COMPUTATIONAL SCIENCE AND TECHNIQUES
Volume 1, Number 2, 2013, 79-92

Publisher: Klaipėda University
http://journals.ku.lt/index.php/CST
Online ISSN: 2029-9966

A SCENARIO TO ACQUAINT WITH THE PROBLEM OF ENGINEERING COMPLIANT SOFTWARE[1]

Vytautas Čyras
Vilnius University, Faculty of Mathematics and Informatics,
Department of Software Engineering, Naugarduko 24, LT-03225 Vilnius
vytautas.cyras@mif.vu.lt

Abstract. Section 1 of this paper follows entirely a scenario from the article "Engineering Compliant Software: Advising Developers by Automating Legal Reasoning" by D. Oberle, F. Drefs, R. Wacker, C. Baumann and O. Raabe, SCRIPTed (2012) 9:3, 280–313, where it serves as a running example. It demonstrates that data transfer violates the law. This motivating scenario has added value in the education of software developers and is worth sharing with the computer communities of other countries including Lithuania. In the scenario, the continental law and EU law sways the particularities of the German law. The motivation for teaching the scenario can be compared with teaching concrete cases in the study of law. Legal reasoning is demonstrated by supplementing the provisions of the German Federal Data Protection Act (FDPA) with those of the Lithuanian Law on Legal Protection of Personal Data, which have the same meaning. In Section 3, we attempt to formulate the software compliance problem. Finally, we explain the notion of subsumption – a legal qualification of facts according to a norm's circumstance. We consider subsumption to consist of two notions: terminological subsumption and normative subsumption.

Key words: regulatory compliance, software development, legal reasoning, legal requirements, subsumption.

Introduction

This paper is inspired by a scenario which is examined in Oberle et al. (2012) on the regulatory compliance problem. Their paper resonated with our thinking. We hold that the scenario is well suited for education. Exploring it can be compared with learning cases *X versus Y* in the study of law. One purpose of this paper is to acquaint software developers with the law. Therefore we discuss the scenario in the context of Lithuanian laws. We aim to replace the provisions of the German Federal Data Protection Act (FDPA), Telecommunications Act (TCA) and Telemedia Act (TMA), by Lithuanian statutory provisions. The following Lithuanian laws are concerned:

- Law on Legal Protection of Personal Data (LLPPD)
- Law on Electronic Communications (LEC)

Textual formulations of the Lithuanian provisions differ from the German formulations, although we hold that the meaning is the same. Software developers are not usually

[1] This work was supported by the project "Theoretical and engineering aspects of e-service technology development and application in high-performance computing platforms" (No. VP1-3.1-ŠMM-08-K-01-010) funded by the European Social Fund.

professionals in law. Therefore textual formulations in the law are a long way from legal requirements that can be interpreted by software developers.

1. Motivating scenario

This section introduces a motivating scenario as a running example.

1.1. Setting

The motivating scenario is limited to the data privacy law. Note, however, that the approach is independent of any particular field of law. We follow the scenario literally (Oberle et al., 2012, p. 283):

"The motivating scenario concerns the fictitious company, "KnowWhere", that offers a "person locator app." This application can be used to track the location of a user who has installed the app on his smartphone. For instance, private customers can use the app to obtain information about the location of their Facebook friends.

As depicted in Figure 1, the person locator app accesses the GPS module of the smartphone and sends the coordinates and a specific Facebook ID to the server application. The server updates the corresponding database entry which also comprises additional information about the person. For obtaining and displaying maps, KnowWhere relies on Google Maps, a service provided by the Google Corporation. Interesting points and locations, defined by GPS coordinates, can be highlighted on a map and marked with the Facebook ID.

Furthermore, KnowWhere offers the "person locator portal" showing maps with the positions of all users that belong to a specified group. The user has to identify himself and specify a group-ID. The server collects all user locations that belong to the given group and uses Google Maps to highlight their positions on the map."

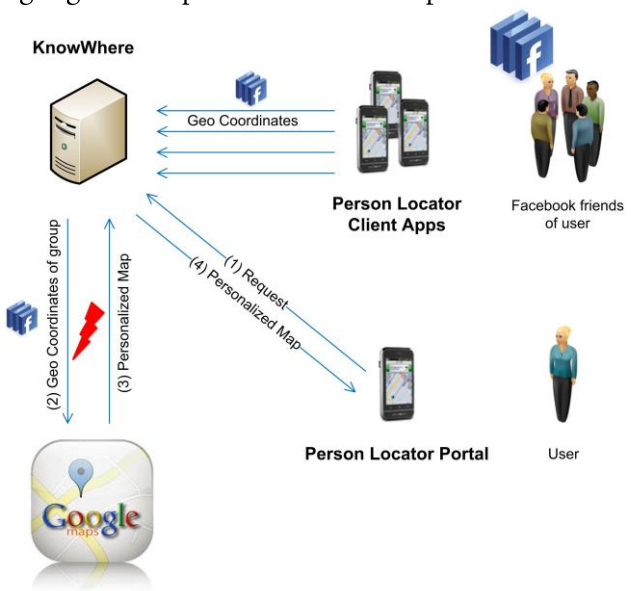

Figure 1. A violation of the Data Protection Act (of both the German FDPA and the Lithuanian LLPPD. This figure is adapted from Oberle et al. (2012), Fig. 3.

The next subsection demonstrates that "the data transfer from KnowWhere to Google can neither be justified by law nor by consent. Therefore, … the conduct of KnowWhere violates data privacy law" (p. 287).

1.2. Manual legal reasoning

The first step of the manual reasoning process is to check whether the data privacy law is applicable. We further follow Oberle et al. (2012, p. 284) to demonstrate the reasoning.

Question 1: Which provision is applicable?

Both the German and the Lithuanian laws define its scope at the beginning. We use small size text and quotation marks below to cite Oberle et al. (2012).

"**Sec. 1 (2) FDPA – Purpose and scope**: This Act shall apply to the collection, processing and use of personal data by … private bodies."	**Art. 1 (2) LLPPD – Purpose, objectives and scope**: The Law shall establish … the rights, duties and liability of legal and natural persons while processing personal data.

KnowWhere is a "private body" (natural person). Therefore both FDPA and LLPPD apply:

"KnowWhere, a "private body" as described by Sec. 2 (4) of the FDPA, discloses Facebook IDs and geo coordinates to other parties, namely, Google Corporation. That would qualify as either a "transfer" of data … or as "use" of data… ." (pp. 284–285)

That would also qualify similarly according to Art. 2 (4) LLPPD – Data processing. Therefore, next is to check whether the data can be classified as *personal*:

"**Sec. 3 (1) FDPA – Further definitions**: "Personal data" shall mean any information concerning the personal or material circumstances of an identified or identifiable natural person ("data subject")."	**Art. 2 (1) LLPPD – Definitions**: Personal data shall mean any information relating to a natural person (data subject) who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

In the next step we have to agree that: 1) Both the user and his friends are "natural persons", 2) Facebook IDs can be identifying information, especially if the IDs feature the full name, and 3) The geo coordinates attributed to the IDs provide further information about the "personal circumstances" of the users (p. 285). Hence, most Facebook IDs and the additional geo data associated with the ID would be classified as "personal data" according to both Sec. 3 (1) of the German FDPA and Art. 2 (1) of the Lithuanian LLPPD.

The next step is to demonstrate that the German FDPA shall only be applicable (p. 285):

"According to Sec. 1 (3) S. 1, the FDPA shall only be applicable if the case at hand is not covered by special legal provisions on data privacy in another legal act. Concerning data handling by private bodies, Sec. 91-107 of the German Telecommunications Act (TCA) and Sec. 11-15a of the German Telemedia Act (TMA) are most relevant.

The TCA contains special data privacy provisions solely for the handling of data by providers of "telecommunication services" as defined in Sec. 3 No. 24. As KnowWhere does not maintain telecommunication infrastructure itself, the TCA is not applicable. Yet, the portal provided by KnowWhere falls within the definition of "Telemedia" in Sec. 1 (1) of the TMA. Whether the data privacy norms in Sec. 11-15a of the TMA overrule the provisions of the FDPA depends on the type of data handled by the telemedia provider. The TMA only covers "inventory data" as defined in Sec. 14 and "usage data" as defined in Sec. 15. The Facebook IDs and the GPS data disclosed by KnowWhere are neither necessary for establishing the contractual relationship with the users, nor for submitting, or invoicing the usage of the portal. KnowWhere does not identify its users by their Facebook IDs, but by their telephone connection. Also, providing GPS data is not necessary to use the personal locator portal as such, but only to enhance its functionalities. Hence, these types of data do not fall under the regime of the TMA.

As a result, the FDPA is applicable."

Similarly, the Lithuanian LLPPD shall be applicable. (The Law on Electronic Communications is not applicable.) Regulation in Germany and Lithuania is similar because of the supremacy of the European Law, namely, directives and regulations including the directives 97/66/EC[2], 2002/58/EC[3] and 2009/140/EC[4].

Question 2: Is the disclosure of user data to Google lawful?

The next step is to check for lawfulness according to both the German FDPA and the Lithuanian LLPPD. The full text of the Article 5 LLPPD is longer than Sec. 4 (1) FDPA. However, item (1) has the same meaning:

[2] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, Official Journal L, 1998-01-30, Nr. 24-1

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L, 2002-07-31, Nr. 201-37

[4] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Official Journal L, 2009-12-18, Nr. 337.

"**Sec. 4 (1) FDPA – Lawfulness of data collection, processing and use:** The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject provided consent."	**Art. 5 (1) LLPPD – Criteria for the Lawful Processing of Personal Data:** 1. Personal data may be processed if: 1) the data subject has given his consent; …

We continue, following pp. 285–286:

"As shown above, the disclosure of Facebook IDs and geo coordinates to Google is either to be qualified as "transfer" that is "processing of data" (Sec. 3 (4) of the German FDPA), or "use of data." Therefore, lawfulness requires either the "permission or order by this Act or other law," or that the "data subject provided consent.""

The same holds for the Lithuanian LLPPD taking into account Art. 2 (4) – "Data processing shall mean any action carried out with personal data: collection, recording, accumulation, storage, classification, grouping, connecting, changing (supplementation or correction), provision, publication, use, logical and/or arithmetical operations, search, dissemination, destruction or any other action or set of actions."

Question 2.1: Is *permission or order by this Act or other law* provided?

Oberle et al. (2012, p. 286) write that "Part III of the FDPA contains the provisions applicable for private bodies (compare Sec. 27 of the FDPA)." In the Lithuanian LLPPD, Art. 5 (1) 2) is applicable:

"**Sec. 28 (1) S. 1 No. 1 FDPA – Collection and recording of data for one's own commercial purposes:** The collection, recording, alteration or transfer of personal data or their use as a means to pursue one's own commercial purposes shall be lawful if necessary to create, perform or terminate a legal obligation or quasi-legal obligation with the data subject, …"	**Art. 5 (1) 2) LLPPD – Criteria for the Lawful Processing of Personal Data:** 2) a contract to which the data subject is party is being concluded or performed;

We further follow p. 286:

"Sec. 28 of the FDPA is applicable only for the handling of data for one's "own commercial purposes." KnowWhere discloses the data to Google in order to be able to provide information about the location of participants and, thus, fulfils the obligation it accepted in the course of providing the app for the users. As this is KnowWhere's "own commercial purpose," Sec. 28 of the FDPA is a suitable permission norm.

Sec. 28 (1) S. 1 No. 1 of the FDPA covers "collection, recording, alteration or transfer" of personal data. According to Sec. 3 (4) No. 3 of the FDPA, disclosure to a "third party"

falls within the definition of transfer. According to Sec 3 (8) S. 2, 3 of the FDPA, a third party is any party other than the controller of private data to whom the FDPA is being applied, in this case KnowWhere, (Sec. 3 (7) of the FDPA) but excluding the persons who are the subjects of the data, and also excluding any parties acting "on behalf of" the data controller. The question is whether Google is a third party, or whether it acts on behalf of the data controller, KnowWhere, as defined in Sec. 11 of the FDPA."

The same also holds according to the Lithuanian LLPPD. We continue (p. 286):

"Sec. 11 of the FDPA lists a variety of requirements ensuring that the data controller is able to monitor and control every step of data handling. KnowWhere has neither negotiated contractual requirements with Google, nor is it able to control or monitor Google's handling of data. Hence, Google does not handle the data on behalf of KnowWhere. Rather, Google handles the data on its own behalf (Sec. 3 (7) of the FDPA). Therefore, Google is a "third party" as defined in Sec. 3 (4) No. 3 of the FDPA. Therefore, the disclosure of the Facebook IDs and geo coordinates of the user's friends is an act of "transfer"."

The same also holds according to the Lithuanian LLPPD. We would also take into account Chapter 9 "Processing of Personal Data and Protection of Privacy" of the Lithuanian LEC. We further follow p. 286:

"The next question is whether the transfer is "necessary" for KnowWhere "to create, perform or terminate a (quasi-)legal obligation with the data subjects." As a key function of the person locator app, KnowWhere promises to provide a service that monitors the current location of the user's friends. Even if KnowWhere is not willing to incur contractual obligations, this relationship can at least be qualified as quasi-legal. Thus, the key question is whether the transfer of the Facebook IDs and the geo coordinates to Google is "necessary" to perform the obligation of monitoring the users' locations. This criterion is two-fold: on the one hand, the processing of data as such is only necessary if the contractual performance cannot be delivered without it in an appropriate way. On the other hand, the data controller has to restrict the amount of processed data to the necessary minimum.

KnowWhere is not reliant on the visual interface of Google Maps in order to monitor current locations. Even if it was, it could use the freely accessible Google Maps data and mark the locations by itself. If KnowWhere still wanted to involve Google in the data provision, it would be sufficient to transfer anonymised or aliased data. All in all, the transfer of the Facebook IDs and geo data to Google is not "necessary" in the sense of Sec. 28 (1) S.1 No. 1 of the FDPA."

A conclusion is that "the data transfer cannot be justified by this provision."

We further agree that "other statutory provisions that permit or order the transfer are not apparent." We would note that a knowledge of law is needed to answer in the affirmative. The conclusion is that "there is no law "permitting or ordering" the data handling by KnowWhere" (p. 287).

Question 2.2: Has the data subject provided consent?

We further follow p. 287:

"Proceeding to the second alternative of Sec. 4 (1) of the FDPA, a lawyer would check for "consent" provided by the data subjects. Operating systems generically ask the user

during installation of an app for access to the smartphone's resources such as the GPS module. An affirmative response would count as a declaration of consent. In order to function as effective consent, declarations would have to fulfil the conditions of:"

"**Sec. 4a (1) FDPA – Effective Consent**: Consent shall be effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use and, as necessary in the individual case, or on request, of the consequences of withholding consent. …"	**Art. 2 (12) LLPPD – Consent** shall mean an indication of will given freely by a data subject indicating his agreement with the processing of his personal data for the purposes known to him. His consent with regard to special categories of personal data must be expressed clearly, in a written or equivalent form or any other form giving an unambiguous evidence of the data subject's free will.

"Due to the generic nature of such questions ("May the app use the GPS module?"), the user is not appropriately informed about the purpose of the collection, processing, and use of his personal data. In particular, the users are not informed about the transfer of personal data from KnowWhere to Google. Therefore, effective consent is not given."

Finally, we agree that "the data transfer from KnowWhere to Google can neither be justified by law nor by consent. Therefore, … the conduct of KnowWhere violates data privacy law" (p. 287).

2. Formalising legal norms

When speaking about formalisations of legal norms, for pedagogical purposes we find it useful here to follow Oberle et al. (2012, pp. 291–294), where a list of references to related approaches is provided. We recall the early works on artificial intelligence and law in the 1980s on modelling legal reasoning and the good old times of Prolog.

Typically, legal norms determine a "legal consequence" (*LC*), given one or more "state of affairs" (*SF*), which fall within the scope of the norm. Schematically, this can be expressed as a logical "rule":

$$SF \rightarrow LC$$

This is to be read as: "when state of affairs (*SF*) is given, then the legal consequence (*LC*) applies." A more general format is:

$$SF_1, SF_2, \ldots SF_n \rightarrow LC_1, LC_2, \ldots LC_m$$

In the example of Sec. 4 (1) of the FDPA (see previous section), the word "only" indicates that there are indeed two *LC*s that must be handled and formalised individually:

- The collection, processing and use of personal data is lawful if permitted or ordered by this Act or other law, or the data subject consented; and
- The collection, processing and use of personal data is unlawful if neither ordered by this Act or other law, nor prescribed by this Act, nor consented to by the data subject.

The next intellectual task for the legal expert is to replace each *SF* and *LC* by elements of the ontology. In a first step, this is achieved by identifying relevant classes. In the example, the *SF*s are replaced by the following classes: Collection, Processing, Use, PersonalData, Permission, Order, Data Subject, and Consent. *LC* is replaced by Lawfulness.

In a second step, explicit links between the chosen classes are inserted by means of relations. The legal norm typically contains indications for such explicit links, e.g., Sec. 4 (1) of the FDPA contains the phrase "use of personal data," which requires the insertion of a performedUpon relation between Use and PersonalData.

In a third step, the legal expert checks for implicit links which are not directly mentioned in the legal norm but are mentally complemented by the interpreter. For example, there exists an implicit link between Consent and the Collection, Processing and Use. Namely, it is the consent that permits such actions.

Finally, the inserted elements of the ontology are logically combined. Ontology languages offer bracketing as well as logical operators (AND, OR) for this purpose. As an example, Sec. 4 (1) of the FDPA entailing lawfulness is formalised as follows:

((Collection(X) OR Processing(X) OR Use(X))
AND performedUpon(X,Y) AND PersonalData(Y))
AND
(Permission(P) OR Order(P)) AND givenFor(P,X)))
OR
(Consent(C) AND DataSubject(D) AND about(Y,D)
AND gives(D,C) AND permits(C,X))
→
Lawfulness(P) AND givenFor(P,X)

X, Y, P, C and D are "variables" that stand for instances of the corresponding class or relation. Their names can be chosen arbitrarily. An expression such as DataSubject(D) can be read as a sentence with an unknown part labelled as D. In turn, D can be bound to a concrete instance, for example, to the user Daniel.

Further note that "formalising the norm graph, as well as the subject matter, is the prerequisite for (semi-)automating the legal reasoning process" (p. 298). Actually, "the main bottleneck of [their] approach is the formalisation of the norm graph" (p. 307). These are still serious problems for research. Therefore we refer the reader to the original article.

3. Formulating the Compliance Problem

Klaus Julisch (2008) suggests a paradigm shift for academia: from "selling" security while organisations seek to "buy" compliance to complementing current security research by additional research into security compliance (p. 71):

"[A]s long as careers are terminated and people go to jail…for failures in compliance – rather than security – the commercial world will continue to pursue compliance rather than security as their primary goal."

This paper is devoted to a broader field, normative compliance, which embraces security regulation as a subfield. In Julisch's definition: "security compliance, in IT systems, is the state of conformance with externally imposed functional security requirements and of providing evidence (assurance) thereof" (p. 72). He defines the security compliance problem as follows:

"**Definition**: Given an existing IT systems *S* and an externally imposed set *R* of security requirements. The **Security Compliance Problem** is to make system *S* comply with the security requirements *R* and to provide assurance that an independent auditor will accept as evidence of the compliance of system *S* with requirement *R*."

Following the definition above, we formulate the problem as follows.

Definition. The software compliance problem is (1) to make software *S* comply with requirements *R* that relate to a law *L*, and (2) to provide assurance that an independent auditor will accept this as evidence (Figure 2).

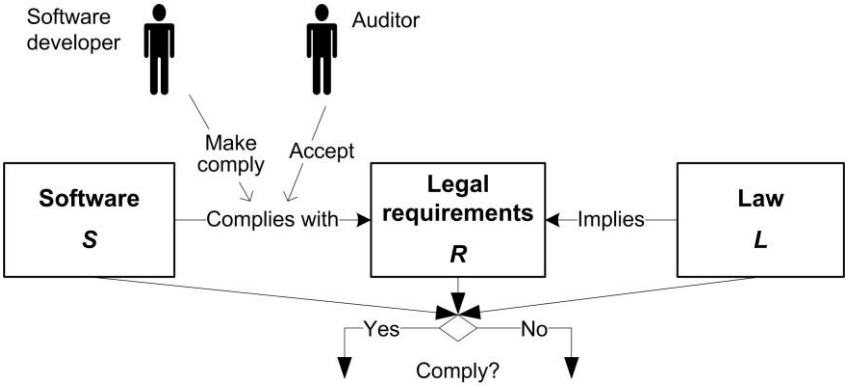

Figure 2. The software compliance problem.

We have simply added a law *L* to Julisch's formulation. The semiformal definitions above can only serve as a first iteration. Problem solutions in practice rarely result in a yes or no. One reason for this is that practice involves more elements and therefore compliance becomes a multi-criteria problem. Feedback loops would improve *S*, *R* and *L*. A conceptualisation of *L* may involve different elements depending on the abstraction level. A legal principle, a whole statute or a specific provision may stand for *L*.

Attempts to formalise the law in the context of the software compliance problem will meet complexity issues. Failure to understand the law is one of the non-compliance reasons. This failure can be examined from the software development perspective and also from the legal perspective. The texts of laws constitute only a part of a whole legal system. The meaning (German *Sinn*) of law – the Ought realm – is difficult to understand from the legal text alone. Therefore it is hard for a freshman to understand the spirit of the law while reading a separate statute. On the other hand, the compliance problem can scarcely be reduced to ticking a box. The law is not easily interpreted for the developers whose purpose is to enforce the law. The following issues raise difficulties, just to name a few:

- *Abstractness of norms*. Norms are formulated (on purpose) in very abstract terms.
- *Principle vs. rule*. The difference in regulatory philosophy between the US and other countries; cf. also the difference between common law and statutory law.

- *Open texture*. This can be illustrated by H. L. A. Hart's example of "Vehicles are forbidden in the park." What counts as a vehicle? Can we make exceptions? Is an ambulance allowed if there is an emergency?
- *The myriad of regulatory requirements*. Compliance frameworks are multi-dimensional.
- *Subsumption*. The subsumption procedure involves an intellectual effort by legal experts.
- *Teleology*. The purpose of a legal norm can usually be achieved in a variety of ways. They do not need to be listed in a statute and specified in detail.
- *Legal interpretation methods*. The meaning of a legal text cannot be extracted from the text alone. Apart from grammatical interpretation, other methods can be invoked, such as systemic and teleological interpretation.

4. Explaining the notion of subsumption

Subsumption refers to the application of the law, or more precisely, the application of a norm to a fact, thus concluding the legal qualification. The English dictionary explains: subsumption – 1. that which is subsumed, as the minor clause or premise of a syllogism; 2. incorporating something under a more general category. Subsumption is central in making a legal decision. Legal qualification, which results in the subsumption procedure within the legal domain, is central for ontologies in law:

"Only the legal qualification of the act gives an answer if a killing (world knowledge) is murder, legal sanction in the form of an execution or allowed act in an international armed conflict" (Schweighofer and Lachmayer, 1997).

We model this in Figure 3.

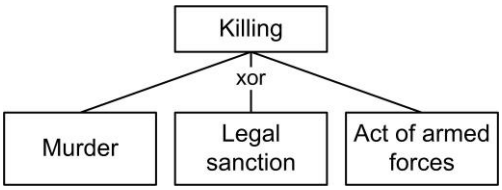

Figure 3. Different legal qualifications of killing.

Similarly, acts involving software within concrete business process workflows can allow different legal qualifications. These acts can be matched with various legal concepts. Therefore subsumption can result in different decisions depending on the concrete case.

We divide the concept of subsumption into two types called *terminological subsumption* and *normative subsumption* (Čyras and Lachmayer, 2013).

The facts of a case are transformed into legal terms. Suppose that an action, a, is treated as a theft, *A*, not a burglary. This corresponds to the first kind of legal subsumption, called *terminological subsumption*. We write a == *A*. The *instance-of* notation of computer science can also be used, a *instance-of A* or the prefix notation *instance-of*(a,*A*). A pool of legal terms is used for the terminological subsumption. This is shown in Figure 4. We use a visualization pattern that is composed of a vertical stage and a horizontal one (Fig. 5). The

two stages depict Hans Kelsen's categorical distinction between Is and Ought (Kelsen, 1967).

The second step is *normative subsumption*. Here the norm $Norm(\forall x\, A(x) \rightarrow B(x))$ is applied to subsume B. The first step, terminological subsumption, corresponds to the unification. It is linked with the minor premise. The second step, *normative subsumption*, corresponds to the major premise $\forall x\, A(x) \rightarrow B(x)$.

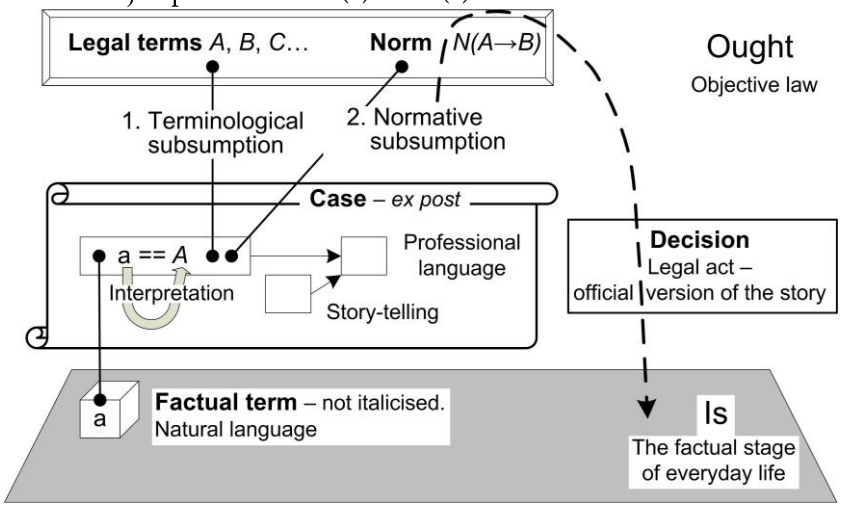

Figure 4. Subsumption: the facts are assigned the legal qualification in accordance with a norm.

The conceptualisation above reflects inference with a syllogism (cf. also the *modus ponens* rule):

Minor premise: Socrates is a human.	$human(Socrates)$
Major premise: Humans are mortal.	$\forall x\, human(x) \rightarrow mortal(x)$
Conclusion: Therefore, Socrates is mortal.	$mortal(Socrates)$

4.1. Modelling terminological subsumption

To model the subsumption procedure, conceptual modelling formalisms which are used in computer science can be applied. General relationships such as *is-a*, *instance-of* and *part-of* are used in object-oriented analysis and systems development. Suppose the fact that *my-door* is open and the norm N "The doors ought to be closed". The norm can be formalised with the following rule: if x is an instance of *Door*, then x ought to be closed. Formally, $\boxtimes\forall x\ x \in Door \Rightarrow O\ closed(x)$, where O is the deontic operator and *closed* a predicate. A situation (i.e., a fact) with the instance *my-door* is from the Is world. The fact is interpreted according to a norm from the Ought world which contains the door concept *Door*. Then *my-door* is *matched* with *Door*, formally *match*(*my-door, Door*). This can be simplified and expressed with a truth statement *instance-of*(*my-door, Door*) or $my\text{-}door \in Door$. This truth statement is from the Is world. A graphical notation is shown in Figure 5. A duty which is conferred on me, to close *my-door*, is from Ought. In the Is world I can decide to leave *my-door* open, thus violating the norm.

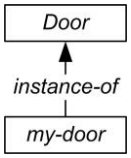

Figure 5. Graphical notation of the instance-of relationship, *instance-of(my-door, Door)*. This visualizes that *my-door* (from the Is world) is matched with the term *Door* within the norm *N* which is from Ought.

Finally, the subsumption procedure is illustrated in Figure 6. A fact a is qualified as a legal term *A*. The norm $A \rightarrow B$ is applied. The conclusion is *B*(a). Suppose that the law comprises other norms, e.g., *A*, $C \rightarrow D$.

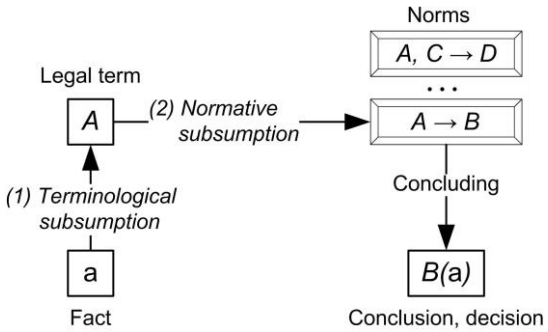

Figure 6. The subsumption procedure.

Next it is worth noting that application of the law has to avoid formalism (mechanistic approaches). This is stressed in legal theory. The idea of constructing a subsumption machine (German *Subsumtionsautomat*, "mechanistic judge") is rejected; see Ogorek (1986), pp. 212, 292ff.

To sum up, we aim to contribute to the problem of relation between fact and circumstance (German *Tatsache und Sachverhalt*). Our approach can be treated as formalisation through symbolisation.

4.2. On legal informatics

Legal informatics can be defined with the metaphor of constructing a bridge between law and informatics. A way from legal provisions to software developers means constructing the bridge in the direction from law to informatics. The compliance problem can be raised in the opposite direction: is a software design decision compliant with the law? This implies a way from informatics to law. This paper demonstrates that the bridge has to be built from the two banks: both from law and from informatics. Intermediate pillars such as formalising the legal concepts and legal norms are important.

Conclusions

This paper can serve as a short tutorial. The idea of the KnowWhere application can be formulated in a few words. The compliance problem can also be formulated laconically: is the law violated or not violated? Although the reasoning used to obtain the answer is not trivial, the software developer is capable of understanding it. The reasoning is important for the development of applications which seem to provide value-added functionality, but will in fact be spying on the user.

To reach a decision whether an action complies with a norm is often not trivial. In any given case all the circumstances have to be weighted. For example, crossing the street on a red light violates the road rules, although it may be justified in the case of an emergency. Hence, only a legal expert can answer the compliance problem in the affirmative. The present paper aims to demonstrate this statement.

Next we provide a definition of the software compliance problem. We list some complexity issues which can lead to a failure of understanding the law and to non-compliance.

Finally, the notion of legal subsumption is explained. This can be treated as an attempt at formalisation through symbolisation. A novelty is that the notion of subsumption is divided into two types – terminological subsumption and normative subsumption.

References

Bonazzi, R., Hussami, L., Pigneur, Y. (2009). Compliance management is becoming a major issue in IS design. In: A. D'atri, D. Saccà (Eds.) Information Systems: People, Organizations, Institutions, and Technologies, Springer, pp. 391–398, http://people.hec.unil.ch/ypigneur/files/2010/01/complianceManagement.pdf.

Čyras, V., Lachmayer, F. (2013). Situation versus case and two kinds of legal subsumption. In: E. Schweighofer, F. Kummer (Eds.) Abstraction and Application, Proceedings of the 16th International Legal Informatics Symposium, IRIS 2013, 21–23 February 2013, Universität Salzburg, Österreichische Computer Gesellschaft, Wien. Also in electronic journal Jusletter IT. Die Zeitschrift für IT und Recht, February 2013, Editions Weblaw, Bern, http://jusletter-eu.weblaw.ch/issues/2013/IRIS.html.

Julisch, K. (2008). Security compliance: the next frontier in security research. In: Proceedings of the 2008 Workshop on New Security Paradigms, NSPW'08, pp. 71–74, ACM, http://www.nspw.org/papers/2008/nspw2008-julisch.pdf.

Kelsen, H. (1967). Pure Theory of Law. 2nd ed., Max Knight, translator. University of California Press, Berkeley, CA.

Law on Electronic Communications, 15 April 2004 No. IX-2135, Lithuanian Gazette, 2004, No. 69-2382, http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=242679.

Law on Legal Protection of Personal Data, 11 June 1996, No. I-1374 (As last amended on 12 May 2011, No. XI-1372). http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=435305.

Oberle, D., Drefs, F., Wacker, R., Baumann, C., Raabe, O. (2012). Engineering compliant software: advising developers by automating legal reasoning. SCRIPTed 9:3, 280–313, DOI: 10.2966/scrip.090312.280 [interactive], http://script-ed.org/wp-content/uploads/2011/12/oberle.pdf.

Ogorek, R. (1986). A king of judges or a subsumption machine? [in German: Richterkönig oder Subsumtionsautomat?] Klostermann, Frankfurt am Main.

Schweighofer E., Lachmayer, F. (2007). Ideas, visualisations and ontologies. In: Proceedings of the First International Workshop on Legal Ontologies LEGONT '97, July 4, 1997, University of Melbourne, Law School, Melbourne, Victoria, Australia, pp. 7–13. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.50.6614.

V. Čyras is a docent (associate professor) in computer science at Vilnius University. In 1979 he graduated from Vilnius University. In 1985 he received a doctoral degree (candidate of sciences of physics and mathematics) from M. V. Lomonosov Moscow State University. In 2007 he received a master of law degree from Vilnius University. His research interests include computer science, law and legal informatics.

SCENARIJUS PRISTATYTI SU TEISE SUDERINAMOS PROGRAMINĖS ĮRANGOS INŽINERIJĄ

Vytautas Čyras

Santrauka

Pristatomas scenarijus iš Daniel Oberle et al. straipsnio e. žurnale SCRIPTed (2012) 9:3, kur jis nagrinėjamas kaip pavyzdys. Jis demonstruoja, kad duomenų perdavimas tarp įmonių gali prieštarauti teisei. Šis scenarijus yra gerai motyvuotas, gali būti etalonu mokinant programinės įrangos kūrėjus ir tinka pristatyti Lietuvos kompiuterininkų bendruomenei. Supažindinimas su juo panašus į precedentų nagrinėjimą teisės studijose. Demonstruojant teisinį samprotavimą, Vokietijos duomenų apsaugos įstatymo nuostatos keičiamos Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymo formuluotėmis. Kaip atskiras rezultatas formuluojamas programinės įrangos suderinamumo su teise uždavinys. Toliau aiškinama teisės taikymo (subsumcijos) sąvoka kaip fakto teisinis kvalifikavimas sutinkamai su teisės normos hipotezėje įtvirtintais požymiais. Mes siūlome subsumcijos sąvoką skaidyti į dvi: terminologinę subsumciją ir norminę subsumciją.

Pagrindiniai žodžiai: norminis suderinamumas, programinė įranga, teisinis samprotavimas, teisiniai reikalavimai, subsumcija.