Why Eliciting and Managing Legal Requirements Is Hard

Nadzeya Kiyavitskaya
University of Trento
nadzeya@disi.unitn.it

Alžběta Krausová
ICRI - K. U. Leuven - IBBT
betty.krausova@law.kuleuven.be

Nicola Zannone
University of Toronto
zannone@cs.toronto.edu

Abstract

The increasing complexity of IT systems and the growing demand for regulation compliance are main issues for the design of IT systems. Addressing these issues requires the developing of effective methods to support the analysis of regulations and the elicitation of any organizational and system requirements from them. This work investigates the problem of designing regulation-compliant systems and, in particular, the challenges in eliciting and managing legal requirements.

1 Introduction

Making IT systems and procedures compliant with regulations is a challenge for every organization. For instance, violations of privacy have been inadvertently supported by information technologies [2], as in the case of Kaiser Permanente (KP), a US health provider, which accidentally disclosed personally identified health information through its web healthcare portal [10].

Organizations employ software products, and develop procedures, to support their business activities. They must ensure that the software products and procedures adopted are compliant with the regulations in force. In the case of non-compliance with applicable laws, an organization may be administratively sanctioned; also, a person who has suffered damage because of a deviation from these norms may claim compensation. Legal incidents do not have only legal and financial consequences for an organization, but also affect the trust that people feel towards the organization [6].

Very often, organizations impose the full burden of devising a regulation-compliant product on software designers and system administrators that do not have any legal education. The analysis of laws is time consuming and error prone, and it must be done by a lawyer specialized in the field. In addition, there is a gap between legal and computer language that makes it difficult to convert legal obligations into organizational and system requirements [12].

These issues affect the development of software products and the development of procedures compliant with relevant regulations. To facilitate the alignment of organizational and system requirements with legislation, designers need methods and tools that assist them to analyze regulatory documents and to elicit their requirements. In this work, we investigate the problem of designing regulation-compliant systems and, in particular, of eliciting and managing requirements from regulations.

The paper is organized as follows. In the next section, we identify the main challenges for the development of regulation-compliant systems. Then, we discuss the identified challenges in detail in Sections 3, 4, 5, and 6. Finally, we conclude in Section 7.

2 Issues

Designing regulation-compliant systems demands the analysis of normative legal texts and the elicitation of their organizational and system requirements. Any attempt to meet these challenges requires organizations to address a number of issues:

- **Information extraction from law:** to find requirements in regulatory documents, organizations must identify relevant pieces of information in these documents and understand the relationships between various information fragments. Although the vocabulary and grammar used is often restricted, legal texts are written in natural language in its full complexity.

- **Choice of law:** organizational and system requirements can arise from different sources of law. Therefore, organizations shall analyze all relevant regulations and prioritize them to identify the legal requirements to be met.

- **Imperfection and vagueness of law:** the interpretation of a law consists in determining the true meaning of the law. Unfortunately, this is difficult because legal documents can contain vague terms, contradictory provisions, and legal lacunae.

- **Dynamics of law:** law is not a static phenomenon. It evolves continuously: new legislation is enacted; old legislation is amended or repealed; important judicial decisions are issued. Requirements to be met by organizations may change consequently. An organization must therefore keep its IT systems and procedures updated and consistent with respect to all applicable regulations.

3 Information Extraction from Law

Nowadays, law strictly regulates the business activities of organizations. Organizations must implement legal requirements when developing their IT systems and defining their policies and procedures. Unfortunately, the analysis of legal texts entails a number of difficulties.

Several efforts have been made to improve the accessibility of laws by offering ontologies, guidelines and standards for legal drafting, such as the Italian NIR standard[1] and the Dutch Guidelines for Legal Drafting.[2] These provide a standardized description of normative documents and guidelines to guarantee interoperability among the IT systems of public authorities. Based on the elaborated standards, a number of tools have been developed to facilitate the analysis of regulations, as for instance, NormaSystem [18], MetaVex [21], SOLON [11], and XMLeges [3]. These tools provide user-friendly environments to create, modify, and annotate legal documents. They also allow the validation of annotated documents against regulation templates in order to detect inconsistencies in the markup, such as, a missing publication date, the duplication of the title or date, or the wrong content type.

However, such legal drafting tools are not suitable for the elicitation of legal requirements. Organizations must take into account different sources of law when eliciting legal requirements, and interpret regulatory documents (see the discussion of these issues in Sections 4 and 5). Also some tools for legal drafting are limited to the regulation template of specific countries. For example, XMLeges is mainly oriented to writing documents according to the Italian NIR standard. Most important, although regulation-drafting environments can help organizations to structure regulations by highlighting syntactic information (e.g., the date of creation or modification of the document, authors, etc.), they are incapable of extracting requirements from legal texts. Indeed, the extraction of information requires capturing semantic relations among words to correctly interpret the meaning of whole sentence.

Towards this goal, Antoniu et al. [5] have introduced a regulations analysis method based on the defeasible theory [17]. According to this theory, facts manually found in regulation documents are represented as defeasible logical rules. Other systematic methods include Privacy APIs [16], the Goal-Based Requirements Acquisition Methodology (GBRAM) [4], and SALEM [7]. The Privacy APIs framework converts rule statements in natural language into formal expressions, which are formally analyzed to identify problematic statements. GBRAM was developed to extract goals from natural language texts and to apply them to privacy policies. One of the results of this analysis was the creation of a set of heuristics for extracting artifacts from legal texts [9], which was then combined into a frame-based method for manually acquiring legal requirements and priorities from regulations [8] and that has been used as a basis for developing a framework for tool-supported identification of requirements in legal documents [14]. The SALEM system adapts a linguistic approach for the extraction of semantic concepts from Italian legal documents, such as actors, actions and properties. It also classifies different types of provisions using a text categorization algorithm.

Regulation analysis methods can aid software engineers in the development of regulation-compliant systems. Indeed, such methods provide a systematic way to elicit, model and analyze requirements from legal texts. Once legal requirements are formally modeled, they can be implemented in a software system or converted into a set of test cases for compliance verification. Yet, these instruments remain unemployed, except for limited studies. The main reason is the lack of tool support, which requires the additional involvement of expensive legal or linguistic expertise to deal with the complicated text of legal documents.

4 Choice of Law

When developing regulation-compliant systems, organizations must consider different sources of law. For instance, US law relies on a mix of legislation, regulations, and self regulations that are grounded in common law, constitutional law, statuary law, and international law. In contrast, organizations in the EU must respect both EU legislation and the national law of the Member State in which they operate. The most relevant sources of EU law are sources of secondary law, namely regulations and directives. According to Article 249 of the Treaty establishing the European Community, *"a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States"* [1]. On the other hand, *"a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods"* [1]. Therefore, EU regulations must be adopted by organizations in their entirety. However, the nature of EU directives also evokes the need to analyze national laws when eliciting legal requirements. Directives only set general princi-

[1] http://www.normeinrete.it/
[2] http://www.justitie.nl/

ples and guidelines and leave each Member State to define specific requirements and measures to address the problem. In fact, directives are intended to harmonize national laws of Member States. When analyzing directives, it is necessary to distinguish between provisions imposing obligations only on Member States, and provisions that also impose rights and obligations upon other subjects.[3]

Achieving compliance with all relevant and applicable laws is a challenging task as regulations from different legal sources can conflict. Legal theory states that inconsistencies should be solved on grounds of legal force, where the legal force of a regulation is derived from its position in the system of law. Every country has its own legal system in which sources of law are organized hierarchically with respect to the tradition of the country. In case of contradictory provisions set by two regulations, the rule contained in the regulation having a higher legal force should be used. However, a law hierarchy is not always well defined. For instance, in the US, the position of international treaties is highly debated, and contradictions with statutes are solved using the "last-in-time" principle[4] [15].

When two regulations at the same level set contradictory provisions, legal theory offers two basic principles[5] to determine which provision should be used:

1. *Lex posterior derogat priori*: a rule stating that the regulation issued later should be applied;

2. *Lex specialis derogat generali*: a rule stating that the more specific regulation should be applied.

Other specific rules may be found in various legal environments. For instance, the EU uses a principle of supremacy of EC law[6] and a principle of direct applicability.[7]

[3]Paragraph 1 of Article 23 of the European Data Protection Directive (95/46/EC) represents a two-level provision that imposes an obligation on Member States and at the same time it guarantees a particular right for an individual person: *"Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered"*.

[4]This principle is recognized in cases such as Whitney v. Robertson, 124 U.S. 190 (1888); Appellants v. Dirk KEMPTHORNE; Secretary of the Interior, et al., Appellees.

[5]These principles are accepted in the EU law by the ECJ, e.g., Opinion of Advocate General Kokott in Case C-275/06; Opinion of Advocate General Ruiz-Jarabo Colomer in Case C-104/03; Judgment of 25 October 2007 in joined cases T-27/03, T-46/03, T-58/03, T-79/03, T-80/03, T-97/03 and T-98/03.

[6]In accordance with the decision of the ECJ in the case 6/64, Flaminio Costa v E.N.E.L., when there are contradictions between a national law and an EC law which *"is legally complete and consequently capable of producing direct effects of the relations between Member States and individuals"*, the EC law will be applied instead of national law.

[7]If a Member State does not implement a directive properly, persons subject to its national law may claim a direct applicability of the relevant EU directive when this is more advantageous for them, as determined by the ECJ in decisions such as Van Gend en Loos (Case 26/62), Defrenne vs. Sabena (Case 43/75), Van Duyn (Case 41/74), etc.

Organizations should be aware of all legislation that regulates their business activities. This implies that organizations must investigate all sources of law to identify the regulations relevant to their businesses. In the case of inconsistencies in the relevant legislation, organizations also need to be able to resolve the conflict and to choose the regulation that shall be enforced. These issues demand methods and tools for regulation management and analysis. The extensive adaptation of regulation-drafting environments, which provide facilities to use syntactic metadata, can help to solve some of these problems, such as regulations structuring, cross-referencing and versioning. Semantic approaches can also be used to assist organizations in identifying and solving inconsistencies in applicable regulations.

Advanced legal information systems (LISs) provide an answer to some of the issues considered here. In particular, such systems store and categorize legal information in such a way that enables the identification of legislation related to a particular legal field or to a specific subject matter. Examples of LISs are ASPI[8] and LexGalaxy.[9] These are Czech LISs that allow searching for legislation on the basis of various criteria. Usually, LISs also store all versions of legal documents and often provide information on relations between these documents. However, organizations must be aware of the hierarchy of laws to solve conflicts. Another solution for determining the relevant legislation for a particular business organization is the creation of repositories collecting business objectives and relating them to the corresponding legislation. These repositories can also contain information on organizational and system requirements to be met by business companies, and should be built on the current industry practices.

5 Imperfection and Vagueness of Law

Legal texts are frequently affected by ambiguities and lacunae. These issues make it difficult to interpret legal texts and elicit organizational and system requirements precisely. The problem of lacunae in regulations arises when some area should be regulated by law but it is not. Organizations may have doubts about their own rights and obligations. In this case, they have to verify whether the lacuna has not been already filled in, for example, by binding judicial decisions (especially in the common law countries). Organizations should also check whether they do not have any obligation or right imposed upon them on the basis of analogy with other regulations, and possibly, with judicial decisions.

Legal texts often make use of vague and non-specific terms that make the interpretation of provisions difficult. In

[8]http://www.aspi.cz/aspi/aspi-informace/english/

[9]http://www.lexgalaxy.cz/

the case of uncertainty about the meaning of a term or a sentence, methods for legal interpretation can assist an organization in interpreting legal texts. These methods can be divided into the following groups [13, 19]:

- *lingual*: interpretation is based on grammatical, morphological, and syntactical rules;
- *logical*: the meaning is discovered with the help of formal logic rules;
- *systematic*: interpretation is made with respect to the whole legal order;
- *historic*: the meaning is clarified on the basis of circumstances under which the regulation was issued;
- *teleological*: interpretation is based on the purpose and a function of the rule.

When eliciting legal requirements from EU legislation, recitals must be given special attention. These instruments specify the context and rationale for the legislation, providing guidelines for its interpretation. In particular, recitals must be interconnected with provisions of the legislation to prevent misleading interpretations. In addition, regulations usually contain articles that define the terminology and concepts of the specific application domain regulated by the particular piece of legislation. For instance, Article 2 of the European Data Protection Directive[10] defines the concepts of *personal data*, *processing of personal data*, and others. Analysts can take advantages of these articles and recitals to build specific application domain ontologies intended to support system design and management.

As interpretation strongly depends on an understanding of the law and its internal structure and relations, legal texts are often difficult to understand for the "layman". Additional support is therefore needed by organizations to make a "correct" interpretation of law. In addition to tools for regulation management, organizations should also obtain tools for legal interpretation and databases of relevant judicial decisions, together with guidelines for using them.

6 Dynamics of Law

Laws change very often. When a relevant law is enacted or amended, organizations must react accordingly. During *vacantia legis*, i.e., the period between the enactment and putting into legal effect of a law, organizations have to take the steps necessary to comply with the new law. The length of this period differs from country to country and may vary within the same country depending on the law:[11] it is usually based on the importance and impact of changes, and has the purpose of giving subjects the time to conform to the new law.

To remain legally compliant, organizations must regularly check for new laws relevant to their businesses. However, not only legislation but also some judicial decisions are important to determine obligations as they may explain complicated situations when relations of various laws are not clear or are conflicting.[12]

After comparing new legislation with the one previously in force to identify new, modified, or deleted organizational and system requirements, organizations need methods to identify which functionality of the system or steps of procedures should be modified to make the system compliant with the new laws. Requirement traceability [20] can assist organizations in this task as it ensures continued alignment between requirements and various outputs of the system development process.

7 Conclusions

Law plays a crucial role in the business activities of organizations. Designing IT systems and procedures compliant with the relevant regulations in force is a challenging task. As shown in this paper, several issues make the accomplishment of this task difficult. Although a number of approaches and tools have been introduced in recent years, they often focus on specific aspects of regulation analysis or drafting tasks and, thus, address the problem only partially. More efforts are needed to improve existing contributions and integrate them to fully assist organizations in eliciting and managing legal requirements.

Acknowledgments This work has been partially funded by the EU Commission through the projects IST-FP6-IP-SERENITY and FP7-PAPYRUS.

References

[1] Treaty establishing the European Community. *Official Journal of the European Union*, (C 325):33–184, 2002. Available at http://eur-lex.europa.eu/.

[2] A. Adams. The Implications of Users' Multimedia Privacy Perceptions on Communication and Information Privacy Policies. In *Proc. of Telecommunications Policy Research Conference*, 1999.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23/11/1995, p. 31*

[11] See, for example, Czech act no. 309/1999 of the Collection of Laws. According to §3, legal regulations come into force on the day of their publication in the Collection of Laws. Regulations become effective on the 15th day after their publication. However, the date of legal effect may be postponed by a special provision contained in the law in question.

[12] A judgment of the ECJ of 29.1.2008 in case C-275/06 (Promusicae) determined rules regarding an obligation to disclose personal data of people using peer-to-peer to holders of intellectual property rights.

[3] T. Agnoloni, E. Francesconi, and P. Spinosa. XmLegesEditor: an OpenSource Visual XML Editor for supporting Legal National Standards. In *Proc. of V Legislative XML Workshop*. European Press Academic Publishing, 2007.

[4] A. I. Antón, J. B. Earp, Q. He, W. Stufflebeam, D. Bolchini, and C. Jensen. Financial privacy policies and the need for standardization. *IEEE Security & Privacy*, 2(2):36–45, 2004.

[5] G. Antoniou, D. Billington, and M. J. Maher. On the Analysis of Regulations using Defeasible Rules. In *Proc. of HICSS'99*, volume 6, page 6033. IEEE Press, 1999.

[6] I. Araujo. Privacy mechanisms supporting the building of trust in e-commerce. In *Proc. of PDM'05*, page 1193. IEEE Press, 2005.

[7] C. Biagioli, E. Francesconi, A. Passerini, S. Montemagni, and C. Soria. Automatic semantics extraction in law documents. In *Proc. of ICAIL'05*, pages 133–140. ACM, 2005.

[8] T. D. Breaux and A. I. Antón. Analyzing regulatory rules for privacy and security requirements. *TSE*, 34(1):5–20, 2008.

[9] T. D. Breaux, M. W. Vail, and A. I. Antón. Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In *Proc. of RE'06*, pages 46–55. IEEE Press, 2006.

[10] J. R. Collmann and T. Cooper. Breaching the Security of the Kaiser Permanente Internet patient Portal: the Organizational Foundations of Information Security. *JAMIA*, 14(2):239–243, 2007.

[11] S. Debaene, R. Van Kuyck, and B. Van Buggenhout. Legislative technique as basis of a legislative drafting system. *Information & Communications Technology Law*, 9(2):149–159, 2000.

[12] P. Guarda and N. Zannone. Towards the Development of Privacy-Aware Systems. *Information and Software Technology*, 2008.

[13] J. Harvánek. *Teorie práva*. Iuridica Brunensia, 1998.

[14] N. Kiyavitskaya, N. Zeni, T. Breaux, A. Antón, J. R. Cordy, L. Mich, and J. Mylopoulos. Automating the extraction of rights and obligations for regulatory compliance. In *Proc. of ER'08*, LNCS. Springer, 2008.

[15] J. Ku. Treaties as laws: A defense of the last in time rule for treaties and federal statutes. *Indiana Law Journal*, 80:319–391, 2005.

[16] M. J. May, C. A. Gunter, and I. Lee. Privacy APIs: Access Control Techniques to Analyze and Verify Legal Privacy Policies. In *Proc. of CSFW'06*, pages 85–97. IEEE Press, 2006.

[17] D. Nute. Defeasible reasoning. In *Proc. of HICSS'87*, pages 470–477. IEEE Press, 1987.

[18] M. Palmirani and R. Brighi. Norma-System: A Legal Document System for Managing Consolidated Acts. In *Proc. of DEXA'02*, pages 295–314, 2002.

[19] D. Patterson. Interpretation in law. *San Diego Law Review*, 42, 2005.

[20] B. Ramesh and M. Jarke. Toward reference models for requirements traceability. *TSE*, 27(1):58–93, 2001.

[21] S. van de Ven, R. Hoekstra, and R. Winkels. MetaVex: Regulation Drafting meets the Semantic Web. In *Proc. of SW4Law'07*, 2007.