CLEI Electronic Journal, Volume 28, Issue 5, paper 4, September 2025

OntoPriv: Towards Designing a DPV-based Legal Ontology for Knowledge Retrieval and Compliance in Privacy Legislation

Gabriela Suntaxi*, Kelvin Ojeda, Francisco Rodríguez, Pablo del Hierro, Jorge Miño, Denys A. Flores
Departamento de Informática y Ciencias de la Computación
Escuela Politécnica Nacional, Quito, Ecuador
{*gabriela.suntaxi, kelvin.ojeda, francisco.rodriguez, pablo.delhierro, jorge.miño, denys.flores*}*@epn.edu.ec*

Abstract

In an increasingly digital world, protecting personal data has become a pressing global issue, prompting the creation of complex regulations aimed at safeguarding individuals' privacy. However, achieving compliance with these frameworks poses significant challenges for organizations, requiring a methodical and well-structured approach. In this context, OntoPriv was developed as a legal ontology tailored to support compliance with Ecuador's Organic Law on Personal Data Protection (LOPDP). OntoPriv serves as a systematic framework that not only clarifies legal obligations but also provides tools to strengthen privacy practices and encourage accountability. This extended work goes a step further by aligning OntoPriv with the Data Privacy Vocabulary (DPV), an internationally recognized W3C standard. This alignment significantly enhances OntoPriv's modularity, semantic depth, and interoperability, effectively connecting local and global data privacy frameworks. By integrating DPV, OntoPriv incorporates standardized concepts such as legal bases, purposes, and risk mitigation strategies. This ensures cross-jurisdictional compatibility and addresses prior challenges like limited interoperability and insufficient semantic connections. This integration positions OntoPriv as a powerful tool that facilitates automated compliance, comprehensive risk assessments, and improved data governance while fostering a shared understanding of privacy standards across different regions. This article discusses OntoPriv's development, the methodology for its alignment with DPV, and its implications for advancing data privacy compliance in Ecuador and beyond.

Keywords: data privacy, data protection regulation, GDPR, LOPDP, legal ontology, compliance, dpv, data privacy vocabulary

1 Introduction

Recent advancements in technology have led to an extraordinary increase in the generation, collection, and preservation of data for further analysis. This process occurs more rapidly regardless of the geographical location of the involved parties. Although there are clear technological innovations and business opportunities in the field of data analysis, ensuring data privacy poses significant difficulties. In fact, high-impact privacy incidents remain a threat, such as the Facebook-Cambridge Analytica scandal [2] and the LinkedIn data leak [3], whose global repercussion underscored the urgent need for robust data privacy standards and regulations to protect citizens. Data privacy and protection of personal information are currently considered as fundamental rights worldwide. Thus, different countries have proposed legal frameworks to guarantee data owners' privacy rights. Examples of such instruments are the European General Data Protection Regulation (GDPR) [4], the Brazilian General Personal Data Protection Act (LGPD) [5], and the Ecuadorian

*Corresponding author. This paper is an extended version of the work published in [1]. We extend our previous work by aligning OntoPriv with the Data Privacy Vocabulary, proposed by W3C, as explained in Section 6.

Organic Law of Personal Data Protection (LOPDP) [6], which aim to establish responsibilities and ensure the ethical handling of personal identifiable information (PII). As a result, PII can be protected during its collection, processing, storage, and disposal, making organizations accountable for its adequate handling, or facing financial sanctions for negligent non-compliance.

Compliance with personal data protection regulations is difficult as it challenges organizations worldwide that manage PII. Achieving compliance requires a systematic method to comprehend and implement data protection strategies and methodologies [7,8], along with a deep understanding of the legal obligations. These regulations are often intricate, comprising a range of conditions, objectives, interrelations, and scopes, which can render them complex and challenging to comply with [9]. Additionally, privacy and compliance efforts need coordination and communication among the various entities involved in the collection, processing, verification, and transfer of PII. Therefore, organizations are confronted with the dilemma of how to ensure compliance with these regulations despite their complexity. However, conventional methods for achieving compliance, such as manually interpreting legal documents and implementing policies in a piecemeal fashion, often prove to be inefficient. Likewise, the interpretation of such texts can vary greatly depending on the experts' interests, abilities, and experience. Alternatively, automation of compliance with personal data protection laws is quite complex. For instance, research in [10, 11] indicates that organizations struggle significantly with grasping the concept of compliance while executing measures to protect PII in line with these regulations. Consequently, data protection laws and their execution fail to meet the requirements, highlighting the need for innovative solutions to help organizations fill this gap. Semantic web technologies coupled with legal reasoning methods can aid and streamline this compliance process [12, 13]. In this context, the application of a formal specification of concepts and relationships, i.e., an ontology [14], could result in organized frameworks of legal knowledge to simplify the interpretation, analysis, application, and comprehension of data protection laws.

In this research, we explain the proposal of OntoPriv, a legal ontology to support the enforcement of data protection legislation; particularly, the Ecuadorian LOPDP, which came into effect in May 2023. OntoPriv is designed to help companies and data owners with queries about the rights and requirements to satisfy this legal framework. The particular contribution of our proposal relies on improving the communication between different actors involved in the collection, processing, verification, and transfer of PII. To further enhance the utility and interoperability of OntoPriv, this work extends our previous one [1] by aligning OntoPriv with the W3C's Data Privacy Vocabulary (DPV) for making OntoPriv a more robust and globally relevant tool for understanding and adhering to data protection regulations. This extension provides a standardized framework for representing data privacy concepts, including legal bases, purposes, risks, and rights. By exploring this alignment, future work can be devised to integrate DPV elements within OntoPriv. With this contribution, we aim to ensure compatibility with international standards, facilitate cross-jurisdictional compliance, and address gaps in our current ontology, such as the lack of detailed representations of automated decision-making queries, compliance with temporal aspects like retention periods, and other technical and operational gaps.

This paper is an extended version of the work published in [1]. This extended version introduces a significant enhancement by aligning OntoPriv with the internationally recognized Data Privacy Vocabulary (DPV). This alignment improves OntoPriv's modularity, semantic richness, and interoperability with global privacy frameworks, addressing limitations such as inconsistent terminology and restricted global applicability.

The outline of the article is described as follows. Section 2 outlines the background and related research, including a comparison of current personal data protection laws. Section 3 details the methodology utilized in our study. Sections 4 and 5 provide an overview of its implementation, including its methods for query processing, and OntoPriv evaluation. In Section 6, we describe the alignment of OntoPriv with DPV in order to discuss the challenges, limitations, use cases, and possible applications in Section 7. Finally, conclusions about our current findings and future research are presented in Section 8.

2 Background and Related Work

This section introduces the theoretical background and some related work about existing legal ontologies.

2.1 Personal Data Protection Legislation

Several personal data protection legislation have been proposed. The General Data Protection Regulation (GDPR) is the legal framework that aims to guarantee data privacy rights to individuals in the EU. In Latin America, Chile was the first country in the region to propose a law for personal data protection in 1999 [15]. Many countries have followed the example of the countries mentioned above and proposed similar legislation aiming to guarantee data privacy for their citizens. In Table 1, a comparison of personal data privacy legislation in Latin America is presented. Countries like Paraguay, Panama, and Ecuador have aligned their data protection legislation to the current GDPR. In our work, the Ecuadorian LOPDP is chosen due to its recent publication and its GDPR compatibility [15]. However, the methodology presented in this work can be followed (Section 3.2) to build a legal ontology based on any existing personal data protection legislation.

2.2 Ontologies

An ontology is a formal specification of a structured knowledge model that defines a system. It consists of entities and relationships [14] conceived from observations, which are useful for a shared conceptualization [31]. Solutions, such as databases or files, to store data can be considered instances of a knowledge model; however, they are designed to store data, not knowledge [32]. Hence, ontologies must have the following components to be considered as such [33]:

- **Classes:** each class in the ontology represents a concept, defining the domain of knowledge.
- **Properties:** are elements that are part of a class. Each class can have zero to more properties, and each property can belong to another class.
- **Relations:** are the connectors or semantic links that are present in the ontology. They can be bidirectional or unidirectional and are domain-specific.
- **Instances:** are the result of combining a class with its properties and relations. They represent a specific object within the ontology. Usually, an instance serves as an example of a real-life scenario that can be presented in the ontology.

If the domain of an ontology contains legal information, the ontology is known as *legal ontology*. Legal ontologies are helpful in designing legal knowledge systems, solving legal problems, and retrieving legal information.

2.3 Alignning OntoPriv with the Data Privacy Vocabulary (DPV)

DPV [34] provides a structured vocabulary for representing privacy concepts such as legal bases, purposes, and compliance tools. Aligning OntoPriv [1] with DPV enhances its interoperability with international standards. For instance, OntoPriv's class "LegalBasis" corresponds to DPV's "LegalBasis", enabling a clearer representation of data processing justifications. Additionally, concepts like "RiskMitigation" and "RetentionPeriod" in DPV complement OntoPriv by addressing gaps in risk analysis and temporal aspects. Additionally, DPV's modular approach facilitates the extension of OntoPriv's domain, integrating standardized terms to improve cross-jurisdictional applicability. Therefore, by adopting DPV elements, OntoPriv can be enhanced to support organizations in fulfilling compliance requirements while maintaining consistency across regulations. I.e., this alignment not only reinforces OntoPriv's usability but also fosters a unified understanding of widespread data privacy practices.

2.4 Related Work and Contribution

Geko et al. [35] built an ontology that addresses the relationships between GDPR and information security. This ontology focuses on the GDPR requirements that organizations have to fulfill to meet information security and leaves out any other information of the legislation. Similarly, GConsent [13] is an ontology that captures GDPR requirements that focus on data management consent, modeling relevant information associated with this scope. In [36], an ontology-based solution was proposed to improve the integration of data protection compliance into business process models. This study focused on the GDPR, highlighting the inclusion of GDPR requirements into business practices and operations using BPMN. Regarding legal aspects, in [12], an ontology based on the GDPR called PrOnto is proposed. This proposal focuses on providing legal knowledge to model privacy agents, rights, and data processing operations. Concluding, although various legal ontologies have been proposed, only few studies deal with personal data protection laws such as GDPR. Our research establishes an starting point which looks up Latin American laws such as the Ecuadorian LOPDP in order to model formal structures to query legal knowledge in search for answers about privacy compliance.

Table 1: Personal Data Protection Legislation in Latin America

Country	Name of the Law	Regulatory control authority	Members of the personal data protection system	Sanctions and violations	Publish Year
Argentina	Law of Personal Data Protection, Law No. 25,326 [16]	National Directory of Personal Data Protection	Data Owner, (Responsible for file, registry, or database), Data user	From 1,000 to 100,000 Argentine pesos From 6 months to 3 years in prison	Oct. 2000
Brasil	Brazilian General Personal Data Protection Act (LGPD) [17]	ANPD (National Data Protection Authority)	Data Owner, Treatment Agents, Control Authority, Data Controller, Operator	N/A	Aug. 2018
Chile	Natural Person Data Protection, Law No. 19628 [18]	Agency for Personal Data Protection	Data Owner, Responsible for the registry or data bank	Remuneration based on the severity of the offense according to article 173 of the Code of Civil Procedure.	Aug. 1999
Colombia	Treatment Policy and Data Protection [19]	The Superintendence of Industry and Commerce	Data Owner, Data Controller, Data Processor	N/A	Oct. 2012
Costa Rica	Law on Protection of the Person Against the Processing of their Personal Data [20]	Agency for Protection of Inhabitants' Data (Prodhab)	Data Owner (Interested), Responsible for the database	Minor: 5 basic salaries Serious: 5 to 20 basic salaries Very serious: 15 to 30 basic salaries and suspension of functions of 6 months.	Sep. 2011
Cuba	Law on Personal Data Protection, Law No. 149 [21]	N/A	Data Owner, Data Processor, Data Controller	20,000 Cuban pesos	Feb. 2023
El Salvador	Law on Personal Data Protection and Habeas Data [22]	N/A	Data Owner Data Processor, Data Controller,	Minor: 5 basic salaries Severe: 6 to 20 basic salaries Very serious: 21 to 50 basic salaries	Jun. 2019
Honduras	In elaboration process [23]	Institute for Access to Public Information (IAIP) - PRODATOS	N/A	N/A	N/A
Mexico	Federal Law on Personal Personal Data Protection in Possession of Private Parties [24]	INAI (National Institute of Transparency, Access to Information and Personal Data Protection)	Data Owner, Third Party, Responsible and Manager	From 100 to 320,000 Mexican pesos	Jul. 2010
Nicaragua	Personal Data Protection Law - Law No. 787 [25]	Directory of Personal Data Protection	Data Owner, Responsible for data files, Third party (Inspectors)	N/A	Mar. 2012
Panama	Personal Data Protection Law - Law No. 81 [26]	National Authority for Information Transparency and Access (ANTAI)	Control Authority, Recipient, Exporter, Regulator, Data Owner (applicant), Data Processor	Minor: 1,000 to 10,000 dollars Serious: are punished based on the type of crime by the ANTAI	May 2021
Paraguay	Data Protection Law Personal Credit, Law No. 6534 [27]	Nation Congress Paraguayan	Data Owner, Responsible Treatment and Manager of Treatment, User of credit information	From 15,000 to 6,000,000,000 guaranies From 5 to 6 months of disqualification from functions, depending on the severity of the offense committed	Oct. 2020
Peru	Peru's Personal Data Protection Law, Law No. 29733 [28]	General Directory of Personal Data Protection, attached to the Ministry of Justice	Data Owner, Database Owner, Treatment Manager, Data Processor, National Authority for Personal Data Protection	The application of fines is specified, but the amount or the application method is not indicated.	Jul. 2011
Republica Dominicana	Dominican Personal Data Law , Protection Law No. 172-13 [29]	Constitutional Court of the Dominican Republic	Affected or interested party, Recipient, Data Processor, Data Exporter, Data Importer, Identifiable person, Data Processor, Third party, Economic agents, Responsible for archiving, Data Owner, Debtor, Consumer, Data User, subscriber or affiliate.	From 10 to 150 minimum wages and from 6 months to 2 years in prison	Dic. 2013
Uruguay	Protection of Personal Data and Action of "Habeas Data", Law No. 18,331 [30]	Regulatory and Control Unit for Personal Data (URCDP)	Data Owner, Recipient, Data Processor, Third Party, Responsible for the database or processing, Data User	The application of fines of up to 15,000 indexed units and suspension of 6 business days or depending on the violation	Aug. 2008
Ecuador	Ecuadorian Organic Law of Personal Data Protection (LOPDP) [6]	National Directory of Public Records (Dinarp)	Data Owner, Data Controller, Data Processor, Recipient, Data Control Authority, Certification Entity, Delegate	Minor: 1 to 10 basic salaries Major: 10 to 20 salaries Private company: 0.1 to 1.0% of the business volume.	May 2021

3 Methodology

To develop our project, we applied Design Science Research (DSR) [37]. DSR is a paradigm that is used in problem-solving; its purpose is to improve human knowledge using the creation of innovative artifacts [37]. DSR has 6 phases, which are identified in Figure 1.

DSR Methodology

- **Phrase 1:** Problem Identification
  - Complex data protection compliance
  - Sistematic Literature Review SLR - Kitchenham (Section 3)
- **Phrase 2:** Objectives of a Solution
  - Ease the understanding of data protection regulations
  - Define OntoPriv
  - Evaluate OntoPriv
- **Phrase 3:** Design & Development (Section 4.2)
  - OntoPriv's Development - MOD-101 + Protégé
- **Phrase 4:** Demonstration
  - OntoPriv Querying Process - SQWRLTab (Section 4.3)
- **Phrase 5:** Evaluation
  - OntoPriv's Evaluation - OntoMetric (Section 5)
- **Phrase 6:** Communication

Figure 1: Project Methodology

3.1 Systematic Literature Review to Support Methodological Design

To support the design and evaluation of OntoPriv, a systematic literature review (SLR) was conducted following the guidelines proposed by Kitchenham et al. [38]. This review aimed to identify the most widely adopted methodologies, tools, and metrics used in ontology development and evaluation.

3.1.1 Research Questions

The SLR was guided by the following research questions:

- Q1: What methodologies are available for developing ontologies?
- Q2: Which is the most popular methodology used for evaluating ontologies?
- Q3: What tools are used for the development of ontologies?

3.1.2 Data Sources and Search Strategy

To ensure comprehensive coverage, six electronic databases were consulted: Google Scholar, IEEE Xplore, ACM Digital Library, SpringerLink, and Redalyc. Two search strings were designed to retrieve relevant literature for each thematic area:

- For development tools:
  `("ontology" OR "ontologies") AND ("tools" OR "software") AND "development"`
- For evaluation methods:
  `("ontology" OR "ontologies") AND ("evaluation" OR "metrics" OR "assessment")`

Search results were exported and screened for duplicates before moving on to relevance assessment.

3.1.3 Inclusion and Exclusion Criteria

The following criteria were applied during the selection of primary studies:

- **Inclusion:**

  - Peer-reviewed articles in English or Spanish
  - Studies addressing tools or evaluation methods for ontology engineering
  - Minimum of 6 pages in length
  - Clear methodological foundation
  - Published in recognized journals, conferences, or repositories
  - Scoring at least 5 out of 7 on a quality assessment checklist
- **Exclusion:**
  - Non-academic sources or gray literature
  - Duplicates or inaccessible texts
  - Studies not focused on ontology-related processes
  - Outdated works (older than 10 years unless considered seminal)

3.1.4 Study Selection and Iteration Process

The review followed a multi-stage filtering process (Figure 2):

1. **Initial Screening:** Titles and abstracts were reviewed for relevance.
2. **Full-Text Review:** Remaining articles were analyzed using the inclusion/exclusion criteria.
3. **Manual Analysis and Quality Assessment:** A manual, detailed analysis was performed on each article to extract relevant information and assess quality.
4. **Final Selection:** After applying the quality filters, a total of 27 articles were selected for in-depth analysis—these include studies addressing both ontology development tools and evaluation techniques, and they formed the evidence base for methodological decisions in the OntoPriv framework.

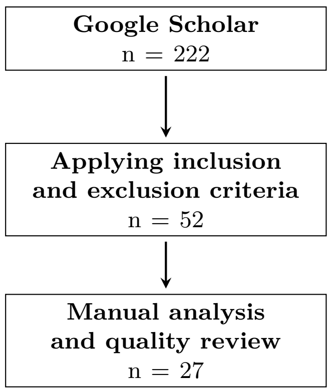


Figure 2: SLR Search Process

3.1.5 Key Findings

We conducted the SLR and answered questions Q1-Q3 based on the selected articles. The results of the SLR revealed the following findings:

1. The predominance of *Protégé* as the primary tool for ontology creation due to its flexibility, open-source nature, and support of OWL standards.
2. *OntoMetric*, *OntoClean*, and *OQuaRE* emerged as the most cited and applicable ontology evaluation frameworks. These tools aided the methodology selection (namely "Ontology Development 101") for the development and validation of OntoPriv.
3. This SLR became the basis for choosing the methodology and guided the design of the evaluation strategy using structured metrics and usability indicators.

These findings are discussed in detail as follows.

3.2 Ontology Development Methodology - Q1

Based on the results of the systematic literature review, a total of 36 distinct ontology development methodologies were identified. These methodologies vary in scope, complexity, and applicability depending on the context of use—ranging from lightweight prototyping to enterprise-level knowledge engineering. Among these, five methodologies stood out as the most frequently used and cited in the literature: *MOD-101* [39], *Methontology* [40], *NeOn* [41], *Upon* [42], and *TOVE* [43]. These approaches were selected based on frequency of appearance in peer-reviewed sources, citation impact, and applicability to different ontology engineering scenarios. MOD-101, in particular, was chosen for this project due to its clarity, and tool compatibility (e.g., Protégé) [44]. Table 2 summarizes the main characteristics of these methodologies.

Table 2: Comparison of Ontology Development Methodologies

Methodology	Key Features	Advantages	Use Cases
MOD-101	Simple, iterative process: domain identification, class/property creation, hierarchy and instance modeling; supported by Protégé.	Easy to implement; excellent for teaching and prototyping; widely supported by tools.	Ideal for small-to-medium ontologies, and rapid prototyping.
Methontology	Full lifecycle approach: specification, conceptualization, formalization, implementation, and maintenance. Includes intermediate artifacts.	Highly structured; strong documentation and traceability; supports reusability.	Research, industrial projects, and complex domains with long-term maintenance needs.
NeOn	Modular, scenario-based methodology with support for reuse, evolution, and collaborative development. Emphasizes networked ontologies.	Supports distributed teams; reuse-oriented; strong modularization strategies.	Collaborative and large-scale ontology engineering projects (e.g., biomedical ontologies).
UPON (Unified Process for Ontology Development)	Adaptation of the Unified Process (from software engineering); iterative and architecture-driven. Emphasizes alignment with domain goals.	Integrates software and ontology development; strong role/task definition.	Ontologies developed in parallel with software engineering projects.
TOVE	Enterprise-focused ontology engineering with formal axioms and competency questions. Emphasizes formal reasoning.	High formal rigor; supports formal verification and logic-based modeling.	Organizational modeling, enterprise integration, business process ontologies.

The analysis revealed that despite the availability of more sophisticated methodologies, MOD-101 continues to be widely adopted, particularly in small-to-medium ontologies and applied contexts. MOD-101 provides a clear and pedagogically effective framework for initial ontology construction, particularly in scenarios where rapid prototyping, traceability, and conceptual formalization are required.

3.3 Ontology Evaluation Methodology - Q2

Regarding the question of which methodology is most commonly used to evaluate ontologies (Q2), research has shown that OntoMetric [45] is the most frequent choice. OntoMetric is an evaluation methodology that assesses the quality of ontologies developed from scratch. It assesses quality based on five qualitative dimensions, each of which evaluates a specific aspect of ontology development. The five dimensions considered in OntoMetric are Content Dimension, Language Dimension, Tool Dimension, Methodology Dimension, and Costs Dimension.

3.4 Ontology Development Tool - Q3

To support the selection of a development tool for the OntoPriv ontology, we reviewed multiple comparative studies and systematic reviews that evaluated ontology engineering environments. Table 3 presents a summary of tools identified in the literature across different authors and timeframes. Although some tools included in these studies—such as WebODE, Swoop, and Apollo—are no longer maintained or have domain-specific applications (e.g., Apollo in gene ontologies), their presence in the literature highlights their historical influence in shaping current practices.

Our analysis indicates that **Protégé** is the most frequently used and cited tool across studies, regardless of publication year. Its continued development, active community, OWL support, extensibility through plugins, and compatibility with widely adopted methodologies such as MOD-101 make it the most appropriate choice for developing the OntoPriv ontology. This selection ensures sustainability, interoperability, and alignment with current best practices in ontology engineering.

Table 3: Tools to develop ontologies

Autor	Tools
Bhaskar Kapoor, Savita Sharma [46]	Protégé 4.3, IsaViz, Apollo, Swoop
Noman Islam, Ghazala Shafi Sheikh [47]	TopBraid, composer, HOZO, OntoBroker, DOE, Ontolingua, Altova, SemanticWorks, OilEd, WebODE, pOWL, Morla, OBO-Edit, WSMO
N. Kaur, H. Aggarwal [48]	Apollo1.0, SWOOP 2.3, Beta4, Protégé 5.0, Graffoo 1.0, Neon 2.5.2
Ripal Ranpara et al. [49]	Protégé 4.3, Isaviz, Apollo, Swoop
Mohammed Yehia H. [50]	Protégé 2000, WebODE, WebOnto, KAON, OILED, OntoEdit, Ontoligua Server, LinkFactory
Marek Hatala et al. [51]	Text2Onto, OntoGen
Núria Casellas [52]	Protégé, SWOOP, WebODE, DOGMA
Fillottrani, Pablo R et al. [53]	ICOM 3.0
Andreia Malucelli [54]	Protégé 2000, WebODE, WebOnto, KAON, OILED, OntoEdit, Ontoligua Server, OWL plug-in, BeanGenrator plug-in, OntoViz
Leki Jovial Mahoro et al. [55]	RDF(S), OWL, Sem Web, dotNetRDF, Protege, Jena API, RDF4J, SPARQL
Manfred Jeusfeld [56]	Apollo, JOE, OntoEdit, Protégé 2000, Chimaera, ICOM, The MOMIS methodology, SymOntoX, WebOnto, KAON, OILEd, PROMPT, OBSERVER

4 OntoPriv Development

In this section, we develop OntoPriv and describe its querying process.

4.1 Privacy-oriented Architecture Components

We start by describing the main components of the LOPDP based on the privacy-oriented architecture proposed in [15]. Figure 3 illustrates a privacy-oriented architecture based on the LOPDP for secure collection, processing, verification, and transfer of personally identifiable information (PII). Actors play specific roles as defined in the LOPDP:

- The *data owner* is the person who owns their PII.
- The *data controller* is a person or legal entity that determines the purpose and treatment of the PII.
- The *data processor* is a personal or legal entity that processes PII.
- The *delegate* is a personal or legal entity in charge of informing the data controller and processor about their obligations regarding data protection.
- The *recipient* is the personal or legal entity that receives PII.
- The *control authority* is the public entity responsible for overseeing the enforcement of data protection regulations.
- The *certification entity* provides certification regarding data protection.

4.2 OntoPriv Structure

To develop OntoPriv, we followed the steps defined by MOD-101 (Section 3.2). To identify its core components, we carefully analyzed the LOPDP and validated the extracted information with domain experts to ensure completeness and accuracy. OntoPriv is composed of the following elements:

Classes: We defined a total of 176 classes. The top-level class is `Organic_Law_on_Personal_Data_Protection`, which serves as the root of the ontology. All other concepts are organized as *subclasses* of this main entity. Notable subclasses include: `Members_of_the_personal_data_protection`, `Personal_data_s

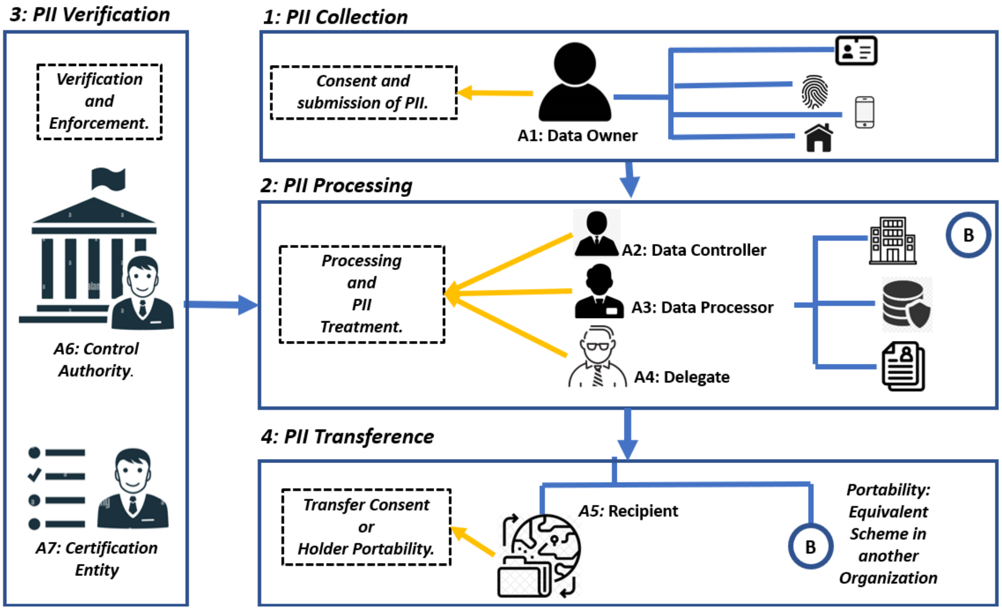


Figure 3: Privacy-oriented architecture components

ecurity, Principles, Processing, Rights, Sanctions, Terminology, Transfer_or_communication, Verification, and Violations.

To ensure logical consistency, key subclasses under Members_of_the_personal_data_protection—such as DataOwner, DataController, and DataProcessor—are explicitly declared as *disjoint classes*, preventing any individual from occupying multiple roles.

Formally, the subclass hierarchy and disjoint axioms are expressed in Description Logic (DL) as follows:

- DataOwner $\sqsubseteq$ MemberOfDataProtectionSystem
- DataController $\sqsubseteq$ MemberOfDataProtectionSystem
- DataProcessor $\sqsubseteq$ MemberOfDataProtectionSystem
- Delegate $\sqsubseteq$ MemberOfDataProtectionSystem
- ControlAuthority $\sqsubseteq$ MemberOfDataProtectionSystem
- DisjointClasses(DataOwner, DataController, DataProcessor)
- DisjointClasses(ControlAuthority, Delegate)

Figure 4 shows the parent classes in OntoPriv. All other classes are derived from these through subclass relationships.

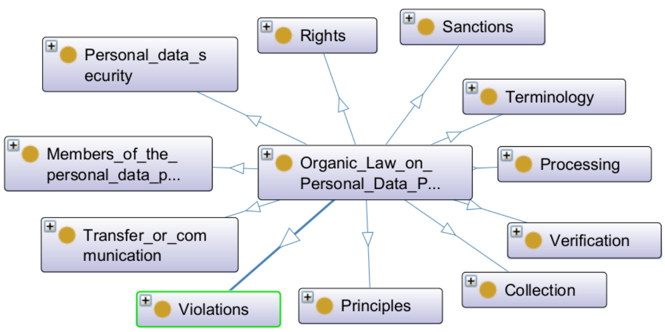


Figure 4: Parent Classes of OntoPriv: A Hierarchical View

Datatype Properties: OntoPriv defines 330 datatype properties, which provide descriptive attributes for each class. For example, the class Right includes properties such as irrevocability, limitation_on_ `exercise_of_rights_by_secondary_laws`, `responsible_for_channeling_exercise_of_rights`, and `responsible_for_guaranteeing_the_rights`, as illustrated in Figure 5.

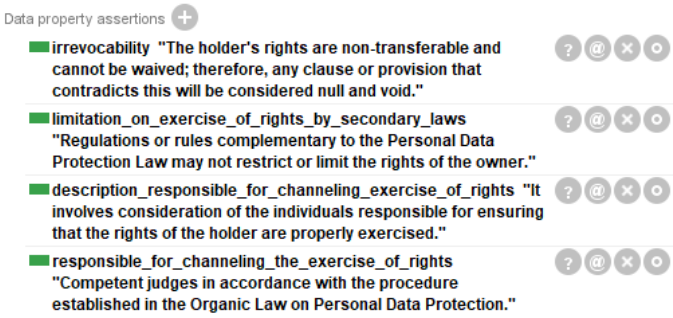


Figure 5: Properties of the Class "Right"

Object Properties (Relations): A total of 122 object properties interconnect OntoPriv classes. For instance, `Members_of_the_personal_data_protection_system` uses the relation `are_composed_of` to connect with specific entities such as `control_authority`, `data_controller`, `data_owner`, `data_processor`, and `delegate`.

Each object property is formally defined with its domain and range, and where appropriate, we specify logical characteristics to enhance semantic reasoning. Examples include:

- $\texttt{are\_composed\_of}: \texttt{MemberOfDataProtectionSystem} \to \texttt{LegalEntity}$ (inverse-functional)
- $\texttt{hasLegalBasis}: \texttt{ProcessingActivity} \to \texttt{LegalBasis}$ (transitive)
- $\texttt{monitors} \equiv \texttt{isMonitoredBy}^{-}$ (inverse)
- $\texttt{responsibleForGuaranteeingRights}: \texttt{MemberOfDataProtectionSystem} \to \texttt{Right}$ (functional)

Figure 6 visualizes how these relations interlink members of the personal data protection system.

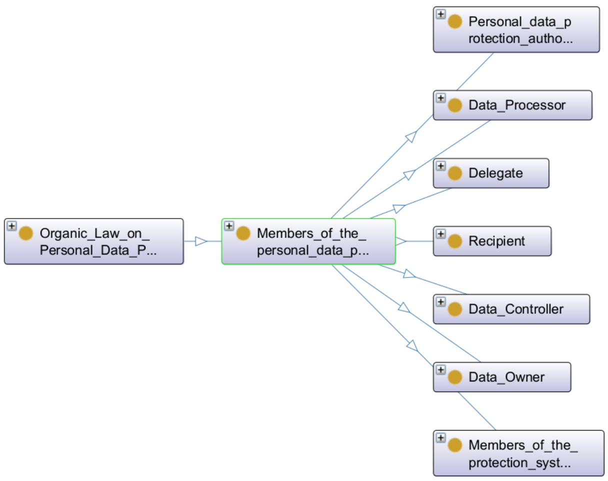


Figure 6: Interconnected Members: Exploring Relations within the Personal Data Protection System

Instances: OntoPriv also includes 176 individuals representing concrete instances of the modeled concepts. For example, a specific `Delegate` may be connected to a `Control_authority` using the relation `shall_be_observed_by`.

To further enhance formal reasoning, we introduce DL-based complex class definitions. For instance:

$$\texttt{ValidConsent} \equiv \texttt{Consent} \sqcap \exists \texttt{hasCondition.ValidityRequirement}$$

$$\texttt{NotificationDelay} \sqsubseteq \texttt{Notification} \sqcap \exists \texttt{hasDuration.}(\leq \texttt{5Days})$$

Additionally, to ensure interoperability with international frameworks, several OntoPriv classes are aligned with the W3C Data Privacy Vocabulary (DPV):

$$\texttt{PersonalData} \equiv \texttt{dpv:PersonalData} \qquad \texttt{Consent} \sqsubseteq \texttt{dpv:Consent}$$

All axioms were implemented in Protégé using OWL 2 and validated using the HermiT reasoner to ensure consistency and inferencing capability.

Finally, we used Protégé to model OntoPriv and visualize its structure. The complete ontology and source files are available in [57].

4.3 OntoPriv Querying Process

OntoPriv allows the formulation of competency questions within the scope of the LOPDP. Using its formally defined classes, object properties, and axioms, OntoPriv enables structured queries that support reasoning and information retrieval aligned with legal requirements. Below are examples of natural language questions that OntoPriv can answer:

- What specific conditions make consent valid, and what implications do they have?
- Who are the members of the personal data protection system?
- At what age can someone give explicit consent to processing their personal data?
- Who within the personal data protection system is responsible for ensuring that rights are exercised, particularly with respect to the right of access?
- How long must the data owner wait to be notified in case of a risk during a data transfer?

To execute queries in Protégé, we used the SQWRLTab plugin, as mentioned in Section 3.2. SQWRL (Semantic Query-Enhanced Web Rule Language) is a rule-based query language for OWL ontologies, supporting reasoning by evaluating class and property assertions based on logic rules. The process for executing a query consists of the following steps:

1. Write the question in natural language.
2. Translate the question into SQWRL syntax using classes and properties defined in OntoPriv.
3. Validate the query. The status must be "OK" on the SQWRLTab interface (see Figure 7), which provides a functional validation and practical demonstration of the utility of the ontology in simplifying the understanding and application of the LOPDP framework.
4. Execute the query and review the results.

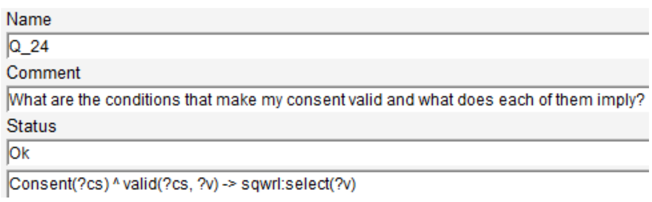


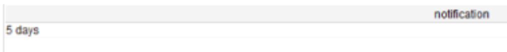
Figure 7: Query Validation

To support interoperability and semantic web standards, OntoPriv now supports SPARQL as its primary query language. SPARQL is a W3C-standardized query language for RDF and OWL ontologies, making it compatible with external systems such as Apache Jena, Virtuoso, and RDF4J. This revision complements the original SQWRL queries by enabling broader adoption and standards-based reasoning. The following examples include both the SQWRL version and its corresponding SPARQL translation.

Question 1: How long must the data subject wait to be notified in case of a risk at the time of a data transfer?

- **Query (SQWRL):** $Notification(?n) \wedge Security\_notification\_of\_infringement(?n, ?notification) \rightarrow sqwrl : select(?notification)$

- **Query structure:**
  - $Notification(?n)$**:** Declares `?n` as an instance of the class `Notification`.
  - $Security\_notification\_of\_infringement(?n, ?notification)$**:** Associates a notification object with its timing or duration through a data property.
  - $sqwrl : select(?notification)$**:** Retrieves the value of the data property representing the required notification time.
- **Query result:** Figure 8 shows the result returned by the query engine.



notification
5 days

Figure 8: Query Result of Question 1 using SQWRLTab

SPARQL Translation:

Listing 1: SPARQL Query 1

```
SELECT ?notificationTime
WHERE {
  ?n a onto:Notification .
  ?n onto:hasDuration ?notificationTime .
}
```

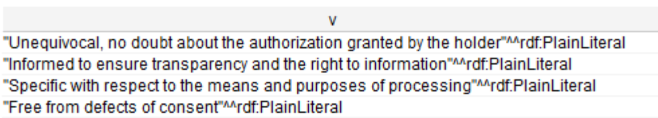
This query retrieves the notification duration for any instance of the class `Notification` via the `hasDuration` property.

Table 4: Result of SPARQL Query 1

notificationTime
5

Question 2: What specific conditions make consent valid, and what implications do they have?

- **Query (SQWRL):** $Consent(?cs) \wedge valid(?cs, ?v) \rightarrow sqwrl : select(?v)$
- **Query structure:**
  - $Consent(?cs)$**:** Declares `?cs` as an instance of the class `Consent`.
  - $valid(?cs, ?v)$**:** Links the consent instance to a condition or status through the property `valid`.
  - $sqwrl : select(?v)$**:** Returns the conditions required for valid consent.
- **Query result:** Shown in Figure 9.



v
"Unequivocal, no doubt about the authorization granted by the holder"^^rdf:PlainLiteral
"Informed to ensure transparency and the right to information"^^rdf:PlainLiteral
"Specific with respect to the means and purposes of processing"^^rdf:PlainLiteral
"Free from defects of consent"^^rdf:PlainLiteral

Figure 9: Query Result of Question 2 using SQWRLTab

SPARQL Translation:

Listing 2: SPARQL Query 2

```
SELECT ?validCondition
WHERE {
  ?cs a onto:Consent .
  ?cs onto:hasValidityCondition ?validCondition .
}
```

Table 5: Result of SPARQL Query 2

validCondition
FreelyGiven
Informed
Specific
Unambiguous

This query retrieves all conditions associated with the validity of consent.
Question 3: Who are the members of the personal data protection system?

- **Query (SQWRL):** $Members\_of\_the\_personal\_data\_protection\_system(?modp) \wedge are\_composed\_of(?modp, ?aco) -$ $sqwrl : select(?aco) \wedge sqwrl : limit(6)$
- **Query structure:**
  - $Members\_of\_the\_personal\_data\_protection\_system(?modp)$**:** Declares `?modp` as the collective group entity.
  - $are\_composed\_of(?modp, ?aco)$**:** Retrieves subclasses or instances representing each system member.
  - $sqwrl : select(?aco) \wedge sqwrl : limit(6)$**:** Selects the six primary members defined in the ontology.
- **Query result:** Shown in Figure 10.

aco
autogen0:responsible_for_treatment
autogen0:delegate
autogen0:personal_data_protection_authority
autogen0:data_owner
autogen0:data_processor
autogen0:recipient

Figure 10: Query Result of Question 3 using SQWRLTab

SPARQL Translation:

Listing 3: SPARQL Query 3

```
SELECT ?member
WHERE {
  onto:PersonalDataProtectionSystem onto:isComposedOf ?member .
}
```

This query returns all members formally defined in the system using the `isComposedOf` relation.

Table 6: Result of SPARQL Query 3

member
onto:DataController
onto:DataProcessor
onto:DataOwner
onto:Delegate
onto:ControlAuthority

Question 4: Who within the personal data protection system is responsible for ensuring that rights are exercised, particularly with respect to the right of access?

Listing 4: SPARQL Query 4

```
SELECT ?actor
WHERE {
  ?actor a onto:MemberOfDataProtectionSystem .
  ?actor onto:responsibleForGuaranteeingRights onto:RightOfAccess .
}
```

Table 7: Result of SPARQL Query 4

actor
onto:ControlAuthority

This query identifies actors assigned responsibility for ensuring that the right of access is respected.

In conclusion, both SQWRL and SPARQL play a valuable role in the validation and practical application of OntoPriv. SQWRL facilitates rule-based reasoning in the Protégé environment, while SPARQL supports standards-based querying and integration with external systems. Together, they strengthen OntoPriv's ability to support data protection compliance through flexible and accessible semantic queries.

5 OntoPriv Evaluation

In this section, we describe the metrics used to evaluate OntoPriv, and then we execute the evaluation and discuss the results.

OntoMetric provides a multidimensional framework aimed at quantifying the quality and usability of an ontology [45]; it is one of the most globally recognized qualitative methodologies compared to others such as OntoClean [58], OntoQA [59, 60], and OQuaRE [60, 61], as well as ROMEO [59, 60, 62]. It encompasses five fundamental dimensions: content, development vocabulary, development tool, development methodology, and associated costs. In this study, a sixth dimension was incorporated, named *Ontology Design Dimension*, focused on schema metrics. This strategy was implemented to address aspects not covered by other ontology evaluation methodologies. The evaluation involved answering specific questions, calculating metrics for each dimension, and distributing scores accordingly.

5.1 Evaluation Design

5.1.1 Qualitative metrics

We evaluated OntoPriv using the OntoMetric methodology, which consists of five qualitative dimensions: content, language, tool, methodology, and cost. We used the metrics proposed in [63] to evaluate each dimension. We score each metric as follows:

- **Fulfills:** 1 point
- **Partially fulfills:** 0.5 points
- **Fails:** 0 points

This scoring process generates numerical interpretations for each qualitative dimension and visualizes completeness when evaluating OntoPriv.

5.1.2 Quantitative metrics

Additionally, we consider a quantitative dimension that analyzes different numerical aspects present in OntoPriv, called Ontology Design. For the quantitative evaluation, we used the metrics proposed in [64]: the number of classes of the ontology, the richness of the attributes, the richness of heredity, and the richness of relationships. One can obtain the first metric, number of classes, from Protégé. The three remaining metrics are obtained using equations 1, 2, and 3, respectively.

$$AR = \frac{|ATT|}{|C|} \tag{1}$$

Where:

- AR: Attribute richness
- $|ATT|$: Number of properties of all classes
- $|C|$: Number of classes

$$IR = \frac{\sum_{C_i \in C} |H^C(C_1, C_i)|}{|C|} \tag{2}$$

Where:

- IR: Richness of Heredity
- $\sum_{C_i \in C} |H^C(C_1, C_i)|$: number of inheritance classes (classes that have a parent class)
- $|C|$: total number of classes

$$RR = \frac{|P|}{|H| + |P|} \tag{3}$$

Where:

- RR: Richness of relationships
- $|P|$: Number of relations (properties + disjunct classes + equivalent classes)
- $|H|$: number of inheritance classes (classes that have a parent class)

To obtain the values needed to compute these equations, one can manually analyze the developed ontology or use a web-based tool that validates and displays statistics about a given ontology. We use the web-based tool proposed in [65].

5.2 OntoPriv Evaluation

In this section, we evaluate OntroPriv using one qualitative and one quantitative dimension. The evaluation of the remaining dimensions can be found in our technical report [57].

We evaluate the content dimension. OntroPriv scored 22 out of 23 in the content dimension evaluation, demonstrating its completeness. The results are shown in Table 8.

Table 8: OntoPriv Content Dimension Evaluation

Content Dimension		
Factor	**Characteristic**	**Score**
Concepts	Essential Concepts	1
	Essential Concepts in Superior Levels	1
	Concepts Properly described in Natural Language (NL)	1
	Formal Specification of Concepts Coincides with NL	1
	Attributes Describe Concepts	1
	Number of Concepts	1
Relations	Essential Relations	1
	Relations Relate Appropriate Conceptss	1
	Formal Specification of Relations Coincides with NL	1
	Arity Specified	1
	Formal Properties of Relations	1
	Number of Relations	1
Taxonomy	Several Perspectives	1
	Appropriate not-Subclass of	0
	Appropriate Exhaustive-partitions	1
	Appropriate Disjoint-partitions	1
	Maximum Depth	1
	Average of Subclasses	1
Axioms	Axioms Solve Queries	1
	Axioms Infer Knowledge	1
	Axioms Verify Consistency	1
	Axioms not Linked to Concepts	1
	Number of Axioms	1
Total		22/23

Next, we evaluate the metric richness of heredity that is part of the design dimension. We use equation 2 and the statistics of OntoPriv obtained using the tool presented in [65].

$$IR = \frac{|175|}{|176|} = 0.994318 \approx 1 \tag{4}$$

This result indicates that OntoPriv is an ontology that focuses on a knowledge domain and delves into it deeply.

Table 9 summarizes the design dimension evaluation of OntoPriv.

Table 9: OntroPriv Design Dimension Evaluation

Dimension Ontology Design		
Metrics	**Results**	**Logical Interpretation**
Classes	176	Number of classes present in the developed ontology
Attribute Richness	1,920455	High
Inheritance Richness	0,994318	Vertical
Relationship Richness	0,477612	High

6 Alignment with the Data Privacy Vocabulary (DPV)

OntoPriv represents a pioneering effort as the first ontology in Ecuador, specifically addressing personal data protection legislation. However, as privacy concerns and international regulations evolve, it is essential to enhance OntoPriv's interoperability, adaptability, and alignment with global standards.

By aligning with the Data Privacy Vocabulary (DPV), OntoPriv not only broadens its scope but also provides an opportunity to address current limitations and strengthen the ontology to a more robust and globally relevant framework. The DPV, developed by the W3C Data Privacy Vocabularies and Controls Community Group (DPVCG), provides a comprehensive and standardized framework for representing privacy concepts, such as legal bases, purposes, rights, and compliance mechanisms [34].

By incorporating DPV elements, OntoPriv bridges the gap between local legislation, like the Ecuadorian Organic Law of Personal Data Protection (LOPDP), and global data privacy frameworks. This fosters interoperability and consistency across jurisdictions. In support of this alignment, we have formally defined key mappings and relationships using Description Logic (DL) syntax.

6.1 Limitations of OntoPriv

This section highlights the main limitations of OntoPriv and demonstrates how aligning it with the Data Privacy Vocabulary (DPV) can mitigate these issues, thereby enhancing OntoPriv's relevance, functionality, and applicability on a global scale.

1. *Limited Interoperability with Global Frameworks:* OntoPriv was designed with a focus on the Ecuadorian LOPDP. While it is effective for national compliance, its concepts and relationships lack standardization, making it challenging to integrate with other regulatory frameworks such as GDPR, CCPA, or LGPD.

2. *Inconsistent Terminology:* The ontology employs specific terminology relevant to Ecuador's jurisdiction, which may not be easily understood by global systems or practitioners, limiting its accessibility and usefulness outside of Ecuador.

3. *Underdeveloped Semantic Relationships:* While OntoPriv includes core relationships (e.g., data processing, consent), it does not leverage advanced semantic relationships like those defined in DPV (e.g., `dpv:hasPurpose`, `dpv:hasLegalBasis`), which support reasoning and compliance checks.

6.2 Addressing OntoPriv's Limitations with DPV

DPV provides a comprehensive and globally recognized framework for modeling data protection concepts and their relationships. By aligning OntoPriv with DPV, we can effectively address its current limitations, including interoperability and semantic depth.

1. *Global Standardization:* DPV offers a structured, jurisdiction-agnostic vocabulary with over 1,000 concepts related to data privacy and protection. By aligning OntoPriv with DPV, we ensure that its terminology and structure comply with global standards.

2. *Interoperability and Adaptability:* DPV's extensibility enables OntoPriv to incorporate concepts from other frameworks, facilitating compliance across multiple jurisdictions.

3. *Rich Semantic Relationships:* DPV introduces advanced relationships like `dpv:hasPurpose` and `dpv:hasLegalBasis`, enhancing OntoPriv's reasoning capabilities.

To ensure OntoPriv's semantics are well-defined and reasoning-ready, we incorporated DL-based axioms describing subclass hierarchies, disjointness, and relational properties.

6.3 Mapping OntoPriv to DPV Concepts

The process of mapping OntoPriv to DPV involved several steps:

1. **Extraction of OntoPriv Classes:** All major classes and subclasses within OntoPriv were identified, categorized, and documented.
2. **Analysis of DPV Terms:** The DPV 2.0 documentation was reviewed to extract relevant classes and properties.
3. **Concept Matching:** OntoPriv classes were aligned with DPV terms. Gaps were noted, and new concepts proposed where necessary.
4. **Definition Comparison:** Attributes and semantics were compared for consistency, ensuring OntoPriv terms matched the intended meaning in DPV.
5. **Iterative Refinement:** Mappings were validated with domain experts and refined through feedback.

Table 10: Revised Mapping Between OntoPriv and DPV Using Formal Axioms

OntoPriv Term	DPV Term	Formal Mapping (DL Axiom)
`Personal_data`	`dpv:PersonalData`	`Personal_data` $\equiv$ `dpv:PersonalData`
`Sensitive_data`	`dpv:SensitivePersonalData`	`Sensitive_data` $\sqsubseteq$ `dpv:PersonalData`
`Biometric_data`	`dpv:BiometricData`	`Biometric_data` $\sqsubseteq$ `dpv:SensitivePersonalData`
`Consent`	`dpv:Consent`	`Consent` $\equiv$ `dpv:Consent`
`Revocation_of_consent`	`dpv:WithdrawConsent`	`Revocation_of_consent` $\sqsubseteq$ `dpv:WithdrawConsent`
`Right_of_deletion`	`dpv:RightToBeForgotten`	`Right_of_deletion` $\equiv$ `dpv:RightToBeForgotten`
`Confidentiality`	`dpv:ConfidentialityAgreement`	`Confidentiality` $\equiv$ `dpv:ConfidentialityAgreement`
`Security`	`dpv:DataSecurityManagement`	`Security` $\sqsubseteq$ `dpv:DataSecurityManagement`
`Legal_basis`	`dpv:LegalBasis`	`Legal_basis` $\equiv$ `dpv:LegalBasis`
`Purpose`	`dpv:Purpose`	`Purpose` $\equiv$ `dpv:Purpose`
`Risk_analysis`	`dpv:Risk`	`Risk_analysis` $\sqsubseteq$ `dpv:Risk`
`Duration`	`dpv:Duration`	`NotificationTime` $\sqsubseteq$ `dpv:Duration`
`Anonymization`	`dpv:Anonymization`	`Anonymization` $\equiv$ `dpv:Anonymization`
`Automated_decision`	`dpv:AlgorithmicLogic`	`Automated_decision` $\sqsubseteq$ `dpv:AlgorithmicLogic`

6.4 Application of OntoPriv Aligned with DPV

The alignment between OntoPriv and DPV offers practical benefits in multiple contexts:

- **Compliance Automation:** OntoPriv+DPV enables tools to perform automated compliance validation with LOPDP and GDPR.
- **Cross-Jurisdictional Interoperability:** Semantic alignment with DPV facilitates data exchange and legal reasoning across legal systems.
- **Semantic Query Processing:** Richer relationships (e.g., `dpv:hasPurpose`) support compliance queries and logic-based auditing.
- **Training and Awareness:** The ontology supports educational use by clearly linking Ecuadorian and international terms.

These applications are powered by OntoPriv's formal specification and DL axiomatization, providing a foundation for logic-based validation, risk analysis, and modular extensibility. Future work will include tools for real-time monitoring, audit traceability, and integration with contracts or policy documents.

7 Discussion

The alignment of OntoPriv with the Data Privacy Vocabulary (DPV) highlights significant advancements in creating a unified framework for addressing personal data protection regulations. OntoPriv, as the first legal ontology developed in Ecuador, sets a precedent for leveraging semantic web technologies to address legislative requirements. The process of mapping OntoPriv to DPV concepts provided valuable insights into the similarities and gaps between local regulations, such as the Ecuadorian LOPDP, and international standards like GDPR.

The iterative mapping process ensured semantic consistency between OntoPriv and DPV terms, enabling the integration of essential concepts such as *LegalBasis*, *RetentionPeriod*, and *AutomatedDecisionMaking*. This alignment demonstrates OntoPriv's adaptability and its ability to enhance regulatory compliance frameworks. By adopting DPV's standardized terms, OntoPriv addresses key challenges such as temporal aspects of data processing, risk assessment, and anonymization techniques, which were previously underdeveloped.

OntoPriv's alignment also has practical implications for organizations operating in multi-jurisdictional contexts. The enhanced interoperability enables seamless data portability and ensures that compliance tools can be universally applied, bridging the gap between Ecuadorian legislation and global frameworks. Furthermore, the inclusion of DPV elements enhances OntoPriv's ability to support automated compliance tools, real-time risk analysis, and semantic query processing.

The development of OntoPriv serves as a demonstration of how local legal frameworks can be extended to align with international standards, fostering trust in data governance. By incorporating concepts like *ComplianceTools* and *Transparency*, OntoPriv not only meets the specific requirements of the LOPDP but also provides a model for other nations seeking to enhance their data privacy infrastructures.

However, challenges remain. The complexity of legal ontologies requires careful maintenance to ensure consistency as new regulations and amendments arise. Additionally, the integration of concepts like *AutomatedDecisionMaking* highlights the need for further research to address ethical concerns and technical implementations.

The alignment between OntoPriv and DPV showcases the potential for collaboration between regional and global standards, paving the way for future innovations in legal ontologies and data privacy frameworks. This collaboration underscores the importance of fostering interoperability to address the evolving landscape of data protection worldwide.

8 Conclusion and Future Work

OntoPriv represents a significant advancement as the first legal ontology specifically tailored to Ecuador's data protection framework, the LOPDP. Its alignment with the Data Privacy Vocabulary (DPV) bridges the gap between local regulations and international standards, providing organizations with a robust tool for navigating complex data protection requirements. By incorporating DPV concepts such as *LegalBasis*, *RetentionPeriod*, and *AutomatedDecisionMaking*, OntoPriv ensures consistency and interoperability across diverse regulatory contexts.

The mapping process highlighted both the strengths of OntoPriv in addressing specific legal requirements and the opportunities for improvement, such as including new classes for temporal aspects, anonymization techniques, and compliance tools. These enhancements extend OntoPriv's capabilities, making it a comprehensive resource for organizations aiming to meet the evolving demands of data privacy governance.

As a pioneering ontology in Ecuador, OntoPriv lays the groundwork for future developments in legal ontologies and semantic web technologies within the region. Its alignment with DPV enhances its usability not only for addressing Ecuadorian data privacy laws but also for providing a framework for interoperability across global standards like GDPR and LGPD. This dual focus ensures that OntoPriv serves both local and international needs, making it an essential tool for organizations operating in multi-jurisdictional environments.

The alignment also demonstrates the value of structured approaches to bridging gaps between local and global legal frameworks. By ensuring semantic consistency and adopting modular principles from DPV, OntoPriv facilitates the representation of complex privacy requirements and helps organizations navigate evolving data protection landscapes.

Future efforts will focus on practical applications of OntoPriv, including automated compliance tools, real-time risk analysis, and the integration of machine-readable legal contracts. In particular, we are preparing a pilot application involving selected public and private institutions in Ecuador to evaluate OntoPriv's effectiveness in supporting legal compliance, privacy governance, and automated reasoning in real-world organizational settings. This deployment will provide empirical evidence of OntoPriv's applicability and inform future improvements. Further alignment with international standards will enable OntoPriv to remain adaptable and relevant as new regulations emerge, ensuring it continues to provide value for privacy governance in Ecuador and beyond. By fostering trust, accountability, and compliance, OntoPriv positions itself as a pioneering framework for the future of legal ontologies.

References

[1] G. Suntaxi, K. Ojeda, and F. Rodríguez, "OntoPriv: Enhancing Understanding and Compliance in Privacy Legislation via Legal Ontologies," in *2024 L Latin American Computer Conference (CLEI)*, 2024, pp. 1–10. [Online]. Available: https://doi.org/10.1109/CLEI64178.2024.10700326

[2] G. Suntaxi, A. A. E. Ghazi, and K. Böhm, "Preserving secrecy in mobile social networks," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, pp. 1–29, 2020.

[3] B. Gibson, S. Townes, D. Lewis, and S. Bhunia, "Vulnerability in massive api scraping: 2021 linkedin data breach," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021, pp. 777–782.

[4] European Union, "General data protection regulation (gdpr)," Sep 2019, [Accessed April 1st, 2024]. [Online]. Available: https://gdpr-info.eu/

[5] Presidência da República Secretaria-Geral , "General personal data protection act (lgpd)," August 2018, [Accessed April 1st, 2024]. [Online]. Available: https://lgpd-brazil.info/

[6] A. N. R. del Ecuador, "Ley orgánica de protección de datos personales," May 2021, [Accessed April 1st, 2024]. [Online]. Available: https://bit.ly/41q3Att

[7] T. Mikkonen, "Perceptions of controllers on eu data protection reform: A finnish perspective," *Computer law & security review*, vol. 30, no. 2, pp. 190–195, 2014.

[8] A. F. Guzman-Castillo, G. Suntaxi, B. N. Flores-Sarango, and D. A. Flores, "Towards designing a privacy-oriented architecture for managing personal identifiable information," *Journal of internet services and information security*, vol. 14, no. 1, pp. 64–84, 2024.

[9] J. Jiang, H. Aldewereld, V. Dignum, S. Wang, and Z. Baida, "Regulatory compliance of business processes," *AI & society*, vol. 30, no. 3, pp. 393–402, 2015.

[10] C. Tankard, "What the gdpr means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5–8, 2016.

[11] S. Sirur, J. R. Nurse, and H. Webb, "Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr)," in *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, 2018, pp. 88–95.

[12] M. Palmirani, M. Martoni, A. Rossi, B. Cesare, R. Livio *et al.*, "Legal ontology for modelling gdpr concepts and norms," *Frontiers in Artificial Intelligence and Applications*, vol. 313, pp. 91–100, 2018.

[13] H. J. Pandit, C. Debruyne, D. O'Sullivan, and D. Lewis, "Gconsent-a consent ontology based on the gdpr," in *The Semantic Web: 16th International Conference, ESWC 2019, Portorož, Slovenia, June 2–6, 2019, Proceedings 16*. Springer, 2019, pp. 270–282.

[14] R. Arp, B. Smith, and A. D. Spear, *Building ontologies with basic formal ontology.* Mit Press, 2015.

[15] A. Guzmán-Castillo, G. Suntaxi, B. N. Flores-Sarango, and D. A. Flores, "Towards designing a privacy-oriented architecture for managing personal identifiable information," *Journal of Internet Services and Information Security*, 2024.

[16] C. de la Nación Argentina, "Ley 25.326 de protección de los datos personales," Sep 2000, [Accessed April 5st, 2024]. [Online]. Available: https://www.argentina.gob.ar/sites/default/files/arg_ley25326.pdf

[17] C. N. de Brasil, "Lei geral de proteção de dados pessoais (lgpd)," Aug 2020, [Accessed April 5st, 2024]. [Online]. Available: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd

[18] C. Chileno, "Ley 19628 sobre protección de la vida privada," Aug 1999, [Accessed April 5st, 2024]. [Online]. Available: https://www.bcn.cl/leychile/navegar?idNorma=141599

[19] C. de Colombia, "Política de tratamiento y protección de datos," Oct 2012, [Accessed April 5st, 2024]. [Online]. Available: https://www.minambiente.gov.co/wpcontent/uploads/2023/03/DS-E-GET-01.pdf

[20] C. de Costa Rica, "Ley de protección de la persona frente al tratamiento de sus datos personales ley 8968," Sep 2011, [Accessed April 5st, 2024]. [Online]. Available: https://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf

[21] A. N. del Poder Popular de Cuba, “Ley 149 de protección de datos personales,” Aug 2022, [Accessed April 5st, 2024]. [Online]. Available: https://www.minjus.gob.cu/sites/default/files/archivos/publicacion/2022-08/goc-2022-o90_0_0.pdf

[22] C. de la República de El Salvador, “Ley de protección de datos personales y habeas data,” Jun 2019, [Accessed April 5st, 2024]. [Online]. Available: https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/2A326CE8-F13A-4828-8640-648235C228BF.pdf

[23] C. de Honduras, “Propuesta de ley de protección de datos personales de honduras,” Jan 2013, [Accessed April 5st, 2024]. [Online]. Available: https://cei.iaip.gob.hn/doc/Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf

[24] C. de la Unión de México, “Ley federal de protección de datos personales en posesión de los particulares,” Jul 2010, [Accessed April 5st, 2024]. [Online]. Available: https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf

[25] A. N. de Nicaragua, “Ley de protección de datos personales, ley n 787,” Mar 2012, [Accessed April 5st, 2024]. [Online]. Available: http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d

[26] A. N. de Panamá, “Ley 81 de protección de datos personales,” May 2021, [Accessed April 5st, 2024]. [Online]. Available: https://www.antai.gob.pa/reglamentan-ley-81-de-proteccion-de-datos-personales/

[27] C. de Datos de Paraguay, “Ley N 6534 de protección de datos personales crediticios,” Oct 2020, [Accessed April 5st, 2024]. [Online]. Available: https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

[28] A. N. de Datos Personales (ANPD), “Ley N 29733 ley de protección de datos personales de perú,” Jul 2011, [Accessed April 5st, 2024]. [Online]. Available: https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

[29] C. N. de la República Dominicana, “Ley de protección de datos personales dominicana, Ley No. 172-13,” Dic 2013, [Accessed April 5st, 2024]. [Online]. Available: https://www.tribunalconstitucional.gob.do/transparencia/marco-legal/leyes/ley-172-13/

[30] R. O. del Uruguay, “Protección de datos personales y acción de “habeas data”, Ley No. 18.331,” Aug 2008, [Accessed April 5st, 2024]. [Online]. Available: https://seleccion.poderjudicial.gub.uy/seleccion/archivos/ley18331habeasdata2008.pdf

[31] N. Guarino, D. Oberle, and S. Staab, “What is an ontology?” *Handbook on ontologies*, pp. 1–17, 2009.

[32] V. Mlačić, S. Virtanen, and A. Hakkala, *Data protection regulation ontology for compliance.* University of Turku, 2022.

[33] N. F. Noy, D. L. McGuinness *et al.*, “Ontology development 101: A guide to creating your first ontology,” 2001.

[34] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, and J. Flake, “Data privacy vocabulary (dpv)–version 2.0,” in *International Semantic Web Conference.* Springer, 2024, pp. 171–193.

[35] M. Geko and S. Tjoa, “An Ontology Capturing the Interdependence of the General Data Protection Regulation (GDPR) and Information Security,” *ResearchGate*, pp. 1–6, Nov. 2018.

[36] C. Bartolini, A. Calabró, and E. Marchetti, “Enhancing Business Process Modelling with Data Protection Compliance: An Ontology-based Proposal,” *ResearchGate*, pp. 421–428, Jan. 2019.

[37] A. Dresch, D. P. Lacerda, J. A. V. Antunes Jr, A. Dresch, D. P. Lacerda, and J. A. V. Antunes, *Design science research.* Springer, 2015.

[38] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering–a systematic literature review,” *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.

[39] N. F. Noy and D. L. McGuinness, “Ontology development 101: A guide to creating your first ontology,” Stanford Knowledge Systems Laboratory, Stanford, CA, Technical Report KSL-01-05, 2001.

[40] M. Fernández-López, A. Gómez-Pérez, and N. Juristo Juzgado, "Methontology: from ontological art towards ontological engineering," 1997.

[41] M. C. Suárez-Figueroa, A. Gómez-Pérez, and M. Fernandez-Lopez, "The neon methodology framework: A scenario-based methodology for ontology development," *Applied ontology*, vol. 10, no. 2, pp. 107–145, 2015.

[42] A. De Nicola, M. Missikoff, and R. Navigli, "A software engineering approach to ontology building," *Information systems*, vol. 34, no. 2, pp. 258–275, 2009.

[43] H. M. Kim, M. S. Fox, and M. Gruninger, "An ontology of quality for enterprise modelling," in *Proceedings 4th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'95).* IEEE, 1995, pp. 105–116.

[44] M. A. Musen, "The protégé project: a look back and a look forward," *AI matters*, vol. 1, no. 4, pp. 4–12, 2015.

[45] P. F. Green and M. Rosemann, *Business Systems Analysis with Ontologies.* Hershey, PA: Idea Group Publishing, 2005. [Online]. Available: https://www.igi-global.com/book/business-systems-analysis-ontologies/122

[46] B. Kapoor and S. Sharma, "A comparative study ontology building tools for semantic web applications," *International journal of Web & Semantic Technology (IJWesT)*, vol. 1, no. 3, pp. 1–13, 2010.

[47] N. Islam and G. S. Sheikh, "A review of techniques for ontology editor evaluation," *Journal of Information & Communication Technology (JICT)*, vol. 9, no. 2, p. 11, 2015.

[48] N. Kaur and H. Aggarwal, "Evaluation of information retrieval based ontology development editors for semantic web," *International Journal of Modern Education and Computer Science*, vol. 9, no. 7, p. 63, 2017.

[49] R. Ranpara, A. Yusufzai, and C. Kumbharana, "A comparative study of ontology building tools for contextual information retrieval," in *Emerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018.* Springer, 2019, pp. 401–408.

[50] M. Y. Hassan, A. Rafea, K. Shaalan, and H. Hassan, "Extracting ontology from different sources."

[51] M. Hatala, D. Gašević, M. Siadaty, J. Jovanović, and C. Torniai, "Can educators develop ontologies using ontology extraction tools: an end-user study," in *Learning in the Synergy of Multiple Disciplines: 4th European Conference on Technology Enhanced Learning, EC-TEL 2009 Nice, France, September 29–October 2, 2009 Proceedings 4.* Springer, 2009, pp. 140–153.

[52] N. Casellas and N. Casellas, "Methodologies, tools and languages for ontology design," *Legal Ontology Engineering: Methodologies, Modelling Trends, and the Ontology of Professional Judicial Knowledge*, pp. 57–107, 2011.

[53] P. R. Fillottrani, E. Franconi, and S. Tessaris, "The icom 3.0 intelligent conceptual modelling tool and methodology," *Semantic Web*, vol. 3, no. 3, pp. 293–306, 2012.

[54] A. Malucelli, *Ontology-based services for agents interoperability.* Universidade do Porto (Portugal), 2006.

[55] L. J. Mahoro and J. V. Fonou-Dombeu, "A comparative analysis of dot net-based and open source platforms for ontologies development," in *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD).* IEEE, 2020, pp. 1–7.

[56] M. Jeusfeld, C. Dong, and M. B. Jeusfeld, "Noe interop (ist-508011)," 2004.

[57] "OntoPriv," Apr. 2024, [Online; accessed 08. June. 2025]. [Online]. Available: https://github.com/kelvinojedaepn/OntoPriv

[58] R. Wilson, J. Goonetillake, W. Indika, and A. Ginige, "A conceptual model for ontology quality assessment," *Semantic Web Journal*, 2022. [Online]. Available: https://www.semantic-web-journal.net/system/files/swj3393.pdf

[59] T. Ivanova and M. Popov, "Ontology evaluation and multilingualism," in *Proceedings of the 21st International Conference on Computer Systems and Technologies (CompSysTech '20)*, 2020, pp. 215–222.

[60] M. McDaniel and V. C. Storey, "Evaluating domain ontologies: Clarification, classification, and challenges," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–44, 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3329124

[61] A. Duque-Ramos, M. Boeker, L. Jansen, S. Schulz, M. Iniesta, and J. T. Fernández-Breis, "Evaluating the good ontology design guideline (goodod) with the ontology quality requirements and evaluation method and metrics (oquare)," *PLOS ONE*, vol. 9, no. 8, p. e104463, 2014. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0104463

[62] M. Rico, M. L. Caliusco, O. Chiotti, and M. R. Galli, "Ontoqualitas: A framework for ontology quality assessment in information interchanges between heterogeneous systems," *Computers in Industry*, vol. 65, no. 9, pp. 1291–1300, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166361514001456

[63] A. Gomez-Perez and A. Lozano-Tello, "Applying the ontometric method to measure the suitability of ontologies," in *Business Systems Analysis with Ontologies*. IGI Global, 2005, pp. 249–269.

[64] Y. Helmy, S. Ali, and M. Abd Ellatif, "Evaluating the proposed public budget ontological model," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 16, no. 7, 2018.

[65] (2023) Ontometrics. Universität Rostock. [Online]. Available: https://ontometrics.informatik.uni-rostock.de/ontologymetrics/index.jsp