IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 April 2023, accepted 9 May 2023, date of publication 15 May 2023, date of current version 1 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3276294

RESEARCH ARTICLE

Designing Intelligent Agents in Normative Systems Toward Data Regulation Representation

PAULO HENRIQUE ALVES [1], **FERNANDO CORREIA** [1], **ISABELLA FRAJHOF** [2], **CLARISSE SIECKENIUS DE SOUZA** [1], **AND HELIO LOPES** [1]

[1] Department of Informatics, Pontifical Catholic University of Rio de Janeiro (PUC-Rio), Rio de Janeiro 22541-041, Brazil
[2] Law Department, Pontifical Catholic University of Rio de Janeiro (PUC-Rio), Rio de Janeiro 22541-041, Brazil

Corresponding author: Paulo Henrique Alves (palves@inf.puc-rio.br)

This work was supported by the National Council for Scientific and Technological Development (CNPq), Brazil.

ABSTRACT Personal data protection regulation plays an important role in defining the rights and obligations of the agents involved in processing personal data (i.e., data subjects, controllers, and processors). These agents are allowed to execute actions to achieve their goals by obeying the personal data protection rules; however, this exercise may spawn data flow information asymmetry; for instance, a company may have more information regarding how that data is being used than individuals. This asymmetry can undermine individuals' ability to protect their rights and interests and lead to a lack of trust in organizations and government bodies responsible for protecting their data. In this context, this article proposes: (i) a consent metamodel based on the literature to aid agents in identifying their major concerns when sharing personal data; (ii) a structure to build use case scenarios in the personal data regulation context; (iii) an intelligent normative multiagent system architecture to represent the personal data regulation rights and obligations, as well as the agent's decision-making process. The latter will consider the normative rewards and punishments in the aforementioned scenario structure; (iv) a use case in the open banking scenario. This article demonstrates how we propose to contribute to representing agents' preferences and data regulation concerns. We do so with a normative multiagent system and designing agents with cognitive reasoning capabilities.

INDEX TERMS BDI architecture, data regulation, multiagent system, norms, personal data.

I. INTRODUCTION

The massive collection of personal data due to widespread goods and services connected to the internet turns the discussion of regulating personal data into a high-priority theme [1], [2], [3], [4], [5]. Personal data processing impacts not only the Data Subjects (DSs), i.e., sometimes referred to as user, client, student, patient, and many others, but also the Data Controllers (DCs) and Processors (DPs), i.e., software warehouses, e-commerce platforms, financial institutions, universities, hospitals, among others. The latter must observe DS rights, as well as comply with their obligations under the personal data protection regulation.

Failing to comply with personal data regulation can result in significant consequences for an organization. Data regulation penalties due to non-compliance can range from small amounts to huge amounts of money, depending on the type of violation and the circumstances of the case. For instance, in 2020, British Airways (United Kingdom), Marriott International (United Kingdom), Google (France), and TIM telco (Italy) tallied more than €380 million (three hundred eighty million) Euros in fines [6].

In this context, consent is one of the legal basis that authorizes data treatment in many regulations, e.g., in the General Data Protection Regulation (GDPR) and in the LGPD. (*Lei Geral de Proteção de Dados Pessoais*),[1] Typically, consent requires that DS are informed of how the data treatment will occur and interact to accept or not the DC terms. This

The associate editor coordinating the review of this manuscript and approving it for publication was Agostino Forestiero.

[1] Law 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Accessed on December 10, 2022. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

information is presented in a privacy policy format to DS decide whether to accept it or not. The non-acceptance of these terms often implies the DS's non-allowance to access the requested service or goods. This interaction may raise doubts and questions related to the interpretation of the consent term if not detailed, explained, and experienced [7], generating information asymmetry.

Varici [8] defines that information asymmetry occurs when one side of the negotiation table has more or better information than the other, which may generate a hazardous environment. For instance, a company may have more information regarding how that data is being used than individuals. This asymmetry can undermine individuals' ability to protect their rights and interests and lead to a lack of trust in organizations and government bodies responsible for protecting their data. Thus, modeling consent entities and their relationship is a crucial step toward improving data agents' knowledge about how their personal data will be treated.

The challenge goes beyond jurisdictions, as an illustration, in 2018, the global bank HSBC failed to implement effective controls to prevent misuse of its services, which led to a \$1.9 billion settlement with the U.S Department of Justice, and regulatory fines and penalties in other jurisdictions [9]. One year after, the same bank was fined £33.6 million (thirty-three million) Pounds by the UK's data protection regulator, the Information Commissioner's Office (ICO), for failing to protect customers' personal data. The ICO found that the bank had failed to implement appropriate security measures to protect personal data.[2] These cases demonstrate the challenges that multinational financial companies may face in complying with data protection regulations, and the severe consequences of non-compliance, which can include significant fines and penalties, as well as reputational damage.

In this sense, user agents can shape and manage personal data available to be collected at the point at which that data is inserted, by whom, how, and with which constraints in the system [10], [11]. Following this affirmative, Multiagent System (MAS) is an Artificial Intelligence (AI) paradigm [12] that enables representing data agents as autonomous agents in a shared environment [13], [14]. As agents cohabit in a shared environment, Normative MAS (NMAS) can orchestrate their behaviors by proposing rewards, punishments, obligations, prohibitions, and permissions to make agents contribute and coexist in society. Moreover, BDI (Belief-Desire-Intention) is a reasoning architecture [15] that enables agents to decide how to accomplish their goals based on their preferences. Combining NMAS and BDI architecture can be an instrument to represent data agents' preferences and data regulation norms in order to clarify and aid agents in their decision-making process, particularly when they are faced with questions related to data sharing and what are the limits of data treatment, which was informed and consented by the DS.

A. PROPOSAL

Whenever the processing of personal data happens, DS must be presented with information regarding what will happen during this activity, such as the purpose, time range, the DS, DCs, and DPs identification, etc. The privacy policy must be disclosed as a rich explanation to justify the actions performed in a specific scenario. In order to represent the privacy policy elements to request the DS's consent, we defined the Consent Metamodel (CM) based on three ontologies in the literature.

These ontologies present many concepts in common. For instance, the consent entity is a legal basis mentioned in all those ontologies, as well as the concept of Data Subject to represent users, and Data Controllers and Processors to represent companies or organizations that are dealing with personal data. Other critical entities presented in these three mentioned ontologies are the concept of Rights and Purpose. The former is responsible for setting up the DSs' rights foreseen in the applied regulation, such as GDPR or LGPD. The latter must express the major goal of collecting and processing data, which must be formulated in clear and objective language to enable the Data Subject to understand and evaluate if he/she will proceed to share his/her data. Thus, CM aims to clarify the required consent entities and their relationship to data agents (DSs, DCs, and DPs). These concepts are not exclusive to GDPR or LGPD. They also might be applied to other data protection regulations worldwide. However, we focused on these two regulations to start the discussion.

Based on this metamodel, this work also proposes GoDReP (Generation of Data Regulation Plots), which aims to enable data agents to describe application scenarios where the Consent Legal Basis is employed. To do so, GoDReP proposes using first-order logic to enhance environmental compliance in the scenarios developed by data agents.

Furthermore, this article also proposes RegulAI (Artificial Intelligence approach for Data Regulation). This approach aims to apply artificial intelligence techniques to represent the data regulation rights and obligations as well as the agent's decision-making process based on CM and GoDReP specifications. RegulAI employs NMAS to represent data regulation constraints and the BDI (Belief-Desire-Intention) reasoning to express the data agent's preferences. Nevertheless, as autonomous entities, NMAS agents may not comply with environmental norms. Hypothetically, it is possible to simulate DCs that intend to proceed with adverse activities in order to benefit from the DS's naivety or lack of knowledge about their rights. Therefore, RegulAI proposes a BDI decision-making process to enable agents to decide whether to comply based on their BDI preferences.

B. USE CASE SCENARIO

In order to materialize the application of our proposals, we present an open banking use case scenario. Open banking is a financial system that allows DSs to migrate their personal and financial data between institutions. The trade-off in such

[2] https://www.bbc.com/news/technology-46117963

action is to receive more credit, better interest rates, and fewer fees. As mentioned by Posner [16], economics and law are highly connected. For instance, the DS can request a credit card from Bank-A, a financial loan from Bank-B, and buy assets from Bank-C. However, there are strict rules set by the Central Bank to enable data exchange between financial institutions. For example, the consent term related to open banking must not be provided by paper or an adhesion contract, by forms with agree option filled by default, or without an explicit will of acceptance from the DS. This requirement is the same foreseen in many personal data regulations, such as GDPR and LGPD, regarding the consent request.

The DSs that want to participate in the open banking ecosystem have to agree with a consent term that allows the institution to share their personal and financial data, e.g., full name and account balance. Following the GDPR and the LGPD rules, the institution must offer the DSs an option to revoke their consent at anytime.

Therefore, this use case scenario can encompass: (i) the CM usage defining the privacy policy attributes required to request the DS's consent, (ii) the GoDReP employment describing the open bank application scenario, and (iii) the RegulAI operation representing the BDI data agents' preferences and the data regulation constraints in an NMAS environment.

C. CONTRIBUTIONS

This article proposes the following contributions:

- We created the CM based on the literature ontologies to express the privacy policy elements to request the DS's consent.
- We developed the GoDReP structure to enable data agents to follow the CM entities and relationships to generate scenarios in order to align their expectations regarding data regulation interpretation.
- We proposed the RegulAI approach on top of normative multiagent systems literature to represent personal data regulation rights and obligations as well as the agent's decision-making process previously described using GoDReP.
- We applied all contributions above in the open banking use case scenario to materialize the employment of our contributions.

D. ARTICLE STRUCUTRE

The remainder of this article is organized as follows. Section II defines the personal data regulation and multiagent concepts used in this article. Section III presents the state-of-the-art. Section IV details the consent metamodel and GoDReP. Section V describes RegulAI as an NMAS architecture considering BDI decision-making process to represent data regulation concerns and agents' preferences. Section VI presents the Open Banking use case scenario. Section VII describes the limitations of this article. Finally, Section VIII presents our conclusions and future work.

II. BACKGROUND

A. DATA REGULATION

Personal data regulation, such as GDPR and LGPD, aims to set rights and obligations when personal data is treated, so that data is shared, treated, and governed appropriately. It is essential to protect individuals' personal data and privacy rights. In order for that to happen, businesses and organizations must handle data responsibly and ethically, according to the law. In this sense, some key principles of personal data regulation include transparency, accountability, fairness, and data minimization. There are many examples of data regulation worldwide besides GDPR and LGPD, including the California Consumer Privacy Act (CCPA) in the United States [17], and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada [18].

In order to ensure adequate protection of individual's personal data, it is important that an independent regulatory agency exists. Such an agency is responsible for enforcing the law, affecting businesses, government, and individuals in many different ways. For businesses, as well as the government, it can impose specific requirements and restrictions on how they collect, use, and store personal data [19], [20], [21], [22]. It can also carry penalties for non-compliance, such as fines and other sanctions. For individuals, data regulation can give them more control over their personal information and greater confidence in how their data is used. However, this plot presents challenges and limitations, including balancing personal data protection with the legitimate interests of businesses and the government. Thus, there is a need to adapt due to the development of rapidly changing technologies and business models.

Regarding the penalties due to non-compliance, e.g., under the GDPR, the fine depends on the type of violation and the circumstances of the case. It can range from a few thousand euros to several million Euros. For example, in 2020, British Airways (United Kingdom), Marriott International (United Kingdom), Google (France), and TIM telco (Italy), led the top four ranking of companies that received the most expensive fines in Europe due to data regulation violations [6]. The total amount of these fines was more than €380 million (three hundred and eighty million) Euros.

In Brazil, the LGPD puts forward a set of rules and obligations that regulate the use of personal data by public and private entities. Thus, controllers and processors must evaluate which legal basis is foreseen in the law authorizing users' data collection (LGPD, Arts. 7 and 11).

Thus, even though GDPR and LGPD are two different pieces of personal data bills, from two different countries, they present similarities. In general, companies may face higher fines for violations that pose a greater risk to the rights and freedoms of data subjects, such as violations of their rights or data security breaches. Therefore, this can indicate that a system developed considering one of these data regulations could be reused in another country by changing a set of business norms and values instead of building them from scratch.

B. LEGAL BASIS

GDPR and LGPD set out the legal basis for collecting, processing, and storing personal data. Both legislations require businesses, governments, and organizations to have a valid legal basis for processing personal data. They list several possible legal basis for processing personal data. The most commons ones are:

(i) Consent: Processing personal data is allowed if the data subject has freely given their explicit consent;
(ii) Contract: Processing personal data is allowed if it is necessary for the performance of a contract with the data subject;
(iii) Legal obligation: Processing personal data is allowed if it is necessary to comply with a legal obligation;
(iv) Vital interests: Processing personal data is allowed if it is necessary to protect the vital interests of the data subject or another person;
(v) Public interest: Processing personal data is allowed if it is necessary for the performance of a task carried out in the public interest, and
(vi) Legitimate interests: Processing personal data is allowed if it is necessary for the legitimate interests of the controller or a third party, provided that those interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

The specific legal basis applied in a given situation will depend on the context and the purpose of the processing. It is important for businesses and organizations to carefully consider which legal basis applies in their case to ensure that their data processing activities are legal, legitimate, and valid.

However, the existence of a valid and effective regulation does not prevent data breaches or abusive and illegitimate data uses [23]. It is important that citizens are aware of their rights and understand how they can enforce them [24], [25]. This knowledge is essential not only for people that have shared their data but also for companies that receive such data. Those companies must be compliant with the data regulation law from the jurisdiction in which they exercise their activities. The law infringement may imply significant financial losses, administrative and judicial processes, as well as damage to reputation.

C. CONSENT

Consent is one of the most commonly used legal basis for processing personal data. It allows individuals to control how their data are used and sets the purposes for which their data will be used. Obtaining consent can be critical in situations where the processing of personal data may be considered sensitive, such as health data or data related to a person's sexual orientation or religious beliefs.

According to LGPD, consent will be valid when freely given, specific, informed, and unambiguous. This means that the individual must clearly understand what they are agreeing to and must not feel pressured or coerced into giving their consent. It is also important that the individual has the option to withdraw their consent at any time. It is the DC's onus (the person or organization collecting and using the personal data) to ensure that they have obtained valid consent from the individual before processing their personal data.

It must be remarked that the Brazilian data protection regulation establishes that individual consent is only one of the legal basis authorizing data processing. In any case, data controllers must abide by the law's principles, rights, safeguards and act in good faith.

DSs, or individuals whose personal information is collected and processed by businesses and organizations, may have many concerns about their data. Some common concerns include:

(i) Privacy: Data subjects may be concerned about their privacy and the unauthorized disclosure of their personal information. They may worry about who has access to their data and how it is being used;
(ii) Security: Data subjects may be concerned about the security of their personal information and the potential for it to be stolen or misused. This can include worries about data breaches and cyber-attacks;
(iii) Control: Data subjects may be concerned about having control over their own data and the ability to access, correct, or delete it if they wish;
(iv) Fairness: Data subjects may be concerned about whether the collection and use of their personal information are fair and justified and whether they are being treated equitably, and
(v) Transparency: Data subjects may be concerned about whether they are being informed about how their data is being collected and used, and whether they are being given sufficient information to make informed decisions.

Overall, data subjects may have a wide range of concerns related to their personal information and how it is being handled by organizations.

Thus, providing clear, straightforward, and complete information in a consent term to guarantee the DS's understanding can be challenging for DCs. Moreover, DSs are responsible for authorizing the use of their data, and evaluating all information regarding data processing can be hard for DSs without legal knowledge. It must be noted that legal knowledge must not be required to give consent. Therefore, the consent term must give specific, straight, and unambiguous information to facilitate the DS's comprehension.

D. MULTIAGENT SYSTEMS

Multiagent Systems (MAS) are distributed computing systems composed of intelligent and autonomous agents able to interact with each other in collaboration to achieve a specific goal in a non-supervised environment without human intervention [15]. These agents can take reactive actions, i.e., reactions triggered by others agents' actions or environmental changes.

In a NMAS, a set of norms defines the environmental boundaries regarding the expected agent's behavior, as well

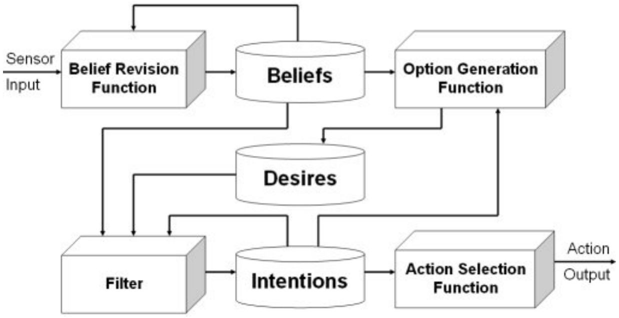


FIGURE 1. BDI architecture [15].

as in the current society, where we have laws and regulations ruling citizens' rights and duties. Regarding citizens' rights, in most jurisdictions, we have sets of laws and regulations to ensure citizens' rights against scenarios of abuses, whether from other people, organizations, or the government itself. In this sense, in NMAS, norms emerge to orchestrate agents' environment without disturbing the agent's autonomous capabilities. In summary, the NMAS elements are:

- **Environment**. It is responsible for supplying data to agents to update their beliefs and norms database.
- **Agent**. An agent is composed of its roles and goals.
- **Agent's Role**. It describes the agent's role in the environment.
- **Organization**. It specifies agents into groups and roles.
- **Norm**. It is composed by its *activation, expiration, deontic concept state, rewards* and *punishments* values and specifies to which agent's role this norm is *addressed*.

Norms can be beneficial or harmful, depending on their alignment with the agent's programmed goals. In this sense, agents must be able to reason about the rewards and punishments defined in an active norm addressed to its role to decide which they should comply with and occasionally violate if it is in conflict with other norms or with the agent's private goals [26], [27], [28], [29].

In this sense, the BDI architecture is a model to enable agents to decide how to accomplish their goals and which norms to comply with or violate [15]. Fig. 1 presents the agent's reasoning process. This process starts with the agent's environmental perception, i.e., the environment's sensor updates the environmental attributes and enables the agent to update its beliefs database. Then, based on its beliefs, the agent generates and stores its desires in the desires database. Next, the agent filters its beliefs, desires, and intentions, selecting the actions that the agent can perform to achieve its goals.

The BDI reasoning architecture can complement NMASs [30] since an agent should deliberate whether to comply with norms based on environmental perception and its goals. The combination of BDI architecture and NMAS allows the representation of the agent's reasoning in a normative data-regulated environment. Thus, MASs can monitor and automate aspects of data regulation, such as reporting data breaches and sharing data between different organizations. For instance, a DC agent should respect the environmental norms, e.g., GDPR or LGPD, whereas DS agent reasons regarding its beliefs, desires, intentions, and goals to decide whether share its personal data.

III. RELATED WORK

A. DATA REGULATION REPRESENTATION

Based on the GDPR, [31] presented an open vocabulary of expressing consent leveraging existing semantic models of provenance, processes, permission, and obligations. The authors presented a reference architecture for data processing management based on consent permission in the GDPR context. However, this work highly depends on both the application and the use case scenario. In this sense, our work proposes GoDReP to describe the data regulation entities and concerns in a context-free structure.

In [32], the authors followed a similar path presenting a GDPR-based formalized ontology focused on data privacy. Such ontology is composed of five main modules: (i) data, (ii) actors and roles, (iii) processing, (iv) legal rules, and (v) legal basis. The goal of these modules is to promote the separation of concerns providing a clear overview of the major concerns of data subjects, controllers, and processors when faced with GDPR obligations. As this ontology delivers entities that are compatible with LGPD, we considered those entities when developing our CM.

Regarding consent, [33] proposed GConsent, an ontology focused on the GDPR consent legal basis (GPDR Art. 6). This ontology aims to represent consent and compliance requirements. Moreover, such ontology presents new entities that were not approached in the previous work, such as consent which was "not given", refused, or withdrawn status. Sill, GConsent introduces the concept of implicit or indirect consent, i.e., consent is given by a legal person on behalf of another. For instance, children and teenagers must request their parents' consent on their behalf to start using bank accounts. However, the use cases presented did not describe the context details in which the proposed entities were applied. In this sense, GoDReP allows DSs, DCs, and DPs to expose their concerns and align their understanding of data regulation impact.

In [34], the authors argue that privacy concerns should be considered from the early system design phases. They propose a Core Ontology for Privacy (COPri) requirements engineering. The goal was to elaborate high-quality requirements models to allow system development in compliance with many data regulations, such as GDPR in the Europe Union, Privacy Act in Australia, PIPEDA in Canada, and HIPPA in the United States regarding the healthcare domain. Moreover, the authors exemplified the COPri instantiation in an Ambient-Assisted Living (AAL) system in the healthcare domain. Despite the multi-regulation adaptability feature, COPri was built targeting software engineers instead of standard users, e.g., citizens and business managers. In our work, GoDReP enables standard users to follow the CM entities and relationships to generate scenarios in order to align their expectations regarding data regulation interpretation.

With a focus on the Brazilian regulation, the GDPR, [35] propose an Ontology for Data Privacy Management based on the LGPD named ODPM. In this work, the authors presented an ontology that enables the representation of the major concerns regarding DSs, DCs, DPs' rights and obligations. To attest to the ODPM ontology capabilities, they applied such ontology in the pandemic outbreak scenario illustrating its use and proposing the adoption of blockchain technology to persist the data transparently, distributed, and immutable. Currently, this is the only ontology that presents the LGPD concerns in the literature; thus, we also considered this ontology in our CM and, hence, in the GoDReP construction.

B. MULTIAGENT SYSTEMS

NBDI is a conceptual framework proposed by [36] that aims to enable software agents to consider their beliefs, desires, and intentions when evaluating the norm's contribution (positive, negative, or neutral) in an NMAS. In [36], the authors defined agents as goal-oriented entities with the purpose of achieving their desires and fulfilling the system norms concomitantly. However, respecting the data regulation proposals when managing personal data is also crucial to MAS developed in such context, including normative and BDI agents. In this sense, RegulAI proposes an architecture to address not only the normative BDI agents but also data regulation rules.

BDI4Jade is a framework that aims to enable the use of the BDI reasoning process in MAS [37], [38]. The authors extended the JADE framework [39], and included BDI capabilities to represent the agent's decision-making process considering their goals and plans. However, they did not explore the BDI capabilities in NMAS. In our work, RegulAI aims to consider the agent's capabilities, i.e., goals and plans, in NMASs.

To support normative agents modeling, [40] and [41] proposed the NorMAS-ML (Supporting the Modeling of Normative Multi-agent Systems) and the ANA-ML Adaptative Normative Agent - Modeling Language), respectively, as tools for modeling normative agents. They are extensions of MAS-ML [42] that enable modeling normative attributes in MAS. Their metamodel aims to improve the understanding of how agents can change their behaviors to deal with norms and captures interactions between agents' norms and adaptation. However, [40] neither [41] considered the reasoning process in their metamodel or data regulation entities. Thus, GoDReP and RegulAI can fit this gap.

To identify environmental norms, [43] proposes the RNDT (Regulative Norms Detection Technique), a technique to detect norms considering their rewards and penalties. Even though addressing norms challenges is not our focus, the authors proposed a norm taxonomy that classifies norms as follows: (i) regulative, (ii) constructive, and (iii) procedural. Moreover, the authors did not consider the BDI reasoning on the agent's decision-making process, although the regulative term emerged through the deontic concepts. Therefore, RegulAI can fill this gap and represent regulative norms considering the agent's purpose.

In previous work [14], we presented an NMAS solution for data regulation, the DR-NMAS (Data-Regulated Normative Multiagent System). The proposed solution aims to represent data regulation concerns by norms development, employing rewards and punishments for obligations and prohibitions to DC agents who decide to comply or violate them. In such an approach, the deontic concept *permission* represents the DS rights, whereas *obligation* and *prohibition* represent the DC's and DP's duties. However, the agent's goals and cognitive reasoning to define the agents' decision-making process were out of scope, as well as the GoDRep approach to develop use case scenarios. Also, in this previous work, we did not perform the consent legal basis evaluation to identify the major entities and their relationships. Thus, we propose CM, GoDReP, and RegulAI to address these points.

C. OPEN BANK APPLICATION SCENARIO

The open banking scenario was selected for the challenges of sharing personal and transactional data among different financial institutions. Although the Central Bank regulates processes regarding data sharing, financial institutions must comply with data protection regulations according to the country's jurisdiction.

A framework for data privacy management was proposed by [44] to address concerns regarding GPDR compliance in the open banking scenario. Even though the authors presented an analysis regarding the attributes that must be informed in the consent term and the DS data sharing authorization process, they did not follow any ontology to base their framework. Hence, applying this framework in other jurisdictions might not be possible or at least more complex than a framework based on an established ontology. In this sense, our solution fills this gap by proposing: (i) CM to identify which entities and relationships should be changed to represent a country's data regulation; (ii) GoDReP to describe the use case scenario in natural language and forced by Prolog sentences, and (iii) RegulAI to represent the agent's reasoning process in the normative environment, generating a consent compatibility index.

Moreover, the digital disruption in the banking scenario can increase the system's efficiency and services, overcoming information asymmetries through big data, artificial intelligence, machine learning techniques, and blockchain technology associated with a straightforward user interface [45]. The authors in [45] mention that these techniques can improve the DS experience and deliver a less bureaucratic process in favor of the DSs. However, there is a lack between the DSs and the technology employment; the DSs should be able to evaluate their rights according to the local data regulation and think over the possible scenarios they could experience.

The authors in [46] mention that beyond the data protection regulation, open banking should follow the PSD2 (Payments Services Directive) that regulates payment-related services to third-party providers. Even though the PSD2 sets the best practices for developing APIs, managing data, and integrating vendors in the European Union, this directive must be translated into law in each specific country to respect the local regulatory jurisdiction. To do so, our proposed solution would contribute to this specification by defining entities, their relationships, scenario description, agents' purpose, and norms representation.

D. CONCLUDING REMARKS

Therefore, according to the presented related works, we have not found a metamodel to represent the Consent legal basis in a specific data regulation, nor a structure that could encompass adaptations that are required when changing the data regulation jurisdiction. Moreover, there is a gap in modeling data regulation use case scenarios to enable DSs, DCs, and DPs to express their understanding regarding regulation interpretation.

Last but not least, no related work presents an architecture representing the data agents' preferences nor offers the open banking scenario as a use case. Thus, in the following sections, we will introduce a proposal for modeling data regulation use case scenarios and their representation in NMAS with BDI agents to fulfill the gaps found in the literature.

IV. MODELING DATA REGULATION

To describe and produce use case scenarios in a specific domain, first, the data agent should understand the data regulation entities and their relationships. In this sense, this article proposes the Consent Metamodel (CM) based on the ontologies found in the literature to offer a summarized view of these entities and their relationships to data agents in a data processing context. These entities represent the privacy policy elements that must be included in the consent term to comply with personal data regulations. Complementary, this article proposes GoDReP (Generation of Data Regulation Plots) to allow data agents to describe use cases and their understanding of personal data regulation interpretation enforced by first-order logic sentences based on CM.

A. CONSENT METAMODEL

Modeling data regulation attributes is relevant for organizations to understand and comply with personal data protection regulations. Failing to comply with legal provisions can result in several consequences for an organization, such as financial and reputational damage (as presented in Section II-A). By defining such attributes, organizations can put appropriate controls in place to ensure that the data is handled following those regulations. These controls may include limiting access to authorized personnel and implementing robust security measures to protect against unauthorized access or breaches.

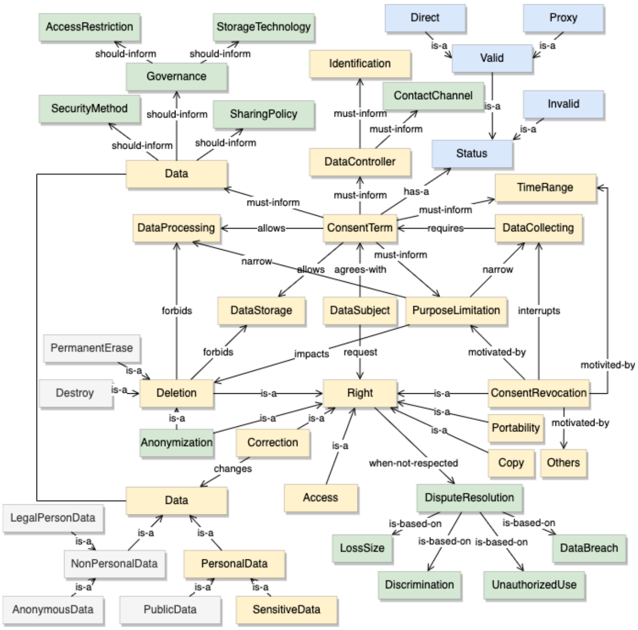


FIGURE 2. Consent metamodel diagram.

On the other hand, from the DSs perspective, personal data regulation establishes rules to DCs and DPs to handle personal data. This can give DSs greater confidence that their personal data will be handled responsibly, transparently, and that their privacy will be respected. Thus, modeling data regulation attributes can help to protect the rights of DSs and ensure that their personal data is handled in a way that respects their preferences.

As mentioned in Section II, this article focuses on the Consent Legal Basis and on defining requirements for generating adequate consent. This can be challenging, especially in a globally connected world, i.e., where companies, governments, and citizens can offer and access services worldwide throughout different jurisdictions. In this sense, [47] proposed a survey to explore the consent's state of the art and its best practices based on a table of competency questions related to GDPR. We enhanced this table by addressing the LGPD provisions for each question, generating Table 1. This table shows the relevant concepts related to the consent legal basis and addresses where their definitions can be found in GDPR and LGPD.

As presented in Table 1, although GDPR and LGPD present different structures, all questions are addressed in both regulations. It means that an ontology built considering the GDPR perspective can be suitable to LGPD, with a few changes, since they present similar concerns. PrOnto and GConsent are ontologies based on the GDPR, just as the ODPM is based on the LGPD, which enables consent knowledge representation. This article proposes the Consent Metamodel (CM) inspired by these three ontologies and the aforementioned competency questions. Fig. 2 depicts CM for GDPR and LGPD. The yellow entities are those present in the PrOnto ontology, as depicted in Table 2.

The blue entities from GConsent help differentiate between valid and invalid consent status and whether the DS gave the consent directly or through a proxy. If the DS agrees with the consent term and decides to give consent, it is called *Direct* consent. On the other hand, if the DS is under a guardian or tutor, such as children or anyone who cannot be legally

TABLE 1. GDPR and LGPD competency questions.

Question	Relevant Concepts	GDPR	LGPD
Who collects the data?	DC, DP	Art. 4 (7), Art. 6, Art. 28	Art. 5, Art. 7, Art. 9, Art. 11, Art. 14
What is the purpose?	Purpose	Art. 4 (4), Art. 7 (32), Art. 6 (1a, 1f, 4)	Art. 6, Art. 7 (7)
How to revoke consent?	Status	Art. 17, Rec. 63, Rec. 66	Art. 9 (2), Art. 15
How long does consent last for?	Time Range	Rec. 32, Rec. 42	Art.6, Art. 9, Art. 15, Art. 16
When was consent given / revoked?	Time Range / Status	Art. 17, Art 19	Art. 8 (5,6), Art. 15
What personal data is collected?	Personal Data Categories	Art. 4 (1), Art. 9	Art. 5, Art. 9, Art. 10
How is the personal data being used?	Processing	Art. 4 (2)	Art. 7, Art. 11, Art. 14
How is personal data collected?	Data Collection	Art. 12, Art. 13, Art. 14, Rec. 39, Rec. 58, Rec. 62, Rec. 73	Art. 3, Art. 14 (3)
With whom is personal data shared?	Data Processing, Sharing Policy	Art. 4 (7), Art. 6, Art. 28	Art. 4, Art.5, Art. 7, Art. 11, Art. 18, Art. 27
Who is responsible for the personal data?	DC	Art. 24, Rec. 74, Rec. 79	Art. 9
Where is personal data stored?	Data Storage	Art. 5	Art. 5
Who is the DC?	DC	Art. 4 (7), Art. 28	Art. 5, Art. 9
How to contact the DC?	DC, Contact Channel	Art. 4 (7), Art. 14, Art. 28	Art. 9
What are the responsibilities of the DC?	DC, Right	Art. 4 (7), Art 14, Art. 28, Art. 37	Art. 7
Who is the DS?	DS	Art. 4 (1)	Art. 5
Whom to contact?	Contact Channel	Art. 12, Art. 13, Art. 14	Art. 5, Art. 9

TABLE 2. PrOnto's entities.

Entity	Description
ConsentTerm	Informs the subject and the DC, the purpose limitation, the data that will be collected and processed, and the time range.
DataSubject	The DS's personal data and rights to be respected
DataController	The DC's identification.
DataCollecting and *DataProcessing*	Collecting and processing techniques limited by presented purpose.
DataStorage	The data storage that can be restricted by a data deletion request.
Data	The data which can be classified as *PersonalData* and *SensitiveData*, but also should have data governance guidelines, sharing policies, and security methods informed.
Right	Represents the DS rights foreseen by a data regulation.
Identification	Define the information that enables identifying DC.
PurposeLimitation	Defines the circumstances that DC can collect and use data.

TABLE 3. ODPM's entities.

Entity	Description
DataGovernance	Impacts data access policies and storage technologies architecture to safeguard data.
SharingPolicy	Describe policies when data are shared with third parties.
SecurityMethod	Describe security measurements to safeguard data.
DisputeResolution	Presents possible causes to start a dispute, such as: *LossSize*, *Descrimination*, *UnauthorizedUse*, *DataBreach*.
Anonymization	Represents a DS right specified by LGPD.
ContactChannel	Define information to DS contact DC.

accountable for themselves, and requires someone else to agree with the consent term on their behalf, it is called *Proxy* consent. For a Proxy consent to be valid, the DS's tutor must receive the privacy policy and the consent must follow the personal data regulation requirements, which include being freely given, specific, informed, and unambiguous. If there is a modification in the consent clause, and the DS has not accepted it yet, or if the due date expires, the consent term is considered invalid. The green entities are inherited from the ODPM ontology, which are described in Table 3.

The gray entities are those which the LGPD does not provide such details as GDPR does. For example, the methods of data deletion and non-personal data are not detailed by LGPD but are present in GDPR. In summary, CM did not apply the *NonPersonalData, AnonymousData, LegalPersonData, PublicData, PermanentErase,* and *Destroy* entities since they are not addressed in depth in the LGPD.

Moreover, there are two definitions of data anonymization. PrOnto considers anonymization as a deletion action, and ODPM considers anonymization not only a form of data deletion but also a DS right. In this sense, we decided to represent both concepts in CM. These entities are essential to understand the environmental factors related to the scenario execution, explanation, and information security.

B. GoDReP-SCENARIO GENERATION STRUCTURE

The Generation of Data Regulation Plots (GoDReP) is a scenario generation structure that aims to enable DSs, DCs, and DPs to build use case scenarios in natural language followed by basic first-order logic expressions in Prolog.[3]

The goal is to allow agents to describe scenarios following a reusable and maintainable structure to align their understanding regarding data regulation impacts and consequences based on their actions. To create a scenario, as depicted in Fig. 3, GoDReP proposes five macro processes:

(i) *Scenario Description*, which aims to identify the agents, purpose, time range, personal data, storage technology, security methods, access restrictions, third-party sharing

[3] Prolog is a descriptive and prescriptive programming language based on first-order logic and formal logic to express relations and represent facts and rules [48].

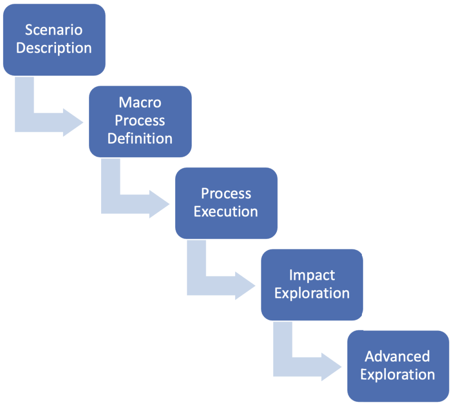


FIGURE 3. GoDReP macro process.

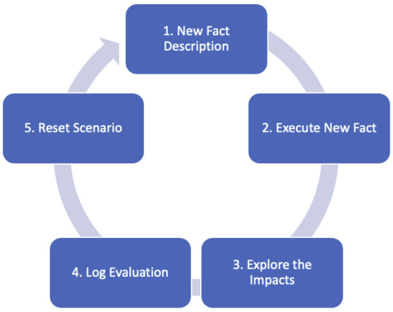


FIGURE 4. GoDReP advanced exploration.

policies jurisdiction, consent compliance requirements based on the jurisdiction;

(ii) *Macro Process Definition*, i.e., the step-by-step design to be executed by the agents;

(iii) *Process Execution*, i.e., the record of the scenario's facts seeking for regulation compliance;

(iv) *Impact Exploration*, i.e., the evaluation of the impacts after the *Process Execution*, and

(v) *Advanced Exploration*, which aims to explore other scenarios to offer evaluation regarding different possible situations.

These processes allow agents to describe the scenarios in detail and explore the understanding of the expected behavior that emerged from the agents' actions.

Moreover, Fig. 4 shows the *Advanced Exploration* process, which proposes the insertion of a new fact and an impact evaluation. The generated log results from the actions performed in the scenario represent secondary evidence of the agent's activity. At the end of each advanced sub-scenario, the new facts are removed, and the flow turns back to the basic scenario state. Hence, the advanced scenarios are independent but rooted on the same basic flow.

The compliance between the ties, facts, and rules is verifiable by running Prolog queries over these relations, evaluating which relationships are valid (''true''), and which formal relationships and objects occur in the proposed environment.

In this sense, Prolog is convenient for exploring rule-based logical queries, and it can support data regulation interpretation. For instance, when we say ''John agrees with the consent term'', we communicate that a relationship, or an agreement, exists between one object ''John'' and the consent term. Moreover, Prolog allows the agents to develop and execute simple queries, such as ''Did John agree with the consent term?'' to determine this relationship value.[4]

TABLE 4. Scenes' description.

Scene	Description
Set consent term	Describe the consent term highlighting the consent requirements.
Verify consent term	The DS can verify throughout queries if the consent term has all items foreseen in the data protection regulation and simulates an agreement.
DS rights	Define the rights based on the data protection regulation.
Consent revocation	The DC has to abide by the DS's request and stop collecting and processing the DS's data.
Impact exploration	Explores the impacts of the previous scenes by performing questions in Prolog to evaluate the facts.

Although GoDReP may indicate a monotonic process execution, scenarios might require changes in the internal processes, i.e., in these cases, the internal process construction will be different from the previously created ones. Moreover, these changes require a user able to change the Prolog code, i.e., a user with programming logic skills.

In this sense, the scenarios' scenes aim to avoid misunderstanding regarding the application domain context. These scenarios respect the GoDReP macro process and the advanced exploration to allow agents to express their understanding regarding their concerns and the expected behavior. The scenes are composed of a basic module and an advanced module. The former is divided into scenes, and the latter explores the insertion of a new set of information to evaluate their impact. The basic module was designed following the structure below, following the concepts presented in Table 4.

The advanced module explores the negotiation scenarios with parameters other than the basic module. Also, this module is composed of cause-effect scenes to evaluate access and processing confirmation, compliance, and information about the consent terms. Those questions aim to aid DSs and DCs in exercising their understanding regarding possible scenarios and the evaluation of their actions. For each ''true'' or ''false'' returned in the Prolog query, GoDReP presents an explanation pointing out the past actions that motivated such a result.

Finally, GoDReP proposes a structure to be reused and adapted to construct negotiation scenarios to mitigate the informational asymmetry related to data privacy, rights, and obligations according to a given data regulation. These negotiation scenarios seek to clarify doubts between agents simulating the expected behaviors in specific cases. Moreover, GoDReP allows the insertion of new clauses related to the domain particularities. Thus, agents can use GoDReP and contribute to constructing an open repository. Instead of

[4] https://github.com/phalves/ConFIA/blob/main/Open_Banking_Scenario.ipynb

building it from scratch, this repository will allow other agents to create use case scenarios based on a previous instantiation.

V. RegulAI

The Artificial Intelligence approach for Data Regulation (RegulAI) aims to apply artificial intelligence techniques to represent the data regulation rights and obligations as well as the agent's decision-making process previously described using GoDReP. This framework proposes applying NMAS to regulate agents' behavior considering data regulation constraints.

As mentioned in Section II-D, NMAS is responsible for defining the *Environment*, *Agents* and their *Roles*, *Norms*, and *Organizations* parameters to ensure that the data regulation will be respected when it emerges in the collection, storage, and use of data, otherwise, agents will suffer punishments.

A new norm can be added into the environment at run-time, and the software agents analyze if the such legal command is activated and addressed to them. Next, they will evaluate if they shall comply or not based on the rewards and punishments.

In the data regulation context, *Norm*'s deontic concept defines if a norm is an obligation, permission, or prohibition [49]. From the DCs and DPs' perspective, norms set their obligations foreseen by a certain data regulation. On the other hand, from the DSs' perspective, the norms set which are their rights, and allow them to exercise them. The addressed agents can decide whether to comply with a norm; they must evaluate the rewards, punishments, and goals to make a decision. Rewards and punishments can be from distinguish nature depending on the use case and the simulation goal. For instance, rewards can be related to increasing reputation and accessing DSs data to agents who comply with a norm. From the punishment's perspective, they can be related to decreasing reputation and issuing fines to agents that decide to violate a norm. Moreover, a *Norm* is activated, or deactivated, if a condition is triggered, turning the norm state to active or inactive.

Agent and *Agent Role* represent DSs, DCs, and DPs entities. *Environment* represents the application domain where the agents reside and provide data to contribute to agents' decision-making process, i.e., agents read the *Environment's* available data and then, based on their goals, decide which action they will perform. *Organization* groups agents that present common goals, e.g., DC agents from a company can be grouped in the same organization.

From the DS's perspective, the BDI decision-making process represents the DS's reasoning. Fig. 5 depicts the normative BDI architecture for designing data regulation representation. This approach aims to provide an explanation for data agents regarding data regulation concerns and the decision-making process when they are involved in a data-sharing plot. Moreover, the proposed architecture is based on two major layers: (i) BDI decision-making process, and (ii) Legal Basis representation. The former provides cognitive intelligence to data agents following the BDI architecture. The latter represents data regulation rights and obligations by norm generation.

In the next sections, we will detail the DS and DC's perspectives when using the RegulAI architecture considering the data regulation norms and the agents' preferences.

A. DS's PERSPECTIVE

From the DS's perspective, the RegulAI process starts when agents are active and observe the environment for events. The *sensors* are responsible for reading the environment's changes and sending them to agents. Next, based on the *sensor*'s returns, DS updates its *Beliefs* and *Norm*'s database, evaluating if any norm is addressed to its role — the system's architecture defines the repetition frequency. Then, DS defines its desires based on its beliefs considering the norms' status addressed to him. The generated desires are stored in the *Desire*'s database.

As we focus on the Consent legal basis, we created a representation of Consent as

$$C =< P, E, S, DC, DS >, \tag{1}$$

where P means the purpose limitation, E means the expiration date, and S represents the data sharing policies to provide clear, straightforward, and complete information.

Then, DS can select a plan based on the Consent Evaluation (CE) and on the Consent Compatibility Index (CCI). CE is defined by

$$CE_{DS} =< D, P, E, S, R_{DC} >, \tag{2}$$

where D is the DS's desire; P, E, S are the DS's preferences, and $0 \leq R_{DC} \leq 9$ is the minimum reputation value acceptable by DS. The DC's reputation is built according to the respected norms, i.e., according to the rewards received.

This representation considers that DS is responsible for providing its preferences (DSP) related to *D, P, E, S,* and R_{DC}, setting weights for each one. DSP is defined as,

$$DSP =< W, X, Y, Z >, \tag{3}$$

where:

- w, if $D_{DS} = P_{DC}$,
- x, if $E_{DS} \subseteq E_{DC}$,
- y, if $S_{DS} \supseteq S_{DC}$,
- z, if $R_{DC_{DS}} \geq R_{DC_{DC}}$,
- $\{w, x, y, z\} \in [0, 9]$,
- $0 \leq sum(w, x, y, z) \leq 10$.

The Consent Compatibility Index (CCI) is a number between 0 and 9 generated from Eq 4. DS can set a minimum score to define an acceptable CCI value according to its preferences and consider this value when deciding whether to share its data. Next, DS should evaluate the norms' rewards and punishments.

$$CCI = \sum_{i=0}^{n(DSP)} DSP_i \tag{4}$$

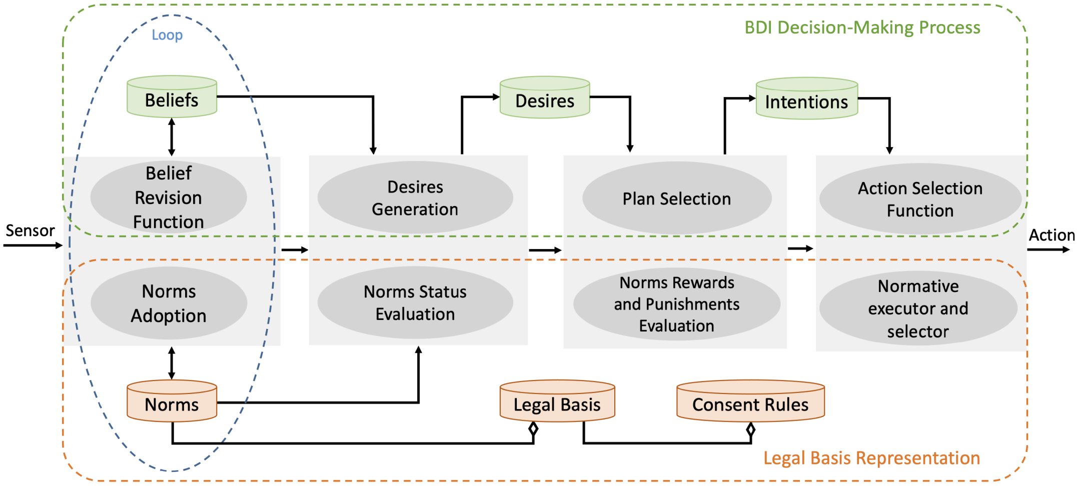


FIGURE 5. Normative BDI architecture for data regulation representation.

Norms define rights (permission) and duties (obligation or prohibition) for agents to execute their goal in a particular context and during a given time. In this sense, deontic concepts can represent data regulation constraints in a normative system. Let $(op \in O, P, F)$, it defines a norm as an obligation (O), a permission (P), or a prohibition (F). Obligation and prohibition are concepts the agent must comply with when such a norm is activated and addressed to him. Otherwise, sanctions or future litigation claiming damages can happen. Conversely, the permission concept allows agents to comply with such a norm facultatively. Thus, a norm follows Eq. 5 construction, let

$$N =< Ad, Ac, Ex, Re, Pu, Op, St >, \tag{5}$$

where Ad represents addressees, Ac represents the activation trigger, Ex represents the expiration trigger, Re represents the norm's reward, Pu represents the norm's punishments, Op represents the deontic concept, and St represents the norm's state.

Thus, the normative contribution (NC) considers the active norms addressed to the Software Agent (SA) to measure the agent desires (D), and norms rewards (Re) and punishments (Pu) as

$$\forall n \in N \begin{cases} NC_n, & \text{if } St = Active \ \& \ Ad = AgRole \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

where $NC_n = D + Re_n - |Pu_n|$.

Finally, the agent's intentions are represented by

$$I =< B, D, CCI, NC, SA_{Plans} > \tag{7}$$

It is important to note that CCI is an element addressed to DSs only, where SA_{Plans} are the available plans considering the software agent's *Beliefs* and *Desires*. Next, the agent decides the compatible action based on its intentions to achieve the selected desire.

B. DC's PERSPECTIVE

From the DC's perspective, software agents must evaluate the environmental norms to decide whether to comply with the current regulation. This agent role will follow the Legal Basis Representation layer depicted in Fig. 5 and defined by its elements in Eq. 1.

First, the agent will read the environmental norms and check which ones are addressed to him. Second, the agent will verify which are the active norms (Eq. 6). Third, the agent will evaluate which norms comply based on the rewards and punishments. Fourth, and finally, the agent will execute his action considering the decision related to the norms that he will comply with or not.

Thus, a DC can define the norms and the consent attributes under a specific data regulation to model the rules that DSs, DCs, and DPs should follow, evaluating the pros and cons of sharing and managing personal data. Moreover, NMAS enables the development of a simulation environment for DSs to experience the defined rules and impacts when sharing data.

Last but not least, NMAS can be used to monitor the use of data by organizations and to flag any instances where the data is being used in ways that are not in accordance with the preferences and expectations of the DS. This can aid in protecting the DSs' privacy and ensure that their data is only used in scenarios that they are comfortable with.

VI. OPEN BANKING USE CASE

In order to materialize the employment of CM, GoDReP, and RegulAI, this section presents a use case scenario in the open banking application domain. Open banking is a financial system that allows DSs to migrate their data between institutions to receive more credit, better interest rates, and fewer fees. This system provides third-party data access through application programming interfaces (APIs). Once allowed by DSs, the financial institution will be able to access the DSs' data for a specific time range. This authorization is given under the acceptance of a consent term, which defines which data will be shared, with whom, and for how long it will take. This consent term must follow the current data protection regulation according to the DC and DS location.

As mentioned in Section II-C, the consent is any freely given, specific, informed, and unambiguous demonstration of the DS's desire by a statement or by a clear affirmative action that signifies agreement to the processing of personal data relating to him or her. DS can revoke its consent at anytime by requesting such action for DC, following the communication channel provided in the consent term. In the open banking scenario, the consent may present different expiration dates depending on the country from DS and DC. For instance, EU sets the expiration should be ninety days at most, while Brazil determines twelve months.

This use case proposes the employment of GoDReP to design an open baking use case scenario where there are two agents, John as a DS agent and Bank-B as a DC agent. John aims to share his data from Bank-A, located in an EU country under GDPR jurisdiction, to Bank-B, located in Brazil (LGPD jurisdiction), to receive offers for better interest rates. In this case, RegulAI will reproduce the DS's decision-making process as well as the DC norms. Next, this use case will experience the creation of a new Bank-A branch in the EU; hence, the new branch will have to follow the Brazilian open banking rules and, thus, new norms will be developed.

To design the financial data-sharing scenario, we followed the GoDReP process. First, the scenario description was developed to contextualize the readers, providing the open banking goals and particularities.

Second, the macro process was defined considering that the consent term presents all attributes foreseen in the data regulation, such as the purpose of collecting data, expiration date, sharing policies, and communication channels. Moreover, for this scenario, we consider that John (i) has given his consent to Bank-A, (ii) will give his consent to Bank-B, and (iii) then will decide to revoke his consent.

Third, the process execution starts with developing the Prolog sentences to: (i) check the consent term attributes provided by Bank-B. For instance, Bank-B's purpose is to offer the best interest rates, the consent is valid for twelve months, and the data will be shared with Bank-B partners, for the same purpose, (ii) simulates the acceptance by John, (iii) settle John's rights, such as data copy and data portability requests, and (iv) finish with John revoking his consent. Fourth, and finally, the impact evaluation describes, for instance, the data breach scenario. Other cause-effect cases are described in detail in the open repository.[5]

After the scenario development using GoDReP, the next step is to start building the RegulAI environment, defining two agents, John and Bank-B as Normative BDI agents to represent John's and Bank-B's decision-making process. Table 5 presents the DC agent (John agent) attributes:

TABLE 5. John as a normative BDI agent.

Beliefs (B_J)	*Bank-A allows DSs to share their data through the Open Bank process*
	Bank-B offers receiving data from DSs through the Open Bank process
	Bank-B offers the best interest rates on the market
Desires (D_J)	*Investing saving's balance for a year in with the best returns*
	Share financial data with Bank-B and Bank-C only
Intentions (I_J)	*it will be generated after John evaluates the consent provided by Bank-B*
Plans ($Plans_J$)	*Open an account on the new bank*
	Transfer money to this new account
	Invest this money

However, besides the BDI attributes definition, RegulAI requires the legal basis definition and its attributes to be considered in John's decision-making process. As this scenario requires the Consent legal basis, John has to inform his consent preferences to generate the *CCI* defined by Eq. 4, and the *CCI*'s minimal score, i.e., the minimum acceptable value so that John can give his consent. For this use case scenario, we will consider minimum $CCI = 6$. Besides, to reach the highest score, the DC must present a consent term with:

- Purpose equals John's desire, then DSP(w) = 4,
- Expiration date equals 365, then DSP(x) = 2,
- Sharing policy equals to "*Share financial data with Bank-B and Bank-C only*", then DSP(y) = 1,
- DC's reputation bigger than 8, then DSP(z) = 3.

Once defined John's preferences, the next step is representing Bank-B's consent terms and the environmental norms. As defined in the scenario described using GoDReP, Bank-B offers receive data from other banks to allow DSs to create new accounts and migrate their investments. To do so, Bank-B requests the DS's consent. This consent term presents the following attributes and values:

- Purpose: *Offer the best interest rates*,
- Expiration: *12 months*,
- Sharing Policy: *Organization with the same purpose only*.

Moreover, as Bank-B is a new bank, its reputation will be considered zero. Thus, these attributes' definitions enable John to calculate the *CCI*. As D_{DS}=P_{DC}, E_{DS}=E_{DC}, $S_{DS} \neq S_{DC}$, and $R_{DS_{DC}} \neq R_{DC_{DC}}$, then $CCI = 6$. Thus, as CCI is equal to the cut score informed by John, and at this point, there is no norm addressed to John, then John has all elements to evaluate his intention defined by Eq. 7. First, the current beliefs enable John to follow his desire. Second, John's desire is compatible with Bank-B's terms, i.e., John will give his consent and, hence, John will be able to execute his plans as intended.

Since there is a valid consent term, Bank-B must follow what was proposed and respect the obligations foreseen in the data regulation. In order to represent the data regulation obligations, permissions, and prohibitions, Table 6 shows a group of norms proposed to this use case scenario following the format defined by Eq. 5. As well as the DS agent, from

[5] https://github.com/phalves/ConFIA/blob/main/Open_Banking_Scenario.ipynb

time to time, the DC agent will verify if a new norm is addressed to him, as depicted in Fig. 5. Then, the DC agent will verify if there is an active norm.

As described in the GoDReP scenario, after John gives his consent, he decides to revoke it. This action activates the *Consent Revocation* norm. Then, we will begin modeling the DC's BDI attributes and the environmental norms. Table 7 the DC agent (Bank-B agent) attributes.

The RegulAI architecture proposes constant beliefs and norms revision to verify if the sensor identifies any environment's change. This step will identify the Bank-B beliefs and the norms addressed to it. Next, the *Desires Generation* will identify which are the desires enabled considering the available beliefs.

In *Norms Status Evaluation*, Bank-B will identify that the *Consent Revocation* (CR) norm is active. In this sense, as Bank-B's desires are (i) *Avoid receiving sanctions and fines* and (ii) *Improve the reputation score*, then *NC* can be calculated as defined in Eq. 6. Moreover, Eq. 8 demonstrates the NC evaluation, i.e., *NC*=3 if Bank-B decides to fulfill the *Consent Revocation* norm, or *NC*=-1 if Bank-B decides to violate this norm; hence, Bank-B will decide to comply with this norm.

$$NC_{CR} = \begin{cases} 2+1-0, & \text{if Bank-B decides to fulfill it} \\ 2+0-3, & \text{otherwise} \end{cases} \tag{8}$$

Following the RegulAI architecture, the next step is selecting the plans considering *NC*. As Bank-B decides to obey *CR* norm, Bank-B will be able to execute all plans foreseen before. Thus, Bank-B has all elements to evaluate its intention defined by Eq. 7. First, the current beliefs enable Bank-B to follow its desires. Second, Bank-B's *NC* allows Bank-B to execute its plans. Then, Bank-B will perform the actions needed based on his plans.

Furthermore, we designed other norms for the Open Banking scenario. For instance, *Consent Renew* is an obligation norm that requires Bank-B to request new consent from DSs. The Brazilian Open Banking regulation sets that after twelve months DC must request DS to renew his consent; otherwise, the DC must revoke the DS's consent automatically. Moreover, if there is an update in any consent attributes, DC must also request a consent renewal.

Another designed norm is the *Data Breach* norms, which defines that Bank-B is prohibited from contributing actively or passively to a data breach incident. It means that Bank-B must provide security actions to avoid a data breach; otherwise, its reputation will decrease, and it will be a target for fines and sanctions.

Last but not least, the *Data Copy* norm was designed to mirror the data copy right foreseen in many data regulations, such as GDPR and LGPD. This norm sets John's right to request a copy of his data from Bank-B. As a right, this norm is optional to John, i.e., John is permitted to request his data.

In another scenario explored in this context, we considered that Bank-A states in Brazil and aims to open a new bank branch in EU. Hence, Bank-A must comply with EU and Brazilian financial regulations. Following GoDReP and the NMAS modeling, this new branch can be represented as an *Organization* entity. This environment requires Bank-A to: (i) change the norm's punishment to update the fines' values, and (ii) change the norm's deactivation related to the consent expiration date, i.e., the Brazilian Open Banking foresees that consent is valid for one year, whereas the EU Open Banking sets the limit of ninety days.

All fines' values must be updated to address the EU regulation. Moreover, the *Consent Renew* norm allows Bank-A to renew John's consent to continue accessing his data. As mentioned previously, the *Consent Renew* norm defines that Bank-A is obligated to send a renewal request if the previous consent is expired or there is an update in any consent term attributes. However, the EU Open Banking regulation sets that the consent is valid for ninety days, instead of 365 foreseen by Brazilian regulation.

VII. LIMITATIONS

A. GoDReP LIMITATIONS

As mentioned before, GDPR and LGPD recommend data anonymization, data minimization, and cryptography employment to safeguard personal data. First, many anonymization techniques could be applied, such as data masking, generalization, pseudonymization, data swapping, data perturbation, and synthetic data [50], [51]. However, GoDReP focused on informing which anonymization technique is applied to preserve the DS's privacy and not evaluating or recommending a specific technique.

Second, the data minimization mentioned in GDPR and LGPD requires that the collected data must be adequate, relevant, limited to the informed purpose, and restricted to what is necessary concerning the purposes that they are processed for [52] and [53]. Moreover, identifying the minimum data set to allow the DC and DP to collect and process data is not trivial and requires further in-depth study. Thus, as well as the evaluation of the data anonymization technique, the discussion of which is the most suitable data minimization method is out of our scope. Third, the cryptography techniques are also subjects to be discussed on behalf of the DS's privacy, and many studies have presented different approaches to explore this area, e.g., [54], [55], and [56]. However, this evaluation deviates from the central subject of this article.

Third, although GoDReP is designed to use the CM based on LGPD and GDPR, GoDReP could be employed in use case scenarios based on other data regulations, but the ontology alignment is required to adapt the CM. As GoDReP proposes the evaluation of data privacy regulation and the development of use case scenarios, to use it correctly it is recommended the participation of at least one person from the Law sector and one from the IT sector or someone with programming skills. Even though this article considered the open banking application domain, other scenarios would require the development of new functions or even changing its structure. From

TABLE 6. Brazilian open banking norms.

Norm Att	Consent Request	Consent Revocation	Consent Renew	Data Breach	Data Copy
Addressees	Bank-B	Bank-B	Bank-B	Bank-B	John
Deontic Concept	Permission	Obligation	Permission	Prohibition	Permission
Rewards	Access to DS's data	Reputation +1	Continue accessing	None DS's data	Reputation +1
Punishments	None	Reputation -3. Fine 10.000	Reputation -4. Fine 10.000	Reputation -9. Fine 20.000	Reputation -2. Fine 5.000
Activation	When requested by a DS	When requested by DS	After 90 days, or there is a purpose update	When Bank-B access DS's data without consent	When requested by DS
Deactivation	When DS revokes or 365 days	When data collection stops	When DS decides to renew or not	When Bank-B fix the open breach	When John receive the requested data
Purpose Limitation	Account creation	Access revocation	Access to DS's	N/A data	Access financial data only
Application Domain	Open Banking	Open Banking	Open Banking	Open Banking	Open Banking

TABLE 7. Bank-B as a normative BDI agent.

Beliefs (B_B)	*Bank-B is open to receiving new accounts request*
	John gave his consent
	John request consent revocation
	Bank-B reputation is 0
Desires (D_B)	*Avoid receiving sanctions and fines*
	Improve the reputation score
Intentions (I_B)	*it will be generated after the norms evaluation*
Plans ($Plans_B$)	*Revoke John's consent immediately if requested*
	Stop collecting and processing John's data if John withdraws his consent
	Stop sharing John's data with third parties if John withdraws his consent

the performance perspective, GoDReP does not expect a high volume of data to process, but DSs, DCs, and DPs should be aware that this can be an issue to be evaluated when dealing with a high amount of data, or scaling GoDReP to an industry-like solution. In summary, GoDReP's complexity depends on its users' legal and programming skills.

Fourth, besides the scenario's application domain, other data regulations may present differences in its structure. HIPAA and PIPEDA [18] are examples of other data regulations. As well as the domain application, in case of changing the regulation jurisdiction, we highly recommend the participation of people from the Law and IT sector to perform changes in the GoDReP scenarios.

Finally, other Legal Bases than Consent could be explored. To do so, the selected Legal Basis entities and relationships should be identified to enable GoDReP employment properly.

B. RegulAI LIMITATIONS

RegulAI aims to represent the scenarios elaborated using GoDReP by addressing data regulation concerns in NMAS. However, to work correctly, the agent's desires and goals must be compared with the consent's purpose. However, since both desires and purposes are expressed in natural language, the automatic comparison may be challenging. A possible solution would be the usage of communication templates with a limited vocabulary to represent these sentences as program commands. Otherwise, the comparison would really focus solely on Natural Language Processing techniques.

Furthermore, eventually, norms can conflict, and this article does not propose a normative conflict resolution in this case. However, there are numerous normative resolution techniques, and they require an in-depth study focused on this point.

Last but not least, as well as mentioned as a GoDReP's limitation, this article is focused on the Consent Legal Basis. However, we do not evaluated other Legal Basis that could benefit from GoDReP, and RegulAI proposals, if applicable. Another similar limitation is changing the data regulation, which was not considered in this article. One could argue that there are other data regulation, or NMAS, relevant aspects that were not emerged and addressed in our approach.

VIII. CONCLUSION AND FUTURE WORK

In this article, we proposed a CM based on three ontologies: (i) PrOnto, (ii) GConsent, and (iii) ODPM. This metamodel aims to support the GoDReP scenarios generation, offering to DSs, DCs, and DPs knowledge of the essential consent elements and their relationships. GoDReP was built to allow data agents to describe use case scenarios and deliberate on the possible data regulation interpretation using first-order logic sentences to verify the scenario's compliance. Moreover, the scenarios developed with GoDReP are data that contribute to expectations alignment between the agents involved, and as an object of discussion related to the interpretation in other jurisdictions. Additionally, these notebooks can influence in the decision's interpretation regarding a case.

Based on the scenario description developed in GoDReP, RegulAI enables data agents to represent their goals, plans, and environmental norms by employing BDI reasoning architecture in a NMAS to express data regulation concerns and expectations regarding the collection, storage, and use of their data. The BDI architecture represents the agent's preferences, and the NMAS defines the data regulation norms that agents must evaluate whether they comply with or not, considering the norm's rewards and punishments.

RegulAI defines a CCI to aid DS agents in evaluating their preferences versus the consent term purpose. Once the preferences are aligned with the consent term purpose, the CCI will return a number, and the DS agent will choose whether to share personal data based on the minimum score defined previously.

For future work, Natural Language Processing (NLP) and Machine Learning (ML) techniques would be applied to evaluate the consent's purpose and the agent's goals and plans to improve the compatibility between them. For instance, NLP and ML can be used in healthcare to analyze the language used in consent forms and patient communication, identify gaps in information, and personalize consent based on patient preferences or limitations. This improves the compatibility between patient consent purposes and the agent's goals. Another future work is developing an in-depth study on the reputation systems to improve the agent's reputation capabilities.

Furthermore, as mentioned in the limitation section, norms may conflict, and deciding which norm to comply with is not trivial. Thus, other future work is on the normative resolution direction. Last but not least, RegulAI would be used, for instance, to monitor systems and notify DSs, DCs, and DPs when a data breach occurs or the DS's personal data is used inappropriately.

REFERENCES

[1] N. Anciaux, P. Bonnet, L. Bouganim, B. Nguyen, P. Pucheral, I. S. Popa, and G. Scerri, "Personal data management systems: The security and functionality standpoint," *Inf. Syst.*, vol. 80, pp. 13–35, Feb. 2019.

[2] C. Mulholland and I. Z. Frajhof, *A LGPD EO Novo Marco Normativo no Brasil*, 1st ed. Scottsdale, AZ, USA: Arquipelago, 2020.

[3] D. A. Tamburri, "Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation," *Inf. Syst.*, vol. 91, Jul. 2020, Art. no. 101469.

[4] J. Breuer and J. Pierson, "The right to the city and data protection for developing citizen-centric digital cities," *Inf., Commun. Soc.*, vol. 24, no. 6, pp. 797–812, Apr. 2021.

[5] M. Stoilova, R. Nandagiri, and S. Livingstone, "Children's understanding of personal data and privacy online—A systematic evidence mapping," *Inf., Commun. Soc.*, vol. 24, no. 4, pp. 557–575, Mar. 2021.

[6] J. Wolff and N. Atallah, "Early GDPR penalties: Analysis of implementation and fines through May 2020," *J. Inf. Policy*, vol. 11, pp. 63–103, Dec. 2021.

[7] T. Dougherty, "Informed consent, disclosure, and understanding," *Philosophy Public Affairs*, vol. 48, no. 2, pp. 119–150, Mar. 2020.

[8] I. Varici, "The relationship between information asymmetry and the quality of audit: An empirical study in Istanbul stock exchange," *Int. Bus. Res.*, vol. 6, no. 10, p. 132, Sep. 2013.

[9] M. A. Naheem, "Risk of money laundering in the U.S.: HSBC case study," *J. Money Laundering Control*, vol. 19, no. 3, pp. 225–237, Jul. 2016.

[10] L. F. Cranor, P. Guduru, and M. Arjula, "User interfaces for privacy agents," *ACM Trans. Comput.-Hum. Interact.*, vol. 13, no. 2, pp. 135–178, Jun. 2006.

[11] R. Berjon, "The fiduciary duties of user agents," *SSRN 3827421*, pp. 1–15, Apr. 2021.

[12] M. Wooldridge, *An Introduction to Multiagent Systems*. Hoboken, NJ, USA: Wiley, 2009.

[13] Y. Shang, "Consensus formation in networks with neighbor-dependent synergy and observer effect," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 95, Apr. 2021, Art. no. 105632.

[14] P. Alves, F. Correia, I. Frajhof, C. S. D. Souza, and H. Lopes, "A normative multiagent approach to represent data regulation concerns," in *Proc. 15th Int. Conf. Agents Artif. Intell.*, 2023, pp. 330–337.

[15] M. Wooldridge, "Intelligent agents," in *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*, vol. 1. Cambridge, MA, USA: MIT Press, 1999, pp. 27–73.

[16] R. A. Posner, *Economic Analysis of Law*. Boston, MA, USA: Aspen Publishing, 2014.

[17] E. Goldman, "An introduction to the California consumer privacy act (CCPA)," Legal Studies Research Paper, Santa Clara Univ., Santa Clara, CA, USA, Tech. Rep., 2020, doi: 10.2139/ssrn.3211013.

[18] D. Xiang and W. Cai, "Privacy protection and secondary use of health data: Strategies and methods," *BioMed Res. Int.*, vol. 2021, pp. 1–11, Oct. 2021.

[19] M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst, and Y. Qiao, "Visual surveillance within the EU general data protection regulation: A technology perspective," *IEEE Access*, vol. 7, pp. 111709–111726, 2019.

[20] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[21] P. Silva, E. Monteiro, and P. Simões, "Privacy in the cloud: A survey of existing solutions and research challenges," *IEEE Access*, vol. 9, pp. 10473–10497, 2021.

[22] L. H. Iwaya, G. H. Iwaya, S. Fischer-Hübner, and A. V. Steil, "Organisational privacy culture and climate: A scoping review," *IEEE Access*, vol. 10, pp. 73907–73930, 2022.

[23] L. Böck, M. Fejrskov, K. Demetzou, S. Karuppayah, M. Mühlhäuser, and E. Vasilomanolakis, "Processing of botnet tracking data under the GDPR," *Comput. Law Secur. Rev.*, vol. 45, Jul. 2022, Art. no. 105652.

[24] A. Rossi and G. Lenzini, "Transparency by design in data-informed research: A collection of information design patterns," *Comput. Law Secur. Rev.*, vol. 37, Jul. 2020, Art. no. 105402.

[25] P. J. van de Waerdt, "Information asymmetries: Recognizing the limits of the GDPR on the data-driven market," *Comput. Law Secur. Rev.*, vol. 38, Sep. 2020, Art. no. 105436.

[26] M. Luck, S. Mahmoud, F. Meneguzzi, M. Kollingbaum, T. J. Norman, N. Criado, and M. S. Fagundes, "Normative agents," in *Agreement Technologies*. Cham, Switzerland: Springer, 2013, pp. 209–220.

[27] J. S. Santos, J. O. Zahn, E. A. Silvestre, V. T. Silva, and W. W. Vasconcelos, "Detection and resolution of normative conflicts in multi-agent systems: A literature survey," *Auto. Agents Multi-Agent Syst.*, vol. 31, no. 6, pp. 1236–1282, Nov. 2017.

[28] P. H. C. Alves, M. L. Viana, and C. J. P. D. Lucena, "An architecture for autonomous normative BDI agents based on personality traits to solve normative conflicts," in *Proc. 10th Int. Conf. Agents Artif. Intell.*, 2018, pp. 80–90.

[29] Y. Shang, "Resilient consensus for expressed and private opinions," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 318–331, Jan. 2021.

[30] B. F. dos Santos Neto, V. T. da Silva, and C. J. P. de Lucena, "Developing goal-oriented normative agents: The NBDI architecture," in *Agents and Artificial Intelligence*, J. Filipe and A. Fred, Eds. Berlin, Germany: Springer, 2013, pp. 176–191.

[31] K. Fatema, E. Hadziselimovic, H. J. Pandit, C. Debruyne, D. Lewis, and D. O'Sullivan, "Compliance through informed consent: Semantic based consent permission and data management model," in *Proc. PrivOn@ ISWC*, 2017, pp. 1–16.

[32] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, and L. Robaldo, "PrOnto: Privacy ontology for legal reasoning," in *Electronic Government and the Information Systems Perspective*, A. KHo and E. Francesconi, Eds. Cham, Switzerland: Springer, 2018, pp. 139–152.

[33] H. J. Pandit, C. Debruyne, D. O'Sullivan, and D. Lewis, *GConsent—A Consent Ontology Based on the GDPR BT—The Semantic Web*. Cham, Switzerland: Springer, 2019, pp. 270–282.

[34] M. Gharib, P. Giorgini, and J. Mylopoulos, "COPri v.2—A core ontology for privacy requirements," *Data Knowl. Eng.*, vol. 133, May 2021, Art. no. 101888.

[35] P. Alves, I. Frajhof, F. Correia, C. de Souza, and H. Lopes, "Controlling personal data flow: An ontology in the COVID-19 outbreak using a permissioned blockchain," in *Proc. 23rd Int. Conf. Enterprise Inf. Syst.*, 2021, pp. 173–180.

[36] B. F. D. Santos Neto, V. T. D. Silva, and C. J. de Lucena, "Developing goal-oriented normative agents: The NBDI architecture," in *Proc. Int. Conf. Agents Artif. Intell.* Cham, Switzerland: Springer, 2011, pp. 176–191.

[37] F. Cunha, L. Marx, M. Rosemberg, and C. Lucena, "Verifying the behavior of agents in BDI4JADE with AspectJ," in *Proc. WESAAC*, 2015, pp. 1–6.

[38] A. Dubey, K. Abhinav, S. Jain, V. Arora, and A. Puttaveerana, "HACO: A framework for developing human-AI teaming," in *Proc. 13th Innov. Softw. Eng. Conf. Formerly Known India Softw. Eng. Conf.*, Feb. 2020, pp. 1–9.

[39] F. Bellifemine, A. Poggi, and G. Rimassa, "JADE—A FIPA-compliant agent framework," in *Proc. PAAM*, vol. 99. London, U.K.:, 1999, p. 33.

[40] E. S. S. Freire, M. I. Cortés, R. M. D. R. Júnior, E. J. T. Gonçalves, and G. A. C. D. Lima, "NorMAS-ML: Supporting the modeling of normative multi-agent systems," *ADCAIJ: Adv. Distrib. Comput. Artif. Intell. J.*, vol. 8, no. 4, pp. 49–81, 2019.

[41] M. Viana, P. Alencar, E. Guimarães, E. Cirilo, and C. Lucena, "Creating a modeling language based on a new metamodel for adaptive normative software agents," *IEEE Access*, vol. 10, pp. 13974–13996, 2022.

[42] E. J. T. Gonçalves, M. I. Cortés, G. A. L. Campos, Y. S. Lopes, E. S. S. Freire, V. T. da Silva, K. S. F. de Oliveira, and M. A. de Oliveira, ''MAS-ML 2.0: Supporting the modelling of multi-agent systems with different agent architectures,'' *J. Syst. Softw.*, vol. 108, pp. 77–109, Oct. 2015.

[43] M. A. Mahmoud, M. S. Ahmad, and S. A. Mostafa, ''Norm-based behavior regulating technique for multi-agent in complex adaptive systems,'' *IEEE Access*, vol. 7, pp. 126662–126678, 2019.

[44] S. Ma, C. Guo, H. Wang, H. Xiao, B. Xu, H. Dai, S. Cheng, R. Yi, and T. Wang, ''Nudging data privacy management of open banking based on blockchain,'' in *Proc. 15th Int. Symp. Pervasive Syst., Algorithms Netw. (I-SPAN)*, Oct. 2018, pp. 72–79.

[45] X. Vives, ''Digital disruption in banking,'' *Annu. Rev. Financial Econ.*, vol. 11, no. 1, pp. 243–272, Dec. 2019.

[46] G. S. Farrow, ''Open banking: The rise of the cloud platform,'' *J. Payments Strategy Syst.*, vol. 14, no. 2, pp. 128–146, 2020.

[47] A. Kurteva, T. R. Chhetri, H. J. Pandit, and A. Fensel, ''Consent through the lens of semantics: State of the art survey and best practices,'' *Semantic Web*, pp. 1–27, Sep. 2021.

[48] W. F. Clocksin and C. S. Mellish, *Programming in Prolog*, 5th ed. Berlin, Germany: Springer, 2003.

[49] B. Žarnić and G. Bašić, ''Metanormative principles and norm governed social interaction,'' *Revus. J. Constitutional Theory Philosophy Law/Revija Za Ustavno Teorijo Filozofijo Prava*, vol. 22, pp. 105–120, Jun. 2014.

[50] S. Murthy, A. Abu Bakar, F. Abdul Rahim, and R. Ramli, ''A comparative study of data anonymization techniques,'' in *Proc. IEEE IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2019, pp. 306–309.

[51] A. Majeed and S. Lee, ''Anonymization techniques for privacy preserving data publishing: A comprehensive survey,'' *IEEE Access*, vol. 9, pp. 8512–8545, 2021.

[52] E. Podda and F. Vigna, ''Anonymization between minimization and erasure: The perspectives of French and Italian data protection authorities,'' in *Proc. Int. Conf. Electron. Government Inf. Syst. Perspective*. Cham, Switzerland: Springer, 2021, pp. 103–114.

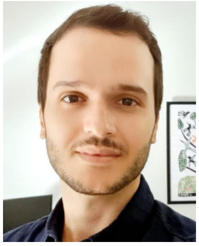
[53] M. S. Bargh, R. Meijer, S. van den Braak, A. Latenko, M. Vink, and S. Choenni, ''Embedding personal data minimization technologies in organizations: Needs, vision and artifacts,'' in *Proc. 14th Int. Conf. Theory Pract. Electron. Governance*, Oct. 2021, pp. 71–79.

[54] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, ''GDPR-compliant personal data management: A blockchain-based solution,'' *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1746–1761, 2020.

[55] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevicius, A.-A.-O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, ''Post-quantum era privacy protection for intelligent infrastructures,'' *IEEE Access*, vol. 9, pp. 36038–36077, 2021.

[56] K. Limniotis, ''Cryptography as the means to protect fundamental human rights,'' *Cryptography*, vol. 5, no. 4, p. 34, Nov. 2021.

PAULO HENRIQUE ALVES received the B.S. and M.S. degrees in information systems and artificial intelligence from Pontifical Catholic University of Rio de Janeiro (PUC-Rio), Brazil, in 2015 and 2017, respectively, where he is currently pursuing the Ph.D. degree in data science focused on personal data regulation. Since 2018, he has been with research and development projects in cooperation with insurance and oil and gas companies. His research interests include multiagent systems, norms, cognitive reasoning, blockchain, business process management, data privacy, and regulation.



FERNANDO CORREIA received the B.S. degree in computer engineering from State University of Feira de Santana (UEFS), in 2014, and the M.S. degree from Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 2017, where he received the Ph.D. degree in informatics, in 2022. He is a Researcher with ExACTa PUC-Rio initiative. His research interests include solving real-world problems with engineering and scientific relevance. He is particularly interested in information extraction, exploration, and the retrieval from a large collection of documents.

ISABELLA FRAJHOF received the B.L. degree from Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 2015, where she received the master's and Ph.D. degrees in theory of state and constitutional law, in 2018 and 2022, respectively. She is a Researcher with the Software Engineering Laboratory (LES) and Legalite PUC-Rio. She is a member of DROIT–Law and New Technologies Nucleo.

CLARISSE SIECKENIUS DE SOUZA graduated as a Translator and Conference Interpreter—English, French, and Portuguese from Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 1979, where she received the M.A. degree in Portuguese, in 1982, and the Ph.D. degree in computational linguistics, in 1987. In January 2020, she retired as a Full Professor from the Informatics Department of Rio de Janeiro's, PUC-Rio. After her retirement, as a Professor Emerita of PUC-Rio, she continues to contribute to the university doing research in AI interpretability and explainability, in the philosophy of computing and technology, and in algorithmically-mediated social processes. She was a creator of semiotic engineering, the first full-fledged semiotic theory of HCI, and the Founder of The Semiotic Engineering Research Group (SERG), for a long time one of the world's leading research centers in computer semiotics. Because of her leadership in this field, she has been the recipient of several awards, such as the ACM SIGDOC Rigo Award, in 2010, the ACM SIGCHI CHI Academy Award, in 2013, the IFIP TC13 Pioneers of HCI Award, in 2014, and the Scientific Merit Award from the Brazilian Computer Society, in 2016.

HELIO LOPES received the bachelor's degree in computer engineering, the master's degree in informatics, and the Ph.D. degree in mathematics from Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 1990, 1992, and 1996, respectively. He is currently an Associate Professor with the Department of Informatics, PUC-Rio. He is the Principal Investigator with the Data Science Laboratory (DASLAB) and the ExACTa initiative (Agile Experimentation, Co-Creation, and Digital Transformation). He is also a Co-Coordinator with the GALGOS Laboratory (optimization algorithms for decision making) and a Colaborator with the IDEIAS Laboratory (computer–human interactions, visualization, and user-experiences). His current research interests include data science, machine learning, and process mining. He has also interest in promoting innovation programs for Industrial Digital Transformation. He is a member of the Brazilian Computer Society (SBC) and the Brazilian Society of Applied and Computational Mathematics (SBMAC). He was elected for three times the President of the Special Interest Group of Computer Graphics and Image Processing (CEGRAPI), SBC, from 2006 to 2007, from 2013 to 2015, and from 2015 to 2017. In 2017, he received the Business Process Intelligence Challenge (BPIC) Best Report Award from the Academic Category. He was the General Co-Chair with SIBGRAPI, in 2017 and 2019, and he was the Program Co-Chair with SIBGRAPI, in 2007. In SIBGRAPI 2020, he was one of the invited speakers. He is an Associate Editor of the journals, *Computers and Graphics* and IEICE *Nonlinear Theory and its Applications* (NOLTA).

• • •