





A Normative Multiagent Approach to Represent Data Regulation Concerns

Paulo Henrique Alves¹^a, Fernando Alberto Correia¹^b, Isabella Zalcberg Frajthof²,
Clarisse Sieckenius de Souza¹^c and Helio Lopes¹^d

¹Department of Informatics, Pontifical Catholic University of Rio de Janeiro - PUC-Rio, Rio de Janeiro, Brazil

²Law Department, Pontifical Catholic University of Rio de Janeiro - PUC-Rio, Rio de Janeiro, Brazil
{palves, fjunior, clarisse, lopes}@inf.puc-rio.br, isbellazfrajhof@puc-rio.br

Keywords: Normative Agents, Multiagent Systems, Data Regulation, Open Banking.

Abstract: Data protection regulation is crucial to establishing the appropriate conduct in sharing and maintaining personal data. It aims to protect the Data Subjects' data, and to define Data Controllers' and Processors' obligations. However, modeling systems to represent and comply with those regulations can be challenging. In this sense, Multiagent System (MAS) presents an opportunity to overcome this challenge. MAS is an artificial intelligence approach that enables the simulation of independent software agents considering environmental variables. Thus, combining data regulation directives and Normative MAS (NMA) can allow the development of systems among distinct data regulation jurisdictions properly. This work proposes the DR-NMA (Data Regulation by NMA) employing Adaptive Normative Agent - Modeling Language (ANA-ML) and a Normative Agent Java Simulation (JSAN) extension to address data regulation concerns in an NMA. As a result, we present a use case scenario in the Open Banking domain to employ the proposed extensions. Finally, this work concludes that NMA can represent data regulation modeling and its application.

1 INTRODUCTION


Data protection regulation is crucial to establish the appropriate conduct in processing, sharing and maintaining personal data (Phillips, 2018). Governments have proposed data regulation bills to protect their citizens. Such action aims to set the rules so that companies, markets, and general businesses are able to process personal data in a respectful and safe manner. The Europe Union (EU) General Data Protection Regulation (GDPR) is an example of such legislation, as well as the Brazilian General Data Protection Law (LGPD) in the Global South. (Erickson, 2018). These regulations aim to protect the Data Subjects (DSs) data by establishing citizens' rights, and Data Controllers (DCs) and Processors (DPs) obligations. However, modeling systems to represent and comply with those regulations can be challenging.


Multiagent Systems (MAS) is an artificial intelligence (AI) approach (Ferber and Weiss, 1999) that


enables the simulation of autonomous software agents in a shared environment (Wooldridge, 2009). Moreover, agents can present common, distinguished, or opposite goals in the same environment, and they can decide which goals they will try to achieve based on their beliefs and plans. For instance, the agents will cooperate with each other in a multi-robot system that operates in a warehouse environment. Conversely, in e-commerce systems, agents present opposite behaviors; while a seller software agent is trying to buy an object for a low price, another agent is attempting to sell it as expensive as possible (Van der Hoek and Wooldridge, 2008).


In this sense, Normative MAS (NMA) emerged as a possible solution to represent environmental norms in which agents will determine whether to comply with them or not. Also, norms enable the expression of deontic concepts (Hübner et al., 2002), rewards, and punishments, which can be used for representing data regulation concerns (López y López and Luck, 2002).

Thus, combining data regulation and NMA enables the development of systems where DS, DC, and DP act as software agents in a simulated environment. The NMA environment can support multiple data

^a <https://orcid.org/0000-0002-0084-9157>

^b <https://orcid.org/0000-0003-0394-056X>

^c <https://orcid.org/0000-0002-2154-4723>

^d <https://orcid.org/0000-0003-4584-1455>

regulation rules by norms application. This combination would aid companies in verifying in advance data regulation compliance when moving from one jurisdiction to another, and adjusting parameters. Last but not least, new agents and norms can be generated by different DSs and DCs to consider different time frames (Sycara, 1998).

Even though the NMAS literature presents few modeling approaches to represent normative agents, it lacks data regulation concerns when developing NMAS. In this sense, this work proposes the use of Adaptive Normative Agent - Modeling Language (ANA-ML) (Viana et al., 2022) and an extension of Normative Agent Java Simulation (JSAN) (Viana et al., 2015) to address data regulation particularities in an NMAS.

In this context, we propose employing the developed extensions in the Open Banking domain. The motivation for the Open Banking scenario is its particularities depending on the jurisdiction in which it is applied. Hence, it offers an adequate context to exemplify the application of different regulation requirements in the same application domain.

The remainder of this work is organized as follows. Section 2 defines the basic concepts used in this work. Section 3 presents the related work. Section 4 describes the modeling and the framework extension to represent normative agents under a data regulation perspective. Section 5 presents a use case scenario in the Open Banking application domain. Section 6 describes the limitations of this work. Finally, Section 7 presents our conclusions and future work.

2 BACKGROUND

2.1 Data Regulation

Data regulation aims to protect DS's data and settles DCs' and DPs' obligations to provide a secure and healthy data-processing-sharing environment. Depending on the jurisdiction, different Legal Basis to process personal data may apply that DCs and DPs may choose when managing personal data. For instance, GDPR presents six Legal Basis to process personal data, while LGPD presents ten. Consent is a Legal Basis that is commonly cited and used by DCs, even though there are other legal provisions that justify the processing of personal data. For example, consent is present in both the abovementioned regulations.

Consent is commonly used as a Legal basis by DCs to process personal data in digital platforms and services. The LGPD, for example, indicates that when

consent is used as a Legal Basis, DS must be informed and expressly consent when their data is shared with third parties. The same is true when the data processing purpose previously informed and consented by DS is altered from the original one. Moreover, consent is used and required for many actions such as marketing calls, messages, website cookies, or other tracking methods. Both GDPR and LGPD qualify how consent shall be manifested by DS (according to LGPD, consent must be given in a free, informed and distinct manner, according to a specific purpose). Also, DCs must inform DS in a clear, simple and direct manner the terms of the data processing, in order to allow DSs to decide to the best of their knowledge (Kadam, 2017).

This information is commonly informed in a Privacy Policy document, which should disclose basic information, such as: (i) purpose limitation; (ii) for how long this consent is valid; (iii) which the DPs are involved; (iv) what are the security policies, and (v) where the personal data is stored (Palmirani et al., 2018) (Pandit et al., 2019) (Alves et al., 2021). Moreover, DCs should provide the application domain particularities (i.e. Open Banking) in such document.

For instance, according to EU Open Banking guidelines, an Open Banking application should renew the DSs consent acceptance every 90 days. However, Brazilian Open Banking specifies that consent must expire in one year. Thus, defining a privacy policy and a consent term in compliance with data regulation can be challenging not only for lawyers but also for solution architects, which must guarantee the system's compliance with data regulation norms.

2.2 Normative Agents

Software agents are autonomous computer programs that can interact with other programs without human intervention (Wooldridge, 2009). In this context, social norms aim to organize this society generated by agents.

A norm specifies how agents should behave to live in society by defining rewards and punishments. Also, considering that a norm may conflict with an agent's individual goal, norms can represent social pressure upon the agent as well (Luck et al., 2013).

The authors in (López and Luck, 2003) and (López et al., 2004) presented a formal normative model based on autonomous agents' reasoning. Usually, there is more than one norm in MAS, and rarely are they isolated. In this sense, these authors proposed a model of a system of norms to guarantee that software agents will deliberate considering the entire system instead of a single norm.

Moreover, the authors in (Viana et al., 2022) present ANA-ML, a modeling language based on a metamodel for adaptative normative software agents. Their metamodel was inspired by (López and Luck, 2003) and (López et al., 2004) to support the modeling of abstractions, such as adaptation.

Finally, as agents must identify norms as social concepts to allow them to perform their actions, the employment of data regulation norms is a challenge that NMAS can overcome to develop and simulate systems that suffer from diverse jurisdictions.

3 RELATED WORK

This section presents works found in the recent literature related to data protection modeling motivation and its application in the Open Banking domain. Also, this section mentions the importance of providing abstraction models to represent data regulation in different contexts and jurisdictions to aid DSs, DCs, and DPs in being aware of their rights and obligations.

Phillips (Phillips, 2018) mentions that data regulation has become a remarkable barrier to sharing personal data over international borders. This work highlights the importance of developing an abstraction to model systems suitable in different jurisdictions that are adaptable to different data regulations. For instance, Phillips mentions the importance of respecting multiple data regulations simultaneously in sharing health data to improve global studies related to HIV and AIDS. In this sense, the NMAS paradigm could be used to develop systems that support multiple data regulations.

The data subject awareness is also a concern, and, regarding that matter, Dougherty (Dougherty, 2020) presents a selection of remarkable factors for DSs to consider before giving their consent. This work mentions that DCs and DPs are obligated to disclose information for transparency. This transparency aims to clarify the DCs and DPs' goals to aid DSs in deciding adequately. In this sense, NMAS would express norms and simulate a regulated environment which may elucidate the consequences of accepting a consent term.

Still, Stoilova et al. (Stoilova et al., 2021) present a systematic mapping regarding the DS perception of personal data and privacy. The authors highlighted that DSs usually do not fully understand essential elements in the consent term, such as their rights. Therefore, it shows the importance of sandboxing a consent term to understand rights and obligations better. Sandbox systems would be developed following the NMAS approach, starting from its model generation,

and then creating an NMAS following the JSAN extension proposed in this work.

In regards to the Open Banking domain, Farrow (Farrow, 2020) argues that PSD2 (Payments Services Directive) should be applied in the Open Banking environment. To do so, PSD2 should be translated into the country's law terms to offer data management and vendor integration. However, financial institutions must adapt PSD2 to different jurisdictions. For instance, a technical service provider offers services on behalf of a financial institution and provides the necessary technological components to execute PSD2 services. This provider might be in a different jurisdiction and may suffer from more than one data regulation. Thus, modeling and developing NMAS is necessary to deliver data regulation concerns.

Moreover, in order to promote transparency in the Open Banking environment, the authors in (Mukhopadhyay and Ghosh, 2021) propose a consortium blockchain to deliver data process transparency in the Open Banking environment to aid DSs in making decisions about providing or withdrawing consent. However, they do not provide distributed concerns when sharing data worldwide. NMAS would aid distributed systems, e.g., blockchain-based solutions and Open Banking applications, to simulate regulation compliance in different jurisdictions.

A frequent burden when dealing with AI is the opacity of the solution returned by these types of systems. Zednik (Zednik, 2021) proposes a normative framework to allow Explainable AI in order to mitigate the opacity of AI systems. The normative framework shows that analytic techniques are helpful for explainability. Thus, analogously, it indicates that an NMAS would be able to explain software agents' behavior in a data-regulated environment. This explanation can aid DSs in mitigating the data flow information asymmetry and, hence, provide DSs with material for better decision-making.

4 DATA REGULATED NORMATIVE AGENTS

Normative agents are simulation tools to experiment with different behaviors in one or more application domains (Luck et al., 2013) (Alves et al., 2018). These agents are independent, they can act based on their perception of the environment and on the consequences of complying or not within a norm. Given the broad use case possibilities when dealing with data regulation and worldwide data regulations, the NMAS paradigm can be an option to model systems that suffer from data regulation impact.

Considering consent as a data regulation Legal Basis for this study, agents can decide whether to accept a consent term based on the environmental norms and their goals. Moreover, a company in Europe Union (EU), i.e., regulated by GDPR, may decide to expand their business to Brazil; if so, the consent term should be updated to consider also LGPD. After modeling the LGPD norms, an NMAS can simulate the new environment and verify the agents' norms adoption.

4.1 Modeling Regulation-Based Normative Agents

NMASs allow the development of systems and simulation scenarios based on an application domain. ANA-ML is a Universal Modeling Language (UML) extension developed to model agents' behavior based on environmental norms (Viana et al., 2022). ANA-ML defines the following elements:

- **Environment**, i.e., available data to inspire agents to select their plans and execute their actions,
- **Agent**, i.e., a software agent with its goal, beliefs, desires, and intentions,
- **Agent Role**, i.e., a software agent role with its obligations,
- **Norm**, i.e., activation, expiration, state, rewards, punishments, and addressed agents data to employ a norm.
- **Organization**, i.e., a group of software agents that will present interaction.

As depicted in Figure 1, the DR-NMAS (Data Regulated - Normative Multiagent System) is a model generated using ANA-ML for the data regulation's applications. In the data regulation context, User Agents act as DSs, Company A acts as a DC, and it also can act as a DP or outsource another company to execute the DP role. A Legal Basis comprises one or more Data Regulations and their particularities. For instance, consent is one Legal Basis foreseen in GDPR and LGPD. An Organization groups the agents by roles and sets the domain singularities, and depending on the application domain, other Legal Basis should be considered.

A data-regulated environment provides data for agents to consider when generating their plans and executing their actions. For instance, a DS agent may identify that its consent is expired, i.e., the DC agent is prohibited from collecting the DS agent data but still doing it. As a result, the DS agent decides to request a consent revocation. The DS agent behavior is a workaround when a DC agent fails to comply with a Data Regulation Norm.

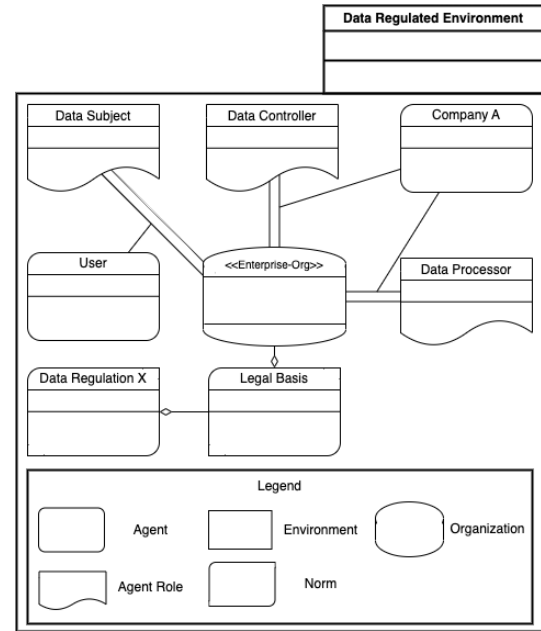


Figure 1: Data Regulated - Normative Multiagent System.

4.2 Agent-Based Data Regulation Framework

Based on the DR-NMAS model, this work proposes an extension of JSAN 2.0 (Viana et al., 2015) to consider the data regulation concerns, as depicted in Figure 2. The green box represents the new entities, and the blue box represents a modified entity. On this new extension, *DataSubject* and *DataController* are frozen spots, i.e., every data-regulated scenario requires this structure. Analogously, *LegalBasis* and *ConsentTerm* are entities required in such an environment. As mentioned before, as *DataProcessor* as *OtherLegalBasis* are optional and can be instantiated depending on the use case scenario. Finally, as presented in the DR-NMAS model, the *EnvironmentSimulation* entity must inform which data regulation will be considered in the simulation.

The *LegalBasis* entity specifies agents and the application domain particularities. For instance, in the Open Banking context, GPDR defines that consents should be valid for 90 days at most; hence, DCs must request approval from DSs every 90 days. However, if the environment simulation is based on LGPD, the consent term is valid up to 1 year¹. Thus, the JSAN extension allows the development of compliance simulations when changing the application domain or

¹GDPR and LGPD Open Banking contrast. Available at: <https://www.openbankingexcellence.org/blog/the-implementation-journey-of-open-banking-rules-in-brazil/>. Accessed on November 15, 2022.

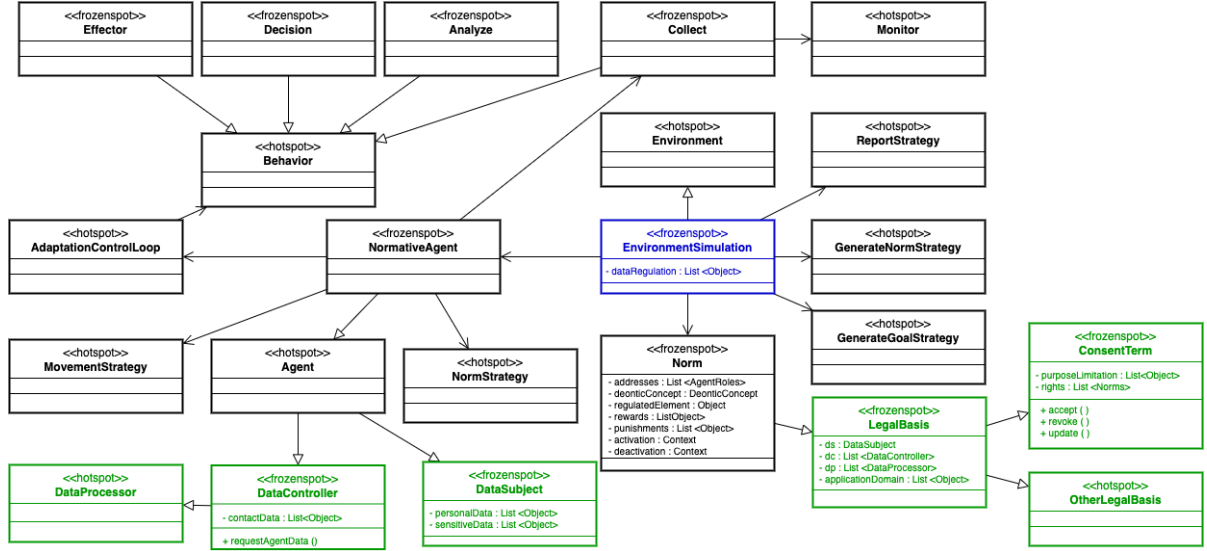


Figure 2: JSAN extension.

data regulation jurisdiction.

Table 1 shows norm examples that must be developed when the DC agent has a valid consent, accepted by a DS agent. *DataCopy* is a DS right, i.e., DS has a *permission* to request a copy of their data anytime. Conversely, the *Revocation* is a DC obligation when a DS requests to revoke its consent. *Rewards* and *Punishments* were defined arbitrarily, which impacted the DC agents' reputation and also settled fines to be paid. DS agents may not share their data with this organization if a DC has a bad reputation. These norms are activated by a DS agent request. However, the *Revocation* norm presents other two triggers: (i) if it is expired, i.e., it approached the date time limit, or (ii) there is a new consent term version, i.e., the old consent term was updated, then DC must request a new acceptance from DSs. They are deactivated based on different triggers. For example, *DataCopy* is deactivated when DS receives the requested data, and *Revocation* is deactivated when DC stops collecting DS's data.

Table 1: Data copy and consent revocation norms.

Norm Attribute	Data Copy	Revocation
Addresses	DS	DC
Deontic Concept	Permission	Obligation
Rewards	Get DS's Data	Reputation +1
Punishments	None	Reputation -3 Fine 10.000
Activation	By DS request	By DS request
Deactivation	DS received requested data	Stops data collection

The consent Legal Basis presents other rights and

obligations that DS, DC, and DP agents must comply with. For example, GDPR foresees the right to be forgotten, and LGPD foresees data deletion. i.e., the data must be not available after the DS's request. The goal is the same from the DS and DP perspective, the data is no longer available for use, but a person from the Law domain should evaluate accurately to verify if there is a relevant difference before creating the multi-agent environment norms.

Other data regulations may present different approaches to allow a healthy relationship environment, such as HIPAA and PIPEDA (Xiang and Cai, 2021), and agent norms are objects that will enable this representation systematically.

5 OPEN BANKING USE CASE

Open banking enables knowledge exchange between financial institutions based on the DS data. For example, a DS can request a loan from bank A, a credit card from bank B, and trade assets in the stock market from bank C. There are other benefits, e.g., a DS can open a new account at bank B by importing his data from a previous account at bank A. In this sense, Open Banking aims to improve the data sharing capabilities, allowing the DS to select when, for how long, and with whom its financial data will be shared.

It is important to observe that DS can revoke its consent at anytime. To do so, DS should access bank A's communication channels and request consent revocation. Usually, there is no limitation for how long DC will collect data; however, the Open Banking domain presents a particularity. As mentioned before,

depending on the jurisdiction, the data sharing will be stopped after a different time range. For instance, EU sets ninety days, and Brazil determines twelve months.

This use case proposes a DR-NMAS model to simulate an EU bank (BankFoo) that aims to open a new branch and offer financial services in Brazil. First, Figure 3 depicts the DR-NMAS model for the Open Banking scenario. Then, Tables 2, 3, and 4 illustrates the norms proposed for this environment.

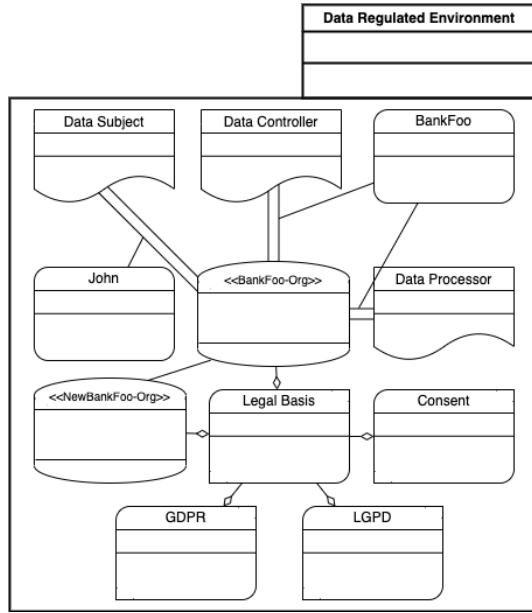


Figure 3: Open Banking DR-NMAS.

In this use case, we considered that BankFoo states in the EU and aims to open a new bank branch in Brazil. Hence, BankFoo must comply with EU and Brazilian financial regulations. Still, we use the Consent Legal Basis for this use case as a demonstrative purpose. Next, BankFoo has to define a consent term, which means creating a norm. Table 2 and Table 3 show the consent norms' attributes and values.

The Consent Request norm allows John to accept sharing his financial data with BankFoo if it is his wish. Next, the Consent Revocation norm allows John to stop sharing his data with BankFoo if he wants to do so. Then, the Consent Renew norm allows BankFoo to renew John's consent to continue accessing his data. BankFoo is *obligated* to send this request if the previous consent is expired or there is a new purpose limitation. Next, Data Breach is a *prohibited* action. This norm defines that if there is a data breach, BankFoo will be punished. Last but not least, Data Copy is a norm that represents the DS' right foreseen in GDPR and LGPD. It *permits* DSs to request all their's data that BankFoo is controlling.

These norms can be generalized to be addressed to DSs that aim to share their data with BankFoo. Thus the DSs can accept or not this consent term, i.e., translating to a deontic concept, they have *permission* to accept. Moreover, in this scenario, BankFoo acts as DC and DP, i.e., BankFoo is entirely responsible for dealing with and managing John's financial data.

Table 3 shows which norm's attributes had to be changed to employ them in compliance with the Brazilian regulation. Thus, BankFoo must update the attributes *Activation* and *Deactivation* from its consent term norm to comply with the jurisdiction where a new branch will be created. Following DR-NMAS, this new branch can be represented as an *Organization* entity.

Finally, Table 4 describes a compliance norm that will be activated if BankFoo does not update the *Activation* and *Deactivation* attributes on its new branch when defining the LGPD norm. This compliance norm states that consent is valid for one year, and BankFoo is prohibited from accessing John's data if there is no valid and active consent authorizing such action. Otherwise, BankFoo will receive a fine of two thousand Reais until getting the appropriate authorization.

Then, considering that John accepted the consent term sent by BankFoo, John requests a copy of his financial data from the old bank following the Data Copy Norm defined in Table 1. As it is a permission foreseen by the data regulation, John is able to proceed with this request, and there are no punishments if he does not claim it. Last but not least, if John regrets sharing his financial data, he can revoke his consent, and his data will not be collected anymore.

Therefore, this use case scenario materializes the concepts presented on the ANA-ML and JSAN extensions based on a specific application domain. Furthermore, the normative agents adequately represented the data regulation concerns. Developing application-based scenarios would aid DSs, DCs, and DPs in consolidating their concerns. Moreover, this simulation could be used to represent jurisprudence².

6 LIMITATIONS

Even though this work proposes a novel approach to illustrate data regulation concerns by normative

²Jurisprudence definition: "The word jurisprudence derives from the Latin term *juris prudentia*, which means 'the study, knowledge, or science of law'. In the United States, jurisprudence commonly means the philosophy of law". Available at: <https://www.law.cornell.edu/wex/jurisprudence>. Accessed on November 15, 2022.

Table 2: EU Open Banking Norms.

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

Table 3: Brazilian Diff Open Banking Norms.

Norm Att	Consent Request	Consent Revocation	Consent Renew	Data Breach	Data Copy
Rewards	Access to John's data	Reputation +2	Continue accessing John's data	None	Get John's Data
Punishments	None	Reputation -3 Fine 5.000	Reputation -4 Fine 5.000	Reputation -9 Fine 30.000	None
Activation	When accepted by John	When requested by John	After 356 days , or there is a purpose update	When BankFoo access John's data without consent	When requested by John
Deactivation	When John revokes, or 365 days	When data collection stops	When John decides to renew or not	When BankFoo fix the open breach	When John receives the requested data

Table 4: LGPD Compliance Norm.

Attribute	Value
Norm Name	Time Range Compliance
Addressee	DC
Deontic Concept	Prohibition
Rewards	None
Punishments	Fine 2.000
Activation	After 1 year of giving consent
Deactivation	After regularization
Application Domain	Open Banking
Purpose Limitation	Prevent unauthorized access
Rights	All foreseen by LGPD

MAS, some limitations should be considered. From the MAS perspective, as norms can conflict with each other, a conflict resolution approach should be considered, as presented in (Kasenberg and Scheutz, 2018). Different data protection regulations can also conflict from the law perspective, so NMA conflict resolution techniques would also be applied to overcome this challenge. Moreover, the Belief-Desire-Intention (BDI) agents with personality traits would be applied to provide intelligent agents into the NMA simulation (Alves et al., 2017; Alves et al., 2018).

From the Law perspective, this work considered the Consent Legal Basis only, as it is present in GDPR and LGPD. However, there are other Legal Basis fore-

seen in both regulations, and each one may present a different amount and definitions of Legal Basis.

Finally, as presented in (Zednik, 2021), the Explainable AI would be explored to provide not only DSs knowledge regarding the consent data sharing and processing clauses but also DCs and DPs requirements to deal with different data regulations and jurisdictions.

7 CONCLUSION

NMA literature foresees the usage of software agents to simulate social norms in order to provide an orchestrated and organized MAS. As normative agents are autonomous entities, they can decide to comply or not with the environmental norms depending on the rewards and punishment impact on their goals.

This work concludes that DR-NMA and the JSAN extension enable the representation of DSs, DCs, and DPs' rights, obligations, and behavior through normative software agents in a data-regulated environment. Moreover, the consent's Legal Basis requirements were transposed to MAS norms in the Open Banking scenario to allow stakeholders to

model agents' behavior.

For future work, a normative conflict resolution approach would be applied to solve conflicts generated operating more than one Legal Basis or more than one jurisdiction simultaneously, e.g., GDPR and LGPD. Moreover, developing an interface to allow DCs to expose themselves to a simulated data-regulated environment is another future work.

From the DCs and DP's perspectives, companies would try changing the jurisdiction and evaluate what must be changed to comply with the target data regulation. Lastly, other use case scenarios will be developed to improve the design of data-regulated NMAS.

REFERENCES

- Alves, P. H., Frajhof, I. Z., Correia, F. A., de Souza, C., and Lopes, H. (2021). Controlling personal data flow: An ontology in the covid-19 outbreak using a permissioned blockchain. In *Proceedings of the 23rd International Conference on Enterprise Information Systems - Volume 2: ICEIS*, pages 173–180. INSTICC, SciTePress.
- Alves, P. H. C., Viana, M. L., and de Lucena, C. J. P. (2017). Working towards a bdi-agent based on personality traits to improve normative conflicts solution. In *SEKE*, pages 531–534.
- Alves, P. H. C., Viana, M. L., and de Lucena, C. J. P. (2018). An architecture for autonomous normative bdi agents based on personality traits to solve normative conflicts. In *ICAART (1)*, pages 80–90.
- Dougherty, T. (2020). Informed consent, disclosure, and understanding. *Philosophy & Public Affairs*, 48(2):119–150.
- Erickson, A. (2018). Comparative analysis of the eu's gdpr and brazil's lgpd: Enforcement challenges with the lgpd. *Brook. J. Int'l L.*, 44:859.
- Farrow, G. S. (2020). Open banking: The rise of the cloud platform. *Journal of Payments Strategy & Systems*, 14(2):128–146.
- Ferber, J. and Weiss, G. (1999). *Multi-agent systems: an introduction to distributed artificial intelligence*, volume 1. Addison-wesley Reading.
- Hübner, J. F., Sichman, J. S., and Boissier, O. (2002). A model for the structural, functional, and deontic specification of organizations in multiagent systems. In *Brazilian Symposium on Artificial Intelligence*, pages 118–128. Springer.
- Kadam, R. A. (2017). Informed consent process: a step further towards making it meaningful! *Perspectives in clinical research*, 8(3):107.
- Kasenberg, D. and Scheutz, M. (2018). Norm conflict resolution in stochastic domains. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 32.
- López, F. L. y. and Luck, M. (2003). Modelling norms for autonomous agents. In *Proceedings of the Fourth Mexican International Conference on Computer Science, 2003. ENC 2003.*, pages 238–245. IEEE.
- López, F. L. y., Luck, M., and d'Inverno, M. (2004). Normative agent reasoning in dynamic societies. In *Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems, 2004. AAMAS 2004.*, pages 732–739. IEEE.
- López y López, F. and Luck, M. (2002). A model of normative multi-agent systems and dynamic relationships. In *Regulated agent-based social systems*, pages 259–280. Springer.
- Luck, M., Mahmoud, S., Meneguzzi, F., Kollingbaum, M., Norman, T. J., Criado, N., and Fagundes, M. S. (2013). Normative agents. In *Agreement technologies*, pages 209–220. Springer.
- Mukhopadhyay, I. and Ghosh, A. (2021). Blockchain-based framework for managing customer consent in open banking. In *The "Essence" of Network Security: An End-to-End Panorama*, pages 77–90. Springer.
- Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., and Robaldo, L. (2018). Pronto: privacy ontology for legal reasoning. In *International Conference on Electronic Government and the Information Systems Perspective*, pages 139–152. Springer.
- Pandit, H. J., Debruyne, C., O'Sullivan, D., and Lewis, D. (2019). GConsent - A Consent Ontology Based on the GDPR BT - The Semantic Web. pages 270–282. Springer International Publishing.
- Phillips, M. (2018). International data-sharing norms: from the oecd to the general data protection regulation (gdpr). *Human genetics*, 137(8):575–582.
- Stoilova, M., Nandagiri, R., and Livingstone, S. (2021). Children's understanding of personal data and privacy online – a systematic evidence mapping. *Information, Communication & Society*, 24(4):557–575.
- Sycara, K. P. (1998). Multiagent systems. *AI magazine*, 19(2):79–79.
- Van der Hoek, W. and Wooldridge, M. (2008). Multi-agent systems. *Foundations of Artificial Intelligence*, 3:887–928.
- Viana, M., Alencar, P., Guimarães, E., Cirilo, E., and Lucena, C. (2022). Creating a modeling language based on a new metamodel for adaptive normative software agents. *IEEE Access*, 10:13974–13996.
- Viana, M. L., Alencar, P. S., Guimarães, E. T., Cunha, F. J., Cowan, D. D., and de Lucena, C. J. P. (2015). Jsan: A framework to implement normative agents. In *SEKE*, pages 660–665.
- Wooldridge, M. (2009). *An introduction to multiagent systems*. John wiley & sons.
- Xiang, D. and Cai, W. (2021). Privacy protection and secondary use of health data: Strategies and methods. *BioMed Research International*, 2021.
- Zednik, C. (2021). Solving the black box problem: a normative framework for explainable artificial intelligence. *Philosophy & technology*, 34(2):265–288.