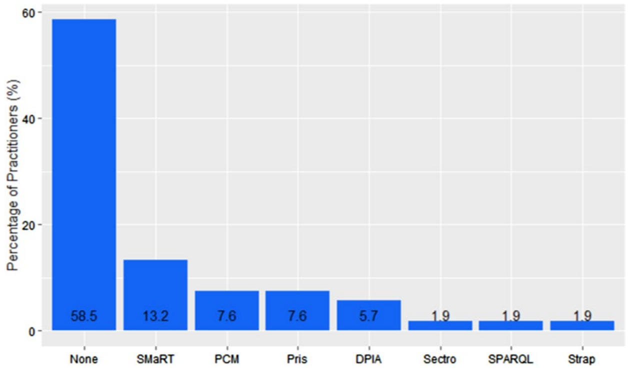


Fig. 7 Tools used by agile teams during requirements elicitation (P15 of Supplementary Material Table 1)

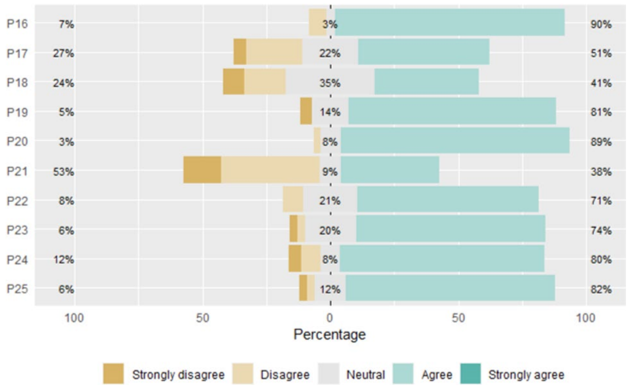


Fig. 8 Agile teams' perception regarding measures adopted by the organizations (P16 to P25 of Supplementary Material Table 1)

the findings of Canedo et al. [26], in which even before the LGPD went into effect, ICT practitioners already believed that the knowledge areas most impacted by LGPD would be Software Engineering Management and Software Construction.

58.5% practitioners stated their agile teams do not use any tool to elicit and document privacy requirements, 13.2% stated they use the SMaRT tool [86], 7.6% use PCM [41] and Pris [87], respectively. 5.7% use DPIA [88] and 1.9% of agile teams stated they use Sectro [89], SPARQL [90] and Strap [91], respectively, as presented in Fig. 7. This finding represents a misalignment between the tools proposed in the literature and their use by industry practitioners, i.e., although tools exist in the literature to support privacy requirements elicitation, they are seldom used by practitioners in the software industry.

Summary: Our findings indicate that the LGPD principles most known to agile teams are: Security, Open Access, Data Quality, Prevention, and Purpose, and the most commonly used principles within organizations are: Security, Transparency, Prevention, Purpose, and Data Quality. The most adopted solutions are User's Access, User's Control, Encryption, Anonymization, and User's Deletion. In addition, the knowledge areas most impacted by the LGPD are Software Requirements and Software Construction, and more than 50% of agile teams do not rely on any tool to elicit privacy requirements

4.2.2 RQ.2. What actions/changes have Brazilian organizations taken to develop LGPD-compliant software?

To answer RQ.2, in addition to reviewing questions asked to the agile teams' practitioners to answer RQ.1, such as the questions that generated Table 2, we asked these practitioners other questions using the Likert scale related to the actions that the organizations they work for have adopted since the Brazilian General Data Protection Law (LGPD) became effective in 2021.

Comparing our previous research's data [17] and the LGPD principles' data that composes Table 2, the knowledge about the Security principle sudden increased (81% of the survey participants know it, whereas, in the previous study, it was known by only 46.2%), along with the increase in each principles usage by the companies lead us to conjecture that although most organizations have made changes to their software development process to ensure they comply with the LGPD, they might have focused in the Security principle in comparison to the others. As 90% of the agile teams strongly agree and agree that the organizational environment interferes with data privacy practices (P16 of Fig. 8), such information corroborates with that assumption.

51% of the respondents stated that the organization they work for had informed all its employees about the LGPD and its deployment in 2021. In addition, regarding whether discussions were held with the agile teams regarding possible changes that would be required in current systems and future systems to be developed by the organization, 22% were neutral, and 27% disagree (P17 of Fig. 8).

41% of the practitioners stated that after the LGPD came into force, the way they work in organizations was changed, 35% were neutral, and 24% stated that there was no change in the way they work in organizations (P18 in Fig. 8). 81% of agile teams agreed that organizational procedures related to user data privacy should be known to all employees in the organization, including the software development team, 14% were neutral, and 5% disagreed (P19 of Fig. 8).

89% of the agile teams' practitioners agreed that the criteria used to determine which work items are critical regarding data privacy should be based on data protection objectives, 8% were neutral, and only 3% disagreed, as presented in P20 of Fig. 8. Regarding whether defining a set of privacy requirements before the requirements elicitation stage can compromise the agility of the software development process, 38% of the agile teams agreed, 9% were neutral, and 53% disagreed that defining a set of privacy requirements beforehand can compromise this process (P21 in Fig. 8).

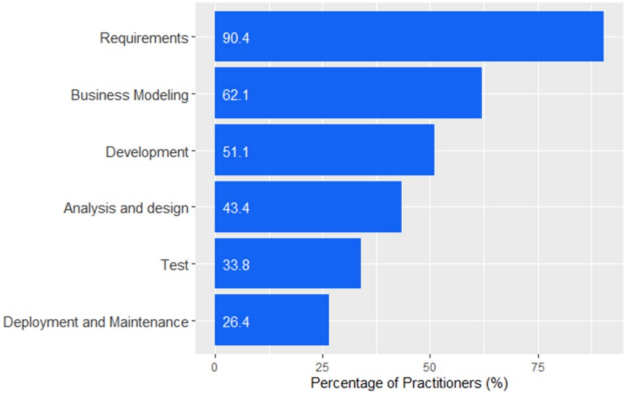


Fig. 9 Phase of software development in which privacy requirements are inserted into user stories (P26 of Supplementary Material Table 1)

71% of the respondents agreed that the data protection set initially defined by the development team should be evolved/changed throughout the software development process, 21% were neutral, and 8% disagreed (P22 in Fig. 8). 74% of the agile teams agreed that using documents from traditional methodologies, e.g., data flow diagram, architecture overview, data model, and class diagram, to identify the flow of data privacy-related information can facilitate the identification and documentation of privacy requirements. 20% were neutral, and 6% disagreed (P23 of Fig. 8).

According to 80% of practitioners, the data model or class diagram can be used to identify and document the privacy requirements of a software, 8% were neutral, and 12% disagreed (P24 in Fig. 8). 82% agreed that the specification of system privacy requirements could be done using use cases or user stories. 12% were neutral, and only 6% disagreed (P25 in Fig. 8). According to Alshammari and Simpson [92], data modelling represents relevant objects, associated properties, relationships, and constraints to specify the required data, and this representation can be used as shared knowledge by several stakeholders to identify the privacy concerns.

90.4% of the agile teams perform the privacy requirements specification using user stories in the requirements phase, 62.4% during the business modeling phase, 51.1% in the development phase, 43.4% in the analysis and design phase, 33.8% in the test phase, and 26.4% insert the data privacy aspects (purpose, adequacy, consent, documentation, accountability, among others) in the deployment and maintenance phase, as presented in Fig. 9.

Summary: Most agile teams' practitioners believe that the organizational environment interferes with data privacy practices and that the procedures adopted by the organization should be known to everyone involved with the process. Most organizations have changed their software development process to ensure compliance with LGPD. Also, most agile teams use user stories in requirements elicitation

In the survey, we also conducted some open-ended questions to comprehend the perception of agile teams regarding some aspects of the LGPD privacy principles. The first question was related to the use of user stories to specify the LGPD principles and what difficulties they might have identified when implementing LGPD data privacy principles into the agile software development process (P27 of Supplementary Material Table 1). We have highlighted some difficulties/challenges mentioned by the practitioners, as we consider them significant and as they ratify our findings:

> *"It is difficult to ensure compliance to LGPD principles using user stories since the correct specification of LGPD principles depends on the experience and engagement of the software development team."*

> *"Sometimes requirements analysts and other internal parties do not know how to specify privacy requirements, and this makes it difficult to ensure compliance with the LGPD. Most of the time, user stories do not have the necessary details to implement the user data privacy principles, and developers need to discuss the optimal way to implement them during the software development phase. As a result, user stories become outdated and useless."*

> *"User stories usually do not describe privacy requirements correctly. Many details are not correctly described, and sometimes it is necessary to implement privacy requirements according to the developer's understanding. This ends up being a problem because they must be clearly specified during the requirements elicitation phase to be implemented correctly."*

> *"Data privacy in the context of technology is a challenge. It requires a set of processes and technologies to address information protection, masking the data from being readable in its storage and subsequently being accessible only by authorized persons and with the appropriate level of security on their devices to prevent information leakage. In addition, there is also the issue of consent and the right to be forgotten, where at any time, the user can request the deletion of his data. This set of rules and requirements must be fully known by the person responsible for developing the user story because it will derive actions not only in the context of software development but also in other areas, such as information security, fraud, and auditing."*

> *"The biggest difficulty in implementing the data privacy principles is due to the lack of knowledge of the team members to perform their elicitation. Usually, we raise these requirements previously in the requirements elicitation phase, and in the implementation,*

> *they are refined with the developers. At this stage, they are updated and documented according to the developers' perception of the needs we described in the requirements specification document (in a very generic way because we have a still abstract idea of what is needed)."*

> *"Some requirements analysts fail to specify privacy requirements correctly. This reflects on the implementation since the developers need to define the requirements again and according to the perception of the development phase without contact with the stakeholders to really understand their needs."*

Most agile teams' practitioners consider that out-of-date user stories can threaten the correct implementation of privacy requirements: "Out-of-date user stories are a major threat, as is any out-of-date documentation. "During the software development process, it is important that requirements are reviewed and updated at all stages of the software development process.

These findings corroborate with Bartolini et al. [48], who investigated the use of user stories in the specification of GDPR privacy principles. The authors concluded that it is challenging to specify privacy principles using user stories since most ICT practitioners do not correctly describe user needs in them, and user stories usually become outdated during the software development phase.

As to whether specifying privacy requirements using user stories or use cases in the requirements specification phase (early design phase) is sufficient to ensure the privacy of users' data, some answers were: "Privacy requirements must be verified throughout the software life cycle, from the initial demand to its closure, and reviewed when adopting solutions that impact them". "Using user stories or use cases is sufficient as long as they are well described and represent the real needs related to user data privacy. Thus, requirements specification when done correctly is sufficient regardless of the technique used."

Regarding what other practices agile teams think can be used to implement LGPD principles, some participants mentioned: "Within sprints and agile peer development the organization should always be concerned about data security, especially because it is a law, all software must meet its requirements. In addition, all sprints must consider the LGPD principles as a premise in the user stories. Thus, it should be checked whether or not the user stories are compliant with the LGPD principles". "Apply quick checklists that are feedbacked in all development projects, seeking improvement and compliance with LGPD in all systems developed by the organization".

All 53 practitioners participating in the survey reported that the organization in which they work does not use any software or guidance to ensure compliance with the LGPD.

We also asked whether the organization they work for modified the software development process to address the privacy requirements after the LGPD came into effect, and the penalties started to be charged for non-compliance as of August 2021. We have highlighted some responses:

> *"Modifications were made in the software development methodologies (adding the requirements arising from the LGPD from the initial demand of the software until its obsolescence); in the contractual terms of the software factories (changing the terms of awareness of the new requirements and the acceptance criteria used by the internal contractual inspection team); and in the quality processes (automating vulnerability tests, consent registration, and data disposal according to the organization's data temporality standards)."*

> *"The organization has hired a data privacy expert to design a process for implementing the LGPD within the organization. The process is in the testing phase but has already shown satisfactory results."*

> *"The organization provided agile teams with training courses and changed the requirements specification phase. It became mandatory for the team to specify all privacy requirements in detail during the requirements phase."*

Summary: Most agile teams' practitioners stated that user stories do not correctly describe privacy requirements and that the teams' lack of knowledge is still a challenge to correctly identifying privacy principles. Also, outdated user stories are a threat to the software development process. None of the organizations use software or guides to ensure compliance with LGPD. The practitioners also stated that most of the organizations they work for had made changes development process to ensure LGPD compliance

4.3 Semi-structured interviews results

4.3.1 Data collection

In order to further develop the responses to RQ.2, we used interviews as our data collection procedure. According to Merriam and Tisdell [93], interviews effectively elicit information about things that cannot be observed. We used semi-structured interviews with open-ended questions because this approach gathers richer responses when compared to structured interviews. These were conducted in Portuguese since it was the main language of the interviewer and interviewees. We contacted the participants who indicated in the survey that they were interested in participating in the interview in advance, and each interview took place in a private online meeting room. The interviews were conducted remotely due to the COVID-19 pandemic.

Table 3 Characteristics of interviewees

ID	Role	Experience	Know LGPD
I1	Requirement engineer	11 years	Yes
I2	Developer	5 years	Yes
I3	Requirement engineer	3 years	Yes
I4	Requirement engineer	6 years	Yes
I5	Requirement engineer	20 years	Yes
I6	Requirement engineer	10 years	Yes
I7	Requirement engineer	13 years	Yes
I8	Requirement engineer	12 years	Yes
I9	Requirement engineer	17 years	Yes
I10	Developer	9 years	Yes

Interviewees accepted voluntarily to participate in the research. They had to agree with the Informed Consent Form, which guarantees the confidentiality of the data provided, the anonymity of the participants, and the right to withdraw from the research at any moment. We have conducted ten semi-structured interviews. All interviews were recorded and transcribed by the first two authors of this research. 3 presents the profile of the ten practitioners who participated in the semi-structured interviews. All interviewees are experienced and work as Requirement Engineers or Developers.

4.3.2 Analysis

Data analysis in qualitative research identifies the meaning of words, and coding is a way of exploring the meaning of the data by looking for similarities and differences between them to categorize and label them. Thus, after transcribing all the interviews, we followed the following phases during data analysis:

- Open Coding Data Collection: In this phase, we performed open coding on the interview transcripts, i. e., we analyzed the raw data line by line. In the end, we generated the categories and how they varied dimensionally. It is worth noting that during this phase of analysis, a constant comparison of the data was performed, during which the first two authors compared one data segment with another to determine the similarities and differences of raw data. Open coding lasted until there was no remaining concern about the study's core category. Early in the analysis, the Agile Teams category (Table 4) showed potential to be the core category and was consolidated as such, representing the end of open coding and the beginning of selective coding.

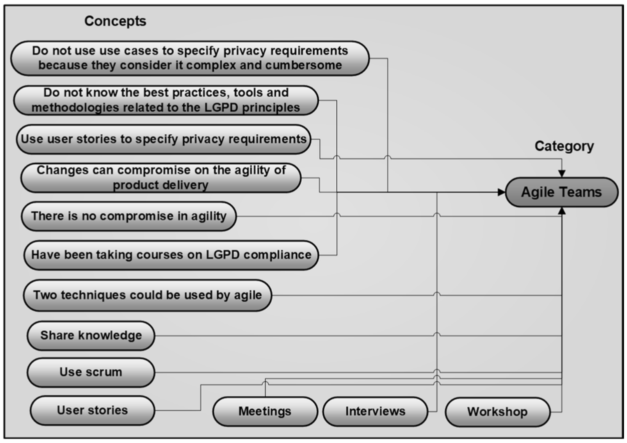

Concepts
Do not use use cases to specify privacy requirements because they consider it complex and cumbersome
Do not know the best practices, tools and methodologies related to the LGPD principles
Use user stories to specify privacy requirements
Changes can compromise on the agility of product delivery
There is no compromise in agility
Have been taking courses on LGPD compliance
Two techniques could be used by agile
Share knowledge
Use scrum
User stories
Meetings
Interviews
Workshop
Category
Agile Teams

Fig. 10 Coding: Building Categories

- Selective Coding Data Analysis: In the second phase, we evolve the initial set of categories by comparing new and previous incidents. In selective coding, only specific variables directly related to the core category are coded, aiming to produce a coherent theory. This phase identifies the core category and the subcategories related to it. Selective coding ends when we reach theoretical saturation, which occurs when the last participants have provided more evidence and examples, but no new concept or category.
- Theoretical Coding: After saturation, we build a theory that accounts for the categories and the relationships between the categories.

The constant comparison method was repeated on the concepts to produce a third level of abstraction called categories. Use user stories to specify privacy requirements as code was grouped together with twelve other concepts into the Agile teams category. Figure 10 illustrates how that abstraction of concepts become a category.

To illustrate more precisely the details of how the coding process was carried out, which resulted in the categories and subcategories related to actions/changes Brazilian organizations have taken to develop LGPD-compliant software, the following are some examples of the evolution of some interview transcript portions (raw data) up to a certain category.

The answers for question Q.4 (Supplementary Material Section 2 varied between yes and partially yes since **Raw data**: "[...] Because it is a very broad topic, we end up having to segment the knowledge and distribute within the teams the responsibility for implementing each principle of the LGPD". **Key point**: "We end up having to segment the knowledge and distribute within the teams the responsibility for implementing each principle of the LGPD. We then assigned codes to the key point. A code is a phrase that

Table 4 Consolidation of survey and interview findings

Survey	Agile teams	Are motivated to comply with the LGPD
		Use scrum
		Most of them do not use any tool to specify privacy requirements
		Use user stories to specify privacy requirements
		Have enough knowledge about the LGPD
		Are being trained by the organizations
		Validation and verification of requirements facilitates implementation of privacy requirements
		Check lists facilitate the identification of privacy requirements
		Data model and class diagram facilitates the identification of privacy requirements
	Challenges	Specify privacy requirements correctly
		Ensuring compliance to LGPD principles using user stories
		User stories outdated and incomplete
		Lack of knowledge to identify data privacy principles
		Lack of a guide or support tool to ensure compliance
		Organizational interference in data privacy practices adopted by agile teams
		Changes in the stages of the development process can compromise the agility of product delivery
	Most known and used principle	Security
	Most used solutions	User's control, user's access, and encryption
	Subjects most affected by the LGPD	Software requirements
		Software construction
		Software design
		Software maintenance
	LGPD impacts	All software development process phases

Table 4 (continued)

Interviews	Agile teams	Have been taking courses on LGPD compliance
		Do not know the best practices, tools and methodologies related to the LGPD principles
		Share knowledge
		Use scrum
		Use user stories to specify privacy requirements
		There is no compromise in agility
		Changes can compromise on the agility of product delivery
		User stories
		Meetings
		Workshop
		Interviews
		Two techniques could be used by agile
		Do not use use cases to specify privacy requirements because they consider it complex and cumbersome
	Challenges	It is difficult to identify privacy requirements
		Lack of process to automate data privacy
		Lack of standardization for classifying sensitive information
		Lack of interaction between the agile teams and the stakeholders
		Lack of a security policy
		Lack of a data privacy policy
		Lack of standardization of techniques and tools for eliciting privacy requirements
		The organization's business processes are not mapped
		Lack of investment in solutions to ensure LGPD compliance
	Most used principles	Security
		Prevention
		Purpose
		Transparency
		Data quality
	Most worked on principles	Security
		Transparency
		Data quality
	LGPD impacts	All software development process phases

summarizes the key point and one key point can lead to several codes". **Code**: Have been taking courses on LGPD compliance. **Code**: Agile Teams. **Raw data**: "It is very difficult for someone to be technically aware of all the best practices, tools and methodologies related to the LGPD principles". **Code**: Do not know the best practices, tools and methodologies related to the LGPD principles. **Code**: Agile Teams. This statement is interesting as it highlights that the implementation of the LGPD has increased the teams' knowledge compared to our previous work [15]. Also, the knowledge of the law principles is distributed among the team members, which is a characteristic of teams working with agile methodologies.

I4 states that (**Raw data**): “all the agile teams in the organization took the LGPD course at the National School of Public Administration (Enap)[1] during working hours”. **Code**: All the agile teams in the organization took the LGPD course. **Code**: Agile Teams. The full codebook is available in the Supplementary Material “6-Perceptions of interviewees-coding.xlsx” file.

Interviewees’ organizations vary between public and private companies. According to them, organizations active in private software development are guiding and implementing LGPD compliance solutions in conjunction with stakeholders and users, according to best practices to ensure compliance with the LGPD guidelines. Interviewee 3 (I3) reported that “My organization has implemented the following changes: the LGPD is being treated as an improvement program, addressing the following aspects: 1) Creation of a privacy office with an eligible Data Protection Officer; 2) Mapping of all information classified as sensitive, according to the LGPD; 3) Implementation of the Discovery process in all the organization’s systems; 4) Creation of a consent management for browsing on digital platforms; 5) Creation of a ‘Right to be forgotten’ management for the information stored by the organization”.

The LGPD principles most used by organizations (Q.5 of Supplementary Material Section 2) from respondents are Security, Prevention, Purpose, Transparency, and Data quality. This finding ratifies and complements our previous work [15]. It also ratifies the survey results presented in Table 2. Regarding Q.6 (of Supplementary Material Section 2), most respondents are working with security, transparency, and data quality.

Regarding the privacy solutions currently used (Q.7 of Supplementary Material Section 2), the following were mentioned: Sailpoint, Identity Governance and Administration, Customer Identity and Access Management, Identity IQ, Privacy by Securiti.ai, Ping, and Cyberark.

All the interviewees stated that the LGPD impacts all phases of the software development process (Q.8 of Supplementary Material Section 2). I8 mentioned that “The LGPD is impacting the entire software development process adopted by the organization, from requirements elicitation, design, development, testing, and maintenance. The team started interacting with those responsible for different activities, for example, the requirements analysts need to interact with the developers to jointly seek the best way to ensure the privacy of the software users’ data”.

All interviewees stated that their team uses user stories to specify and document privacy requirements (Q.9 of Supplementary Material Section 2). I5 mentioned that: “we use user stories in privacy requirements elicitation. With the LGPD, we are adding the information regarding user data that should be anonymized.”

The answers were divergent regarding whether defining a set of privacy requirements before the requirements elicitation stage can compromise the agility of the software development process (Q.10 of Supplementary Material Section 2). Some respondents stated that it does (6 respondents), I10 stated that “any change in the development process steps can compromise on the agility of product delivery. However, if the set of requirements is well defined and implemented, the product delivery time can be maintained”. 4 interviewees informed that it does not: “[...] there is no compromise in agility, as long as this set of requirements has been previously validated and approved by stakeholders and users. In addition, this set of requirements also needs to be associated with a normative or organizational policy of security and data privacy.”

Regarding the procedures adopted by software development teams in privacy requirements elicitation (Q.11 of Supplementary Material Section 2), the interviewees mentioned: 1) definition of data privacy and security needs to be automated or modified; 2) holding weekly meetings with stakeholders and users during the specification of all software privacy and security requirements; 3) modeling of all business processes, containing the improvements identified and discussed among stakeholders and users; 4) implementation of privacy and security requirements, as well as their respective business rules, use cases, and user stories; and 5) execution of user tests of the implemented privacy and security requirements. Furthermore, I2 mentioned that “the techniques and tools for performing privacy requirements elicitation are defined according to the team’s knowledge. Since all the agile teams in the organization know user stories, there is not much discussion regarding which technique to use; we always opt to use user stories.”

The interviewees’ answers were divergent regarding whether the specification of the privacy requirements of software can be performed using use cases or user stories (Q.12 of Supplementary Material Section 2). I1 stated that “from now on this scenario tends to change, where use cases and user stories should start to contemplate privacy issues, I think either of the two could be used by agile teams effectively”. I6 stated that “in my opinion user stories are more suitable for privacy requirements elicitation than use cases because they are more agile and easier to change throughout the development process. Use cases are more complex and can cause more rework. I7 stated that “when we use user stories in conjunction with business process mapping, we can identify all the privacy requirements. Also, when questions arise, we hold meetings with stakeholders and users to understand the requirements better. This has generated a high degree of satisfaction with the data privacy needs of the software users. I9 said that “it does not matter if we use use use cases or user stories, what we need to do is to identify

[1] https://www.enap.gov.br/en/courses.

all the privacy requirements correctly and document them clearly and objectively, so that all the developers on the team can implement them without any mistakes".

The following challenges for privacy requirements elicitation were mentioned (Q.13 of Supplementary Material Section 2): 1) It is difficult to get all stakeholders involved; 2) Most organizations do not have their business processes mapped; 3) The organization does not have professionals qualified in terms of the LGPD; 4) Organizations are not investing in software solutions to ensure LGPD compliance; 5) It is not easy to align business needs with the LGPD without creating new processes or work demands; 5) Agility in defining requirements and their implementation. These results allow us to infer that some of the challenges mentioned in privacy requirements elicitation continue to be similar to the challenges already reported in the literature for eliciting requirements [44, 59], i.e., they are challenges that permeate Requirements Engineering, regardless of the development methodology adopted (Agile or traditional). I7 mentioned that "in organizations that already have a legacy system, where the demands are usually always associated with this legacy or old practices, the biggest challenge is the culture change".

Summary: The interviews' results do not deviate much from the survey findings, wherein the interviewees' perception, all disciplines of the software development process are impacted by the LGPD, and practitioners use user stories in privacy requirements elicitation. Also, organizations are educating agile teams on the LGPD

4.4 Summary of results

Most of the agile teams participating in both the survey and the interviews utilize the Scrum methodology in the software development process. According to the results, it is possible to perceive that there has been an increase in the understanding and knowledge regarding the principles of the LGPD as compared to previous studies [17, 20]. This change in the perception of agile teams is perceptible through the following statements: 1) agile teams have enough knowledge about the LGPD; 2) knowledge about the LGPD principles has increased substantially since the last survey, although their implementation has increased marginally; 3) agile teams are being trained by their organizations concerning the LGPD, which allows us to infer that this training is related to having enough knowledge about the LGPD and its principles.

Regarding the challenges faced by agile teams, according to the survey and interviews findings, there is a lack of standardization in the choice of techniques and tools to support privacy requirements elicitation. This finding ratifies the results of the survey conducted by Alhazmi et al. [36]. In the survey, common challenges to agile software development were identified according to previous studies [96, 97], such as: specifying requirements correctly, incomplete user stories, and that changes in process steps can compromise agility.

In the interviews, some challenges were mentioned, also related to agile software development [96, 97], such as: a) lack of interaction between the agile teams and stakeholders; b) lack of organization's business process mapping; c) lack of a security and data privacy policy; and d) lack of investments in software solutions to ensure compliance with the LGPD. This allows us to infer that organizations have trained their employees but need to further develop actions to mitigate these challenges. These findings ratify and complement the findings of Canedo et al. These findings ratify and complement the findings of Canedo et al. [17]. Table 4 presents the consolidated results of the survey and interviews after data analysis.

5 Limitations and threats to validity

This section discusses the limitations and threats to validity concerning our systematic literature review, interviews, and survey's planning, design, and execution. We adopted the approach presented by Wohlin et al. [98].

5.1 Construct validity

Construct validity refers to the decisions on methods and tools and whether they are appropriate for the research questions. We utilized the manual and automatic search strategy. The risk is that if the selection criteria set for the systematic literature review (SLR) are insufficient, some papers will not be found when SLR. However, we cannot guarantee that all primary studies related to privacy requirements elicitation in the context of agile software development have been selected in the execution of the systematic literature review, or even if journals or conferences with a good impact factor or studies with a good number of citations were prioritized. To mitigate this threat, three researchers conducted searches on the established digital databases. Furthermore, based on our experience, we believe we have included several key papers on empirical evidence on privacy requirements elicitation. Hence, we believe that most of the included papers come from the search string, indicating that we have likely found the majority of all relevant papers. This implies that our method selection was appropriate.

The quality of the questions and answers is key to ensuring that a survey measures what it intends to measure. We have taken several steps to reduce this threat. First, we reused questions and answer options from a previously published survey [17] for the demographic questions. Second, we have performed a pilot with five practitioners from the industry. To evaluate the instrument's understandability, pilot participants answered the questionnaire by themselves without any mentoring.

Our research is an exploratory study conducted through an online survey. Thus, we tried to reduce the number of open-ended questions since they spend more of the practitioners' time, which may cause more withdrawal. Thus, we decided to put fewer open-ended questions in the survey. Another aspect is that practitioners may use different techniques or tools simultaneously to elicit privacy requirements, either in different projects or in the same project. Thus, we designed some multiple-choice questions to reflect all the current practices. We focus this study on finding out which LGPD principles practitioners currently know and work on, and which challenges practitioners perceive when eliciting privacy requirements.

Although Grounded Theory offers defined procedures for data analysis, our qualitative research may contain some research bias. Indeed, other researchers might find a different interpretation after analyzing the same data, but we believe that the main perceptions would be preserved. This is a specific threat related to GT studies, which do not claim to generate definitive findings. For this reason, we do not claim that our findings are absolute or final.

5.2 External validity

This survey's findings cannot claim to cover the perception of the whole population of practitioners working in agile software development (ASD). First, it is unclear what would be the extension of such a population. Second, sampling by convenience is likely to attract more motivated people, which could not represent the whole population [99]. The personal interest in the LGPD, agile teams, and privacy requirements elicitation topics related to our survey, might have influenced the decision of the practitioners to participate. Finally, our decision of sampling by convenience to target expert practitioners resulted in a small sample size (n = 53). However, our study provided interesting findings that help draw an initial characterization of the changes in organizational processes and software development processes to ensure compliance with LGPD. We gathered participants with varying roles, without any dominant category of practitioners. Although a homogeneous sample could lead to a better characterization of a specific group, a heterogeneous sample provides richer information to portray the state of the practice. Finally, the replication of the survey is easy and feasible. So, future replications of this study may expand the sample and allow for a deep analysis of this scenario.

A noteworthy limitation of this research is that we evaluated agile teams' perceptions regarding Brazilian organizations' actions to ensure LGPD compliance. However, we have not verified in practice whether all organizations have effectively implemented changes in the software development processes they adopt. We have no means to ensure that the assessed organizations reflect all Brazilian companies within this study scenario since the control authorities have not yet published a list of Brazilian organizations developing software in compliance with LGPD. Nonetheless, this research focuses on agile teams' perceptions rather than direct observations.

5.3 Internal validity

The selection of participants and how to treat their answers may affect the internal validity of this survey. To avoid responses from people outside the expected profile, we clearly explained the desired profile on the survey. We also included surveys questions about the experience with agile software development. The participants' general profile comprises practitioners with considerable expertise in ASD. Regarding the experience in the privacy requirements elicitation activities, our sample is very balanced toward people that work more frequently in agile teams software development with data privacy concerns.

Another threat is that the semi-structured interviews were conducted by two of the co-authors of this paper, which may have induced the interviewees' responses. To mitigate this threat, the fourth and fifth authors analyzed the results obtained so that there was no bias regarding the conclusion of the interviewee's perception. In addition, we interviewed a small number of practitioners, which could be a threat to validity, although we gave preference to practitioners who stated that they perform the role of Requirement Engineer, had at least three years of experience in that role, and were familiar with the LGPD.

6 Conclusions

This paper investigated the perception of agile teams regarding the actions Brazilian organizations are implementing to develop LGPD compliant software. We updated the systematic literature review conducted in our previous study [17] and conducted a survey with agile teams' practitioners from several Brazilian organizations to understand their perception regarding the organizational actions adopted due to LGPD.

To complement the information obtained, we also conducted semi-structured interviews with ten experienced practitioners. Our findings reveal that agile teams' knowledge of the LGPD, compared to previous studies [17, 26], has increased substantially regarding every principle, with a mean increase of 32.23% being as high as a 50.8% increase regarding the Data Quality principle knowledge, and as low as a 7.9% increase regarding the Transparency principle; and every participant knows at least one principle (median = 6 principles known; mean = 6.22; stdev = 3.42). Moreover, the comparison between our previous study regarding the principles' implementation had a slight mean increase of 11.87%; and every participant's organization also implements at least one LGPD principle (median = 5 principles implemented; mean = 5.15; stdev = 2.85). Furthermore, there is a mutual agreement among the agile teams that the LGPD impacts all phases of the software development process.

The use of user stories in conjunction with process modeling may show a more effective result in requirements elicitation. Nevertheless, agile teams still face some challenges in requirement elicitation, such as difficulty aligning business needs with the LGPD without creating new processes or work demands, lack of specialized qualification of practitioners, and lack of software solutions to support LGPD compliance. The five principles most known by agile teams are Security, Open Access, Data Quality, Prevention, and Purpose, and the five principles most implemented by organizations after the sanction of penalties imposed by LGPD are Security, Transparency, Prevention, Purpose, and Data Quality. This result allows us to conclude that the larger-scale implementation of these principles is due to the legal demands regarding the assurance of data privacy and the purpose of user data storage by organizations.

An important finding is that agile teams stated that most organizations are making changes to their organizational processes and software development process to ensure compliance with LGPD. Also, practitioners are being trained on the LGPD, and the software requirements and software construction areas of knowledge are the most impacted by the law. On the other hand, an alarming finding is that most agile teams do not use any tool to support privacy requirements elicitation.

As future work, we intend to conduct a controlled experiment in an organization to understand how the actions adopted by it are impacting the software development process. In addition, we will perform a diagnosis of the adopted practices to verify the degree of compliance with LGPD.

Data Availability The data that support the findings of this study are openly available in Zenodo at https://zenodo.org/record/6989476.

Declarations

Conflicts of Interest The authors declare no conflict of interest.

References

1. Regulation GDP (2018) Eu data protection rules. Eur Commission, Accessed in Oct 9, 2019. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2. da República P (2018) Lei geral de proteção de dados pessoais (lgpd). Secretaria-Geral, Accessed in Oct 9, 2019. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
3. Kalloniatis C, Kavakli E, Gritzalis S (2009) Methods for designing privacy aware information systems: a review. In: Panhellenic conference on informatics, pp 185–194. IEEE computer society
4. Thomas K, Bandara AK, Price BA, Nuseibeh B (2014) Distilling privacy requirements for mobile applications. In: 36th international conference on software engineering, ICSE '14, Hyderabad, India - May 31 - Jun 07, 2014, pp 871–882. https://doi.org/10.1145/2568225.2568240
5. Hadar I, Hasson T, Ayalon O, Toch E, Birnhack M, Sherman S, Balissa A (2018) Privacy by designers: software developers' privacy mindset. Empir Softw Eng 23(1):259–289. https://doi.org/10.1007/s10664-017-9517-1
6. Balebako R, Marsh A, Lin J, Hong J, Cranor L (2014) The privacy and security behaviors of smartphone. In: Workshop on usable security (USEC 2014), San Diego, 2014
7. Skinner G, Chang E (2005) Pp-sdlc the privacy protecting systems development life cycle. Proceedings of the IPSI-2005 France
8. Patil S, Kobsa A (2004) Preserving privacy in awareness systems. In: Wissen in Aktion, pp 119–130
9. Christel MG, Kang KC (1992) Issues in requirements elicitation. Technical report CMU/SEI-92-TR-012 – carnegie mellon university pittsburgh Pa software engineering institute. https://apps.dtic.mil/sti/pdfs/ADA258932.pdf
10. Pacheco CL, García IA, Reyes M (2018) Requirements elicitation techniques: a systematic literature review based on the maturity of the techniques. IET Softw. 12(4):365–378
11. Rzepka WE (1989) A requirements engineering testbed: concept, status and first results. In: Proceedings of the twenty-second annual hawaii international conference on system sciences. Volume II: software track, vol. 2, pp 339–340. IEEE computer society
12. De Lucia A, Qusef A (2010) Requirements engineering in agile software development. J Emerg Technol Web Intell 2(3):212–220
13. Ramesh B, Cao L, Baskerville R (2010) Agile requirements engineering practices and challenges: an empirical study. Inf Syst J 20(5):449–480
14. Younas M, Jawawi D, Ghani I, Kazmi R (2017) Non-functional requirements elicitation guideline for agile methods. J Telecommun Electron Comput Eng (JTEC) 9(3–4):137–142
15. ...Wagner S, Fernández DM, Felderer M, Vetrò A, Kalinowski M, Wieringa RJ, Pfahl D, Conte T, Christiansson M, Greer D, Lassenius C, Männistö T, Nayebi M, Oivo M, Penzenstadler B, Prikladnicki R, Ruhe G, Schekelmann A, Sen S, Spínola RO, Tuzcu A, de la Vara JL, Winkler D (2019) Status quo in requirements engineering: a theory and a global family of surveys. ACM Trans Softw Eng Method 28(2):9:1-9:48
16. Li ZS, Werner C, Ernst NA, Damian DE (2020) GDPR compliance in the context of continuous integration. CoRR arXiv:2002.06830
17. Canedo ED, Calazans ATS, Cerqueira AJ, Costa PHT, Masson ETS (2021) Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil. In: 29th IEEE international requirements engineering conference, RE 2021, Notre Dame, IN, USA, September 20-24, 2021, pp 58–69. IEEE. https://doi.org/10.1109/RE51729.2021.00013
18. Experian S (2020) Pesquisa lgpd (lei geral de proteção a dados). Serasaexperian pp 01–16. https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf
19. cão Nacional dos Profissionais de Privacidade de Dados AA (2021) Panorama de conscientização nacional sobre a lgpd 2021. Associação Nacional dos Profissionais de Privacidade de Dados pp 01–15. https://www.convergenciadigital.com.br/doc/21/cnppd2021_luizlima.pdf

20. Canedo ED, Calazans ATS, Cerqueira AJ, Costa PHT, Masson ETS (2020) Using the design thinking empathy phase as a facilitator in privacy requirements elicitation. In: AMCIS. association for information systems
21. Ferrão SÉR, Carvalho AP, Canedo ED, Mota APB, Costa PHT, Cerqueira AJ (2021) Diagnostic of data processing by brazilian organizations - a low compliance issue. Information 12(4):168
22. Canedo ED, Cerqueira AJ, Gravina RM, Ribeiro VC, Camões R, dos Reis VE, de Mendonça FLL, de Sousa Jr. RT (2021) Proposal of an implementation process for the brazilian general data protection law (LGPD). In: J. Filipe, M. Smialek, A. Brodsky, S. Hammoudi (eds.) Proceedings of the 23rd International Conference on Enterprise Information Systems, ICEIS 2021, Online Streaming, April 26-28, 2021, Scitepress, Vol 1, pp 19–30. https://doi.org/10.5220/0010398200190030
23. ISO B (2011) Iec 29100, 2011. bs iso/iec29100: Information technology—security techniques—privacy framework. Tech rep, Technical report, British Standard and the International Organization
24. Ayala-Rivera V, Pasquale L (2018) The grace period has ended: an approach to operationalize GDPR requirements. In: RE, pp 136–146. IEEE computer society
25. OneTrust D (2019) Comparing privacy laws: Gdpr versus lgpd. DataGuidance by OneTrust, Accessed in October 9, 2019. https://www.dataguidance.com/comparing-privacy-laws-gdpr-v-lgpd/
26. Canedo ED, Calazans ATS, Masson ETS, Costa PHT, Lima F (2020) Perceptions of ICT practitioners regarding software privacy. Entropy 22(4):429
27. Otto PN, Antón AI (2007) Addressing legal requirements in requirements engineering. In: 15th IEEE international requirements engineering conference, RE 2007, Oct 15-19th, 2007, New Delhi, India, pp 5–14. https://doi.org/10.1109/RE.2007.65
28. Bednar K, Spiekermann S, Langheinrich M (2019) Engineering privacy by design: are engineers ready to live up to the challenge? Inf Soc 35(3):122–142. https://doi.org/10.1080/01972243.2019.1583296
29. Martins ADF, da Silva Barros PV, Monteiro JM, de Castro Machado J (2020) LGPD: a formal concept analysis and its evaluation. In: Anais do XXXV Simpósio Brasileiro de Bancos de Dados, SBBD 2020, online, Sep 28 - -Oct 1, 2020, pp 259–264. SBC. https://doi.org/10.5753/sbbd.2020.13651
30. Bax MP, Barbosa JLS (2020) Proposta de mecanismo de consentimento na lei geral de proteção a dados - LGPD (consent mechanism proposal in LGPD). In: da Silva Lemos DL, Sales TP, Campos MLM, Fiorini SR (eds), Proceedings of the XIII seminar on ontology research in Brazil and IV doctoral and masters consortium on ontologies (ONTOBRAS 2020), Vitória, Brazil, Nov 23-26, 2020, CEUR workshop proceedings, vol 2728, pp. 316–321. CEUR-WS.org. http://ceur-ws.org/Vol-2728/doctorate4.pdf
31. Araújo E, Vilela J, Silva C, Alves C (2021) Are my business process models compliant with lgpd? the LGPD4BP method to evaluate and to model LGPD aware business processes. In: Araujo RD, Dorça FA, de Araujo RM, Siqueira SWM, Fontão AL (eds.), SBSI 2021: XVII Brazilian Symposium on Information Systems, Uberlândia, Brazil, June 7 - 10, 2021, pp. 46:1–46:9. ACM. https://doi.org/10.1145/3466933.3466982
32. Ribeiro RC, Canedo ED (2020) Using MCDA for selecting criteria of LGPD compliant personal data security. In: Eom S, Lee J (eds) dg.o20: The 21st annual international conference on digital government research, Seoul, Republic of Korea, June 15–19. ACM, pp 175–184 https://doi.org/10.1145/3396956.3398252
33. Mendes J, Viana D, Rivero L (2021) Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the brazilian general data protection law: An initial proposal. In: Vasconcellos CD, Roggia KG, Collere V, Bousfield P (eds), SBES '21: 35th Brazilian symposium on software engineering, Joinville, Santa Catarina, Brazil, 27 Sept 2021 - 1 Oct 2021, pp 263–268. ACM https://doi.org/10.1145/3474624.3477069
34. Muncinelli G, de Lima E, Deschamps F, da Costa S, Cestari JMAP (2020) Components of the preliminary conceptual model for process capability in lgpd (brazilian data protection regulation) context. In: Pokojski J, et al. (ed), T.E. for complex socio-technical systems – real-life applications. computer science https://doi.org/10.3233/ATDE200125
35. Sakamoto LS, Alves D, Abe JM, de Souza JS, de Souza, NA, Martinez AAG (2021) Software optimization for LGPD compliance using paraconsistent evidential annotated logic $e\tau$. In: Watróbski J, Salabun W, Toro C, Zanni-Merk C, Howlett RJ, Jain LC (eds), Knowledge-based and intelligent information & engineering systems: proceedings of the 25th international conference KES-2021, virtual event / Szczecin, Poland, 8-10 September 2021, Procedia Computer Science, vol 192, pp 3049–3059. Elsevier. https://doi.org/10.1016/j.procs.2021.09.077
36. Alhazmi A, Arachchilage NAG (2021) I'm all ears! listening to software developers on putting GDPR principles into software development practice. Pers Ubiquitous Comput 25(5):879–892. https://doi.org/10.1007/s00779-021-01544-1
37. Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Q. 35(4): 989–1015. http://misq.org/catalog/product/view/id/1518/s/information-privacy-research-an-interdisciplinary-review/
38. Kalloniatis C, Kavakli E, Gritzalis S (2008) Addressing privacy requirements in system design: the pris method. Requir Eng 13(3):241–255. https://doi.org/10.1007/s00766-008-0067-3
39. Gurses S, del Álamo JM (2016) Privacy engineering: Shaping an emerging field of research and practice. IEEE Secur Privacy 14(2):40–46. https://doi.org/10.1109/MSP.2016.37
40. Dennedy MF, Fox J, Finneran T (2014) The privace engineer's manifest. Apress open, New York
41. Peixoto M, Silva C, Lima R, Araújo J, Gorschek T, Silva J (2019) Pcm tool: privacy requirements specification in agile software development. In: Anais Estendidos da X Conferência Brasileira de Software: Teoria e Prática, pp 108–113. SBC
42. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W (2011) A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir Eng 16(1):3–32. https://doi.org/10.1007/s00766-010-0115-7
43. Islam S, Mouratidis H, Kalloniatis C, Hudic A, Zechner L (2012) Model based process to support security and privacy requirements engineering. IJSSE 3(3):1–22. https://doi.org/10.4018/jsse.2012070101
44. Tsilionis K, Maene J, Heng S, Wautelet Y, Poelmans S (2021) Conceptual modeling versus user story mapping: Which is the best approach to agile requirements engineering? In: Cherfi SS, Perini A, Nurcan S (eds) Research challenges in information science - 15th international conference, RCIS 2021, limassol, Cyprus, May 11–14, 2021, proceedings lecture notes in business information processing, vol 415. Springer, New york, pp 356–373
45. Lin J, Yu H, Shen Z, Miao C (2014) Using goal net to model user stories in agile software development. In: SNPD, pp 1–6. IEEE computer society
46. Lucassen G, Dalpiaz F, van der Werf JMEM, Brinkkemper S (2016) The use and effectiveness of user stories in practice. In: REFSQ, lecture notes in computer science, vol 9619, pp 205–222. Springer
47. Lombriser P, Dalpiaz F, Lucassen G, Brinkkemper S (2016) Gamified requirements engineering: model and experimentation. In: REFSQ, lecture notes in computer science, vol 9619, pp 171–187. Springer

48. Bartolini C, Daoudagh S, Lenzini G, Marchetti E (2019) Gdpr-based user stories in the access control perspective. In: Quality of information and communications technology - 12th international conference, QUATIC 2019, ciudad real, spain, September 11-13, 2019, Proceedings, pp. 3–17. https://doi.org/10.1007/978-3-030-29238-6_1
49. Rygge H, Jøsang A (2018) Threat poker: solving security and privacy threats in agile software development. In: NordSec, lecture notes in computer science, vol 11252, pp 468–483. Springer
50. Kitchenham BA, Brereton P, Turner M, Niazi M, Linkman SG, Pretorius R, Budgen D (2010) Refining the systematic literature review process - two participant-observer case studies. Empir Softw Eng 15(6):618–653
51. Wilson V (2014) Research methods: triangulation. Evid Lib Inform Pract 9(1):74–75
52. Flick U (2018) An introduction to qualitative research. Sage Publications Limited, Beverley Hills, CA
53. Kvale S (1995) The social construction of validity. Qualit Inquiry 1(1):19–40
54. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Department of computer science University of Durham Durham, UK
55. Peixoto MM (2020) Privacy requirements engineering in agile software development: a specification method. In: REFSQ workshops, CEUR workshop proceedings, vol 2584. CEUR-WS.org
56. Curcio K, Navarro T, Malucelli A, Reinehr SS (2018) Requirements engineering: a systematic mapping study in agile software development. J Syst Softw 139:32–50
57. Zamudio L, Aguilar JA, Barba CT, Misra S (2017) A requirements engineering techniques review in agile software development methods. In: ICCSA (5), lecture notes in computer science, vol 10408, pp 683–698. Springer
58. Viitaniemi M (2017) Privacy by design in agile software development. Master's thesis, master's degree programme in information technology, Tampere University of Technology
59. Loser K, Degeling M (2014) Security and privacy as hygiene factors of developer behavior in small and agile teams. In: HCC, IFIP advances in information and communication technology, vol 431, pp 255–265. Springer
60. Wagner TJ, Ford TC (2020) Metrics to meet security & privacy requirements with agile software development methods in a regulated environment. In: International conference on computing, networking and communications, ICNC 2020, Big Island, HI, USA, Feb 17-20, 2020, pp 17–23. https://doi.org/10.1109/ICNC47757.2020.9049681
61. Calazans ATS, Cerqueira AJ, Canedo ED (2020) Empathy and criativity in privacy requirements elicitation: systematic literature review. In: WER. Editora PUC-Rio
62. Oliver I (2016) Experiences in the development and usage of a privacy requirements framework. In: 24th IEEE international requirements engineering conference, RE 2016, Beijing, China, September 12-16, 2016, pp 293–302. https://doi.org/10.1109/RE.2016.59
63. Katsuno Y, Kundu A, Das KK, Takahashi H, Schloss R, Dey P, Mohania MK (2016) Security, compliance, and agile deployment of personal identifiable information solutions on a public cloud. In: 9th IEEE international conference on cloud computing, CLOUD 2016, San Francisco, CA, USA, June 27 - July 2, 2016, pp 359–366. https://doi.org/10.1109/CLOUD.2016.0055
64. Galvez R, Gurses S (2018) The odyssey: modeling privacy threats in a brave new world. In: 2018 IEEE European symposium on security and privacy workshops, EuroS &P workshops 2018, London, United Kingdom, April 23-27, 2018, pp 87–94. https://doi.org/10.1109/EuroSPW.2018.00018
65. Rindell K, Hyrynsalmi S, Leppänen V (2018) Aligning security objectives with agile software development. In: Proceedings of the 19th international conference on agile software development, XP 2019, companion, Porto, Portugal, May 21-25, 2018, pp. 3:1–3:9. https://doi.org/10.1145/3234152.3234187
66. van der Heijden A, Broasca C, Serebrenik A (2018) An empirical perspective on security challenges in large-scale agile software development. In: Proceedings of the 12th ACM/IEEE international symposium on empirical software engineering and measurement, ESEM 2018, Oulu, Finland, October 11-12, 2018, pp 45:1–45:4. https://doi.org/10.1145/3239235.3267426
67. Maier P, Ma Z, Bloem R (2017) Towards a secure SCRUM process for agile web application development. In: Proceedings of the 12th international conference on availability, reliability and security, Reggio Calabria, Italy, Aug 29 - Sep 01, 2017, pp 73:1–73:8. https://doi.org/10.1145/3098954.3103171
68. Netto D, Silva C, Araújo J (2019) Identifying how the brazilian software industry specifies legal requirements. In: Proceedings of the XXXIII Brazilian symposium on software engineering, SBES 2019, Salvador, Brazil, Sep 23-27, 2019, pp 181–186. https://doi.org/10.1145/3350768.3352730
69. Newton N, Anslow C, Drechsler A (2019) Information security in agile software development projects: a critical success factor perspective. In: ECIS
70. Tøndel IA, Cruzes DS, Jaatun MG, Rindell K (2019) The security intention meeting series as a way to increase visibility of software security decisions in agile development projects. In: ARES, pp 59:1–59:8. ACM
71. Ionita D, van der Velden C, Ikkink HK, Neven E, Daneva M, Kuipers M (2019) Towards risk-driven security requirements management in agile software development. In: CAiSE forum, lecture notes in business information processing, vol 350, pp 133–144. Springer
72. Tøndel IA, Jaatun MG, Cruzes DS, Williams L (2019) Collaborative security risk estimation in agile software development. Inf Comput Secur 27(4):508–535
73. Bernsmed K, Jaatun MG (2019) Threat modelling and agile software development: Identified practice in four norwegian organisations. In: Cyber Security, pp 1–8. IEEE
74. Pessoa CR, Nunes BC, de Oliveira C, Marques ME (2021) Effects and projections of the brazilian general data protection law (lgpd) application and the role of the dpo. In: Digital transformation and challenges to data security and privacy, pp 195–208. IGI Global. https://doi.org/10.4018/978-1-7998-4201-9.ch011
75. Palhares F (2021) Brazil's data protection law: Putting brazil on the map of data privacy frameworks. In: Digital transformation and challenges to data security and privacy, pp 98–118. IGI Global, https://doi.org/10.4018/978-1-7998-4201-9.ch006
76. Silva J, Calegari N, Gomes E (2019) After brazil's general data protection law: Authorization in decentralized web applications. In: Amer-Yahia S, Mahdian M, Goel A, Houben G, Lerman K, McAuley JJ, Baeza-Yates R, Zia L (eds), Companion of The 2019 World Wide Web Conference, WWW 2019, San Francisco, CA, USA, May 13-17, 2019, pp 819–822. ACM. https://doi.org/10.1145/3308560.3316461
77. Allen IE, Seaman CA (2007) Likert scales and data analyses. Qual Prog 40(7):64–65
78. Glaser BG, Strauss AL, Strutzel E (1968) The discovery of grounded theory; strategies for qualitative research. Nursing Res 17(4):364
79. Coleman G, O'Connor R (2007) Using grounded theory to understand software process improvement: a study of irish software product companies. Inf Softw Technol 49(6):654–667
80. Luz WP, Pinto G, Bonifácio R (2018) Building a collaborative culture: a grounded theory of well succeeded devops adoption in

practice. In: ESEM, pp 6:1–6:10. ACM. https://doi.org/10.1145/3239235.3240299

81. Adolph S, Hall W, Kruchten P (2011) Using grounded theory to study the experience of software development. Empir Softw Eng 16(4):487–513
82. GLASER B (2002) Constructivist grounded theory? forum: qualitative social research. On line J 3(3)
83. Stol K, Ralph P, Fitzgerald B (2016) Grounded theory in software engineering research: a critical review and guidelines. In: ICSE, pp 120–131. ACM
84. Macedo PN (2018) Brazilian general data protection law (lgpd). Nartional congress, accessed in Oct 18, 2019 . https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf
85. Bourque P, Fairley RE (2014) Swebok v3.0, guide to the software engineering body of knowledge
86. He Q, Antón AI, et al (2003) A framework for modeling privacy requirements in role engineering. In: Procedures of REFSQ, vol 3, pp 137–146. REFSQ. https://core.ac.uk/display/21027630
87. Kalloniatis C, Kavakli E, Kontellis E (2009) Pris tool: A case tool for privacy-oriented requirements engineering. In: MCIS, p 71. Athens University of economics and business / AISeL
88. Dashti S, Ranise S (2019) Tool-assisted risk analysis for data protection impact assessment. In: Privacy and identity management, IFIP advances in information and communication technology, vol 576, pp 308–324. Springer
89. Pavlidis M, Islam S (2011) Sectro: A CASE tool for modelling security in requirements engineering using secure tropos. In: CAiSE forum, CEUR workshop proceedings, vol 734, pp 89–96. CEUR-WS.org
90. Mohammadi NG, Leicht J, Ulfat-Bunyadi N, Heisel M (2019) Privacy policy specification framework for addressing end-users' privacy requirements. In: Trust, privacy and security in digital business - 16th international conference, TrustBus 2019, Linz, Austria, August 26-29, 2019, proceedings, pp 46–62. Springer. https://doi.org/10.1007/978-3-030-27813-7_4, https://dblp.org/rec/conf/trustbus/MohammadiLUH19.bib
91. Jensen C, Tullio J, Potts C, Mynatt ED (2005) Strap: a structured analysis framework for privacy. Tech rep, Georgia Institute of Technology
92. Alshammari M, Simpson A (2017) A UML profile for privacy-aware data lifecycle models. In: Katsikas SK, Cuppens F, Cuppens N, Lambrinoudakis C, Kalloniatis C, Mylopoulos J, Antón AI, Gritzalis S (eds) Computer security - ESORICS 2017 international workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, september 14–15, 2017, revised selected papers, lecture notes in computer science, vol 10683. Springer, New york, pp 189–209. https://doi.org/10.1007/978-3-319-72817-9_13
93. Merriam SB, Tisdell EJ (2015) Qualitative research: a guide to design and implementation. Wiley, New york
94. Kasauli R, Knauss E, Horkoff J, Liebel G, de Oliveira Neto FG (2021) Requirements engineering challenges and practices in large-scale agile system development. J Syst Softw 172:110851
95. Martins HF, de Oliveira Junior AC, Canedo ED, Kosloski RAD, Paldês RÁ, Oliveira EC (2019) Design thinking: challenges for software requirements elicitation. Information 10(12):371
96. Dikert K, Paasivaara M, Lassenius C (2016) Challenges and success factors for large-scale agile transformations: a systematic literature review. J Syst Softw 119:87–108. https://doi.org/10.1016/j.jss.2016.06.013
97. Raharjo T, Purwandari B (2020) Agile project management challenges and mapping solutions: a systematic literature review. In: ICSIM '20: The 3rd international conference on software engineering and information management, Sydney, NSW, Australia, Jan 12-15, 2020, pp 123–129. ACM. https://doi.org/10.1145/3378936.3378949
98. Wohlin C, Runeson P, Höst M, Ohlsson MC, Regnell B (2012) Experimentation in software engineering. Springer, Newyork
99. Kitchenham BA, Pfleeger SL (2008) Personal opinion surveys. In: Guide to advanced empirical software engineering, pp 63–92. Springer

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.