Contractual Risk Management in an ICT Context – Searching for a Possible Interface between Legal Methods and Risk Analysis

Tobias Mahler & Jon Bing

1 Introduction

In Richard Susskind's book *The Future of Law*,[1] the author predicts a paradigm shift in the approach to a legal problem: From *problem solving* to *problem prevention:*

> "While legal problem solving will not be eliminated in tomorrow's legal paradigm, it will nonetheless diminish markedly in significance. The emphasis will shift towards legal risk management supported by proactive facilities, which will be available in the form of legal information services and procedures. As citizen learn to seek legal guidance more regularly and far earlier than in the past, many potential legal difficulties will be dissolved before needing to be resolved. Where legal problems of today are often symptomatic of delayed legal input, earlier consultation should result in users understanding and identifying their risk and controlling them before any question of escalation."

This raises the questions of what kind of methods a lawyer can employ to ensure legal risk management. The conventional legal method commonly discussed in legal literature focuses on identifying which law applies to a given case (*"da mihi facta dabo tibi jus"*). In this sense, it is a reactive method. We may look for additional or supplemental methods in other disciplines. One possibility is obviously to use the methods for risk analysis developed for system analysis or security management, and apply these in addition to conventional legal methods. But in order to apply such a method of risk analysis to legal issues, we need to identify the interfaces between existing legal methods and risk analysis or management.

2 Motivation

The phrase "legal risk management" is frequently used for instance in the marketing efforts of law firms to advertise or promote their services, mainly addressed to the corporate client.

"Risk management" is a technical phrase generally understood as a set of co-ordinated activities directing and controlling an organisation with respect to "risks" of a nature to be specified. Disciplines like engineering, economics or computer science use a variety of methods to manage risks of different kinds related, for instance, to products, markets, or information systems. The "risk" may be economic loss, reduction of integrity or security of a system, delays in system development, *etc*.

The use of the term "risk management" in a legal context seems to imply that there is a clear understanding of how methods for risk management can be applied within the legal domain. However, in the examples examined, the phrase is used only in its more every day understanding, indicating that lawyers will

1 Susskind, Richard, *The Future of Law*, Clarendon, Oxford 1998, p. 290.

offer their services to clients with the objective of reducing risks, typically of an economic nature, but also for running into future disputes (with the implied costs and economic uncertainty of such a situation).[2] The use of the phrase is rarely explained with reference to a certain methodology.

So far no generally accepted methodology for legal risk management has been developed, and we are only starting to understand the implications of relating some of the methods from the repertoire of risk management to legal problems.[3]

The focus on risk management in the present paper is motivated by the need for a proactive legal analysis, which identifies probable or possible future problems, and which seeks to mitigate these. The proactive approach may be seen in contrast to the more traditional reactive approach of legal analysis, which has concentrated on determining the applicable law after the problem has occurred in real life. A proactive legal analysis also includes elements which determine the relevant law, but in addition it needs to deal with an unknown future in which the client[4] wants to protect his assets (of a certain nature) from crumbling.

A proactive perspective is not novel in itself; private practicing lawyers have always looked to the future in advising their clients, as indeed mentioned in their description of their own services. But at least in Europe, the proactive approaches seem not to have been extensively examined by academic lawyers, neither in research, nor in the teaching proactive methods to law students. Legal theory provides relatively modest guidance for a proactive legal analysis.

The needs for improved proactive methods require that lawyers direct their attention towards the methods developed within other disciplines, to assess their utility within the legal domain. Risk management has been developed and used for engineering, computer security or financial investments – in these cases, the risks can be identified, analysed and addressed in a structured way. This paper will make an initial examination to what extent, and in which way, such methods for risk management may be applied within the legal domain.

Risk management could in principle be applied to a number of different legal tasks and issues, and the choice of method may depend upon the nature of the task or issue addressed. For example, if the task is to analyse a particular planned activity, the risk management could concentrate on compliance with the existing legal norms flowing from regulations[5] or contracts.[6] Focusing on compliance may require certain risk management methods, which may differ

---

2 The phrase is used in this sense also in legal literature, a recent example is Trzaskowski, Jan, *Legal Risk Management in Electronic Commerce – managing the risks of cross-border law enforcement*, PhD thesis, Copenhagen Business School autumn 2005 (ms).

3 *Cf.* Wahlgren, Peter, *Juridisk riskanalys*, Jure, Stockholm 2003.

4 In this paper, and for the sake of argument, it is presumed that the lawyer acts in the interest of a certain client who operates a business or other enterprise.

5 In this paper, ”regulations” will be used as a term including both statutory instruments and subordinate instruments issued under the authority of these – the exact terminology applied to such instruments will vary between jurisdictions.

6 By ”contract” we refer to an agreement between two or more parties, binding under the law on basis of the private autonomy of the parties.

from those appropriate if the focus is not compliance with existing norms, but rather designing new rules by formulating the clauses of a contract to be negotiated. The contract is designed to manage risks of another nature than deviation from the governing law; the risks will in such a situation typically be implied by the nature of the enterprise to be governed by the contract under development.

The choice of methods may also be related to the nature of the legal issue to be analysed, and the kind of assets which are to be protected. In drafting a clause in a contract related to financial matters, the attention should be directed towards methods of financial risk management. If the asset at stake is "information"[7] rather than money, we may have to employ different methods, for instance those used for information security.

This paper therefore does not address any and all types of legal tasks or legal issues. It concentrates on methods for drafting provisions governing information flows, in order to consider how methods of risk management may be utilised to improve and enrich the more traditional methods applied by lawyers.

In the following sections we will

- Describe the method of a conventional legal analysis (Section 3);
- Introduce risk management and analysis as these methods are used in other disciplines (Section 4);
- Review existing proactive legal approaches (Section 5) and
- Discuss how contract drafting can be improved through risk analysis (Section 6).

3 Conventional Legal Analysis

A conventional legal analysis is rather informal, and may be characterised as a legal argument, consisting of a sequence of activities, basically comprising:[8]

- Exploring the legal issue to be addressed (the facts in context, the "problem");
- Retrieving possible legal sources (regulations, case law *etc*);
- Identifying which of the retrieved sources are relevant;
- Interpretation of the relevant sources to understand the existence or detailed content of the legal norms which can be based on them;
- Possible harmonisation between conflicting norms which may be applied;
- Representing the resulting understanding of the applicable norms to the fact (decision, recommendation or otherwise).

---

7 In this paper, "information" is used in an informal meaning, the distinction between "data" and "information" often made in computer science is not made.

8 *Cf.* Bing, Jon (ed.), *Handbook of Legal Information Retrieval*, North-Holland, Amsterdam 1984, p.6-49.

This can also be resented by a simple flow diagram:

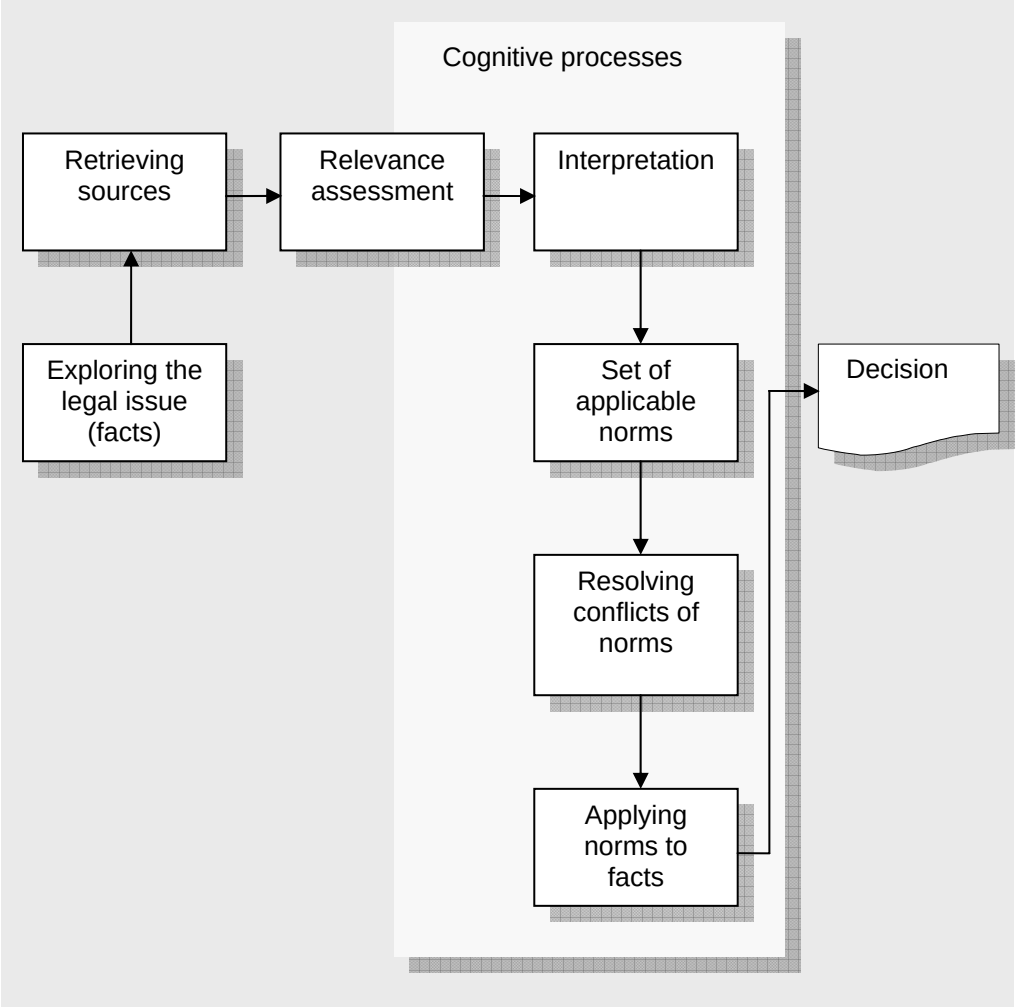

Figure 1. Legal decision process

A legal issue – the "problem" – is always the basis of a legal argument. The problem may be specific, like a case before the court, or more general, as would be the basis for a legal text book.

The applicable legal norms, or the law to be applied to the problem, must always be based on legal sources. A "legal source" is a phrase used to indicate those instruments qualified by the legal meta-norms within a jurisdiction on which the argument for the existence or content of a legal norm must be based. The distinction between a legal norm and another type of norm (social, ethical, moral *etc*) is determined by whether the norm is based on legal sources.

What is to be qualified as a legal source, will partly be determined by the sources themselves, primarily those which (according to the same meta-norms) have a high rank. There is no known instance of an exhaustive list of such sources being formalised, therefore it will eventually have to be based on a consensus in the lawyer community, and the status of some types of sources may be contested (as are the decisions by first and appellate instance court decisions

in Norway). Typically, the sources are the constitution, statutes, secondary legislation, decisions by supreme courts, and legal literature. The types vary between jurisdictions, for instance legislative history is a source used intensively in Norway, but generally not recognised in the United Kingdom.

Lawyers will rely on different strategies to retrieve sources that may be relevant[9] to an issue. One major strategy relies on legal background knowledge – a lawyer may obviously have extensive prior experience from similar issues and will therefore know where to look for possible relevant sources, for instance which sections of the statutes may apply. Another major strategy relies on using knowledge of the facts embedded in the legal issue, converting these into a search request that can be used in conjunction with an available information retrieval system. There may be several available, from back-in-the-book indexes to sophisticated computerised systems.[10] Hyperlinks will be part of the retrieval tools, enhancing the traditional way of linking sources through citations.

The sources will typically be texts.[11] The texts are subject to interpretation. The process of interpretation may be trivial, reduced to a question of "reading" the texts. But it may also be more sophisticated, in which the doctrine on interpretation will govern the process. This is qualitatively different from "reading" or "understanding" a non-legal natural language text, for instance there will be norms governing the use of legislative definitions, inter- or intra-consistency between regulations, analogue reasoning *etc*.

The interpretation process is also a learning process, through interpretation the lawyer understands more of the legal issues, and may have to re-explore the problem to disclose more facets of the issue, or to retrieve supplemental legal sources. This implies that the process is iterative, and has to be repeated until the lawyer either finds that he or she has arrived at an appropriate understanding of the law governing the issue, or – more trivial, but perhaps more common – simply runs out of resources measured in time or costs.

The texts are of a syntactic nature, the understanding of the texts of a semantic nature; it is a cognitive process in the mind of the lawyer arguing the issue. It may be described as arriving at an understanding of the norms governing the issue, "norm" being somewhat further explained below. In some cases, the sources may contain sufficient leeway for there being available more than one set of norms with outcomes that cannot simultaneously be applied – in such a case, there is a conflict of norms which is solved by harmonisation. There are several principles for harmonisation, one being *lex superior* (a norm based on a source of higher rank is given predominance over a norm based on a source of lower rank) or client loyalty (the norm most favourable to the client is chosen). Also, the process of interpretation itself may have as an objective to remove possible conflict of norms. To some extent, the lawyer may have a

9 The notion of "relevance" is not trivial, but will not be pursued here, see Bing, Jon (ed.) *Handbook of Legal Information Retrieval,* North-Holland, Amsterdam 1984, p. 197-203.

10 Lawyers were actually the first profession to computerize all their primary sources and make them on-line for retrieval, in Norway the first commercial system was launched in 1981.

11 There may be exceptions, for instance customary law, but these examples are of little consequence in the context of this paper.

choice between harmonising the arguments in such a way that no conflict appears, or to construct the arguments in order to identify conflicting norms, which then are harmonised.

In principle the process of interpretation and harmonisation takes place in the mind of the lawyer. Obviously, the process has to be represented – and the lawyer will ideally not be an oracle coming up with an applicable norm solving the issue, but report on the process, explaining the sources identified as relevant, which problems of interpretation and harmonisation have been encountered, including how they have been resolved, and why the lawyer has chosen this strategy. This will lead up to the reasons (or justifications) for the decision.

If the legal analysis concerns a contract, the legal method must reflect the nature of contracts. A contract is a document explicating the rights and duties between two or more parties. In this context, a "contract" is qualified as a written document, while a binding agreement does not have to be in writing.[12] Otherwise, the terms "contract" and "agreement" are often used as synonyms.

A contract has to be contained within the applicable regulatory norms. Typically, these norms are wide, and the situation is often described as giving the parties "freedom" to draw up contracts regulating in practice anything, and any side of the co-operation. However, the regulations will censor some contractual clauses.[13]

In principle, the contract is a legal source, but of a different kind from the other legal sources mentioned above. Regulations are based in the authority of the legal system, which ultimately is derived from the constitution.[14] The contract is based on the authority of the parties as natural or legal persons, which have the freedom to bind themselves legally by accepting duties. The legal system will back this up by resources for enforcing the contracts, typically through the court system and executive authorities, in case of a violation of the contractual duties.

Conventional legal methods facilitate the solution of legal problems through the identification of the applicable law, but they give little guidance to the proactive identification of risks or effective treatments of such risks.

4 Risk Management and Risk Analysis

All types of undertaking may be faced with situations that constitute both opportunities for benefit and threats to their success. Risk management relates to the analysis of these situations, and provides a set of methods for reasoning about such risks. Risk analysis is one of the tasks included in risk management.

---

12 This is subject to the law on the formation of agreements within the jurisdiction; in Norway no formality is required, an oral agreement is in principle equally binding to a written agreement.

13 The traditional Norwegian statutory provision being that contracts have to be within the limits of "decency and good faith", the immediate wide sense of this phrase having been exemplified and made more stringent by case law over the centuries.

14 Or, in the rare instances of jurisdictions lacking a constitution, some basic norms are typically of customary nature.

This section introduces a taxonomy for risk management and briefly summarizes how the method is understood selected other disciplines.

4.1 Taxonomy

The term "risk management" can be defined according to the vocabulary for risk management in standards, provided by the International Organisation for Standardisation.[15]

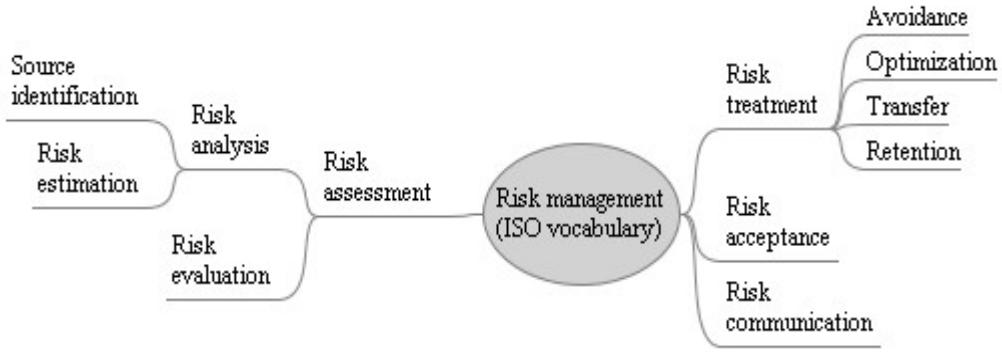

Figure 2. ISO risk management vocabulary

Risk management is understood by ISO[16] as a set of co-ordinated activities to direct and control an organisation with regard to risk. The term "risk" is understood as the combination of the probability of an [unwanted] event and its consequences.[17] A closer analysis of this and other definitions of risk will have to determine whether this definition is appropriate for the legal domain.[18] According to the ISO vocabulary, risk management consists of

- Risk analysis, i.e. the systematic use of information to
  - identify sources (items or activities having a potential for a consequence)
  - and to estimate the risk. i.e. assign values to
    the probability of a risk, and
    the consequences of a risk
- Risk evaluation, i.e. the process of comparing the estimated risk against given criteria;

15 ISO, *Risk management – vocabulary – guidelines for use in standards,* Guide 73, 2002.

16 ISO, *ibid*, definition 3.1.7.

17 ISO, *ibid*, definition 3.1.1.

18 For an analysis of the term "risk" in contract law, see Keskitalo, Petri, *From assumptions to risk management: an analysis of risk management for changing circumstances in commercial contracts, especially in the Nordic countries: the theory of contractual risk management and the default norms of risk allocation,* Kauppakaari, Helsinki 2000, p. 47-75.

- Risk treatment, i.e. the process of selection and implementation of measures to modify risk by avoiding, minimising, transferring or retaining the risk;
- Risk acceptance, i.e. the decision to accept a risk;
- Risk communication.

4.2 Enterprise and Financial Risk Management

Legal risk management should be related to the organisational and financial aspects of e.g. a contract. Therefore, a potential source for legal risk management comes from enterprise risk management and financial risk management. The latter provides a methodology for reasoning about financial risks, particularly with respect to financial products and their interplay in portfolios.[19] Financial aspects are also relevant to the field of enterprise risk management. This is defined as the

> "process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.[20]

4.3 Security Risk Management

Risk management methods from the information security domain are of particular interest to this paper, because they are concerned with risks in relation to information and information systems. Risk management is already being widely used with respect to security, in particular information security,[21] in order to identify, analyse and treat security risks. Risk analysis methods for information systems focus on the identification of security incidents, e.g. hacker attacks, and provide a structured analysis in order establish effective treatments, e.g. improvements in the information system. However, it is also possible that legal measures, like a confidentiality clause in a contract, may reduce certain information security risks. The use of methods from security risk management in a legal context will be discussed below in Section 6.3.

---

19 Allen, Steven, *Financial risk management: a practitioner's guide to managing market and credit risk,* Wiley, Hoboken, N.J. 2003.

20 Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise risk management framework,* 2004, an executive summary is available at "www.coso.org/ Publications/ ERM/COSO_ERM_ExecutiveSummary.pdf".

21 See, e.g. Seip, Annikken Bonnevie, *Hvem sin risiko? Risikovurdering av sikkerhetsopplegg med eksempler fra saksbehandlersystemer,* in Arild Jansen and Dag Wiese Schartum, *Informasjonssikkerhet: rettslige krav til sikker bruk av IKT,* Fagbokforlaget, Bergen 2005.

5 Existing Proactive Legal Approaches

Literature on legal risk management seems to be rather limited, despite the interest for risk management methods by the legal practitioner. This section introduces some of the current Scandinavian[22] approaches to legal risk management and the US theory of preventive law.

Both legal risk management and preventive law have the objective to introduce new methods to the legal domain by linking law to proactive methods from other disciplines. While the comparatively more recent theories of risk management are based on methods from engineering and business management, preventive law, dating back from the 1950s, also draws on the experience from preventive medicine.

5.1 Methods for Legal Risk Analysis

Peter Wahlgren[23] concentrates on risk analysis, i.e. one central element in a risk management process. Risk analysis methods, including fault tree analysis, matrixes, checklists *etc*, are compared to typical risk related legal work tasks, in particular legal analysis and contractual analysis. Wahlgren's main conclusion is that the methods of risk analysis can support many of the tasks as complementary methods.

However, there appear to be a number of challenges and limiting factors related not only to the traditions and education of lawyers, but also to the nature of law, where legal expert judgements play a significant role. This nature may pose some limitations for the possibilities to formalise the reasoning about legal risks.

5.2 Contractual Risk Management for Changing Circumstances in Commercial Contracts

Petri Keskitalo provides an analysis of risk management for changing circumstances in commercial contracts, and puts forward a "theory of contractual risk management and default norms of risk allocation", building on elements from the legal theory of contracts and transaction cost economics.[24]

The theory of contractual risk management itself consists of five phases:

- Identification of business strategies, where non-legal aspects of business management dictate the goals of commercial transactions;

---

22 Interestingly, the search for more detailed literature on legal risk management or risk analysis outside Nordic law has so far not been successful. Further search for such literature or risk management is expected to clarify if the academic interest for risk management is a Scandinavian phenomenon.

23 Wahlgren Peter, *Juridisk riskanalys*, Jure, Stockholm 2003.

24 Keskitalo, Petri, *From assumptions to risk management: an analysis of risk management for changing circumstances in commercial contracts, especially in the Nordic countries; the theory of contractual risk management and the default norms of risk allocation*, Knauppakaari, Helsinki 2000.

- Identification and evaluation of risks, based on transaction cost economics and the default norms of risk allocation;
- Spotting and reconstructing of alternative contractual "tools" for risk management;
- Evaluation and forecasting of the viability of the alternative tools for risk management, and
- Contractual allocation of risks.

The practical second part of the work focuses mainly on the identification and evaluation of risks, based on transaction cost economics and the default norms of risk allocation. Keskitalo's approach regarding the risks related to changing circumstances is rather close to the established legal theory, where this is a classical issue. The issue is related to contractual doctrines like impossibility, reasonability, commercial impracticability and mistakes. The contractual allocation of risks has always been central in contract literature, and will be a central element of contractual risk management.

Despite some terminological divergences, the theory of contractual risk management shows clear similarities with the way risk management is understood e.g. by the ISO. Keskitalo's theory of contractual risk management focuses in the risk identification phase on the default norms of risk allocation. These default norms are of course being identified and interpreted according to the traditional legal method as described in Section 3 above. Keskitalo also incorporates a phase that corresponds to the risk treatment, i.e. the process of selection and implementation of measures to modify risk by avoiding, minimizing, transferring or retaining the risk, which he denominates "spotting and reconstructing of alternative contractual 'tools' for risk management".

5.3 Legal Risk Management

Iversen[25] provides a rather practical approach, which mainly seems to be based on methods from enterprise risk management. He understands legal risk management as an integral part of corporate governance.[26] Iversen refers to an OECD definition, according to which corporate governance focuses on "[t]he relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined."[27] Consequently, Iversen focuses on the broad picture of risks for an enterprise and describes how enterprise-internal as well as external lawyers can identify, evaluate, handle and control legal risks and possibilities. Iversen covers the following areas of enterprise-focused legal risk management:

---

25 Iversen, Jon, *Legal Risk Management*, Thomson, Copenhagen 2004.

26 Iversen, Jon, *ibid*, p. 85.

27 OECD, *Experiences from the Regional Corporate Governance Roundtables*, 22 March 2004, as quoted by Iversen, *ibid*, p. 15.

- Structural risk management refers to the enterprise's legal and organisational structure, which will play a major role in relation to liability risks and risks related to criminal law.
- Regulatory risk management is related to the enterprise's compliance with the legal framework, and can be carried out through compliance programmes.
- Contractual risk management focuses on the risks related to contracts entered into by the enterprise. For this purpose Iversen includes manuals in contracting and contract dissolution. This understanding of contractual risk management seems to be based rather upon a collection of experiences than on analytical tools.
- Litigation risk management concentrates on fighting or defending a case in a court of law.
- Document risk management is an important part of enterprise risk management and covers risks related to electronic or paper-based documents.

5.4 Preventive Law

The theory of preventive law has its basis in the United States, where it was established by Louis M. Brown. The approach can be summarized as follows:[28] Preventive law is comprised of legal and practical principles for anticipating and avoiding legal problems. The goal of preventive law is to provide for the "legal health" of individuals and business entities. The concept is a familiar one in the context of medicine. Preventive law is based on the assumption that there is a clear recognition that the most successful medical treatment is prevention. Preventive law focuses, for example, on how to prevent liability, e.g. product or environmental liability, or how to perform a legal audit, i.e. performance audit that is aimed at assessing an organization's success and effectiveness in law compliance. This approach was established in the 1950s and seems to be based on the concept of prevention in medicine. Although preventive law was established prior to the emergence of enterprise risk management[29] and corporate governance, the two concepts do not contain major contradictions.

5.5 Emerging Methods for Legal Risk Management

This brief overview illustrates that the existing approaches to a proactive legal method differ in their focus and origin rather than in their substance. The difference between Keskitalo's theory and Iversen's approach seems to originate from the distinct perspectives: While Keskitalo takes a micro perspective, on a

---

28 Gruner, Richard S., *Introduction to preventive law*, on-line course, lesson 1, available at "www.cyberinstitute.com/preventivelaw/". For more details on the concept see Brown, Louis Morris, *Preventive law*, Westport, Conn., 1970.

29 According to Field, Peter, *Modern risk management, a history*, Risk Books, London 2003, p. XXV, the key theoretical bases for the development of (enterprise) risk management were established in the 1970s and 1980s.

single contract, is Iversen's focus on risk management in a wider perspective, i.e. on legal risk management for a corporation. This difference in perspective is illustrated by Figure 3.

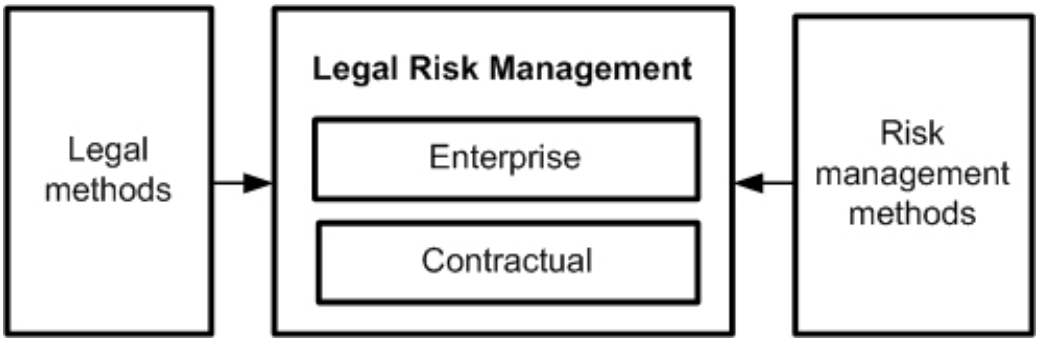

Figure 3. Macro (enterprise) and micro (contract) perspective on legal risk management

The more general enterprise-wide legal risk management defines risk criteria, which can be used in a more specific risk assessment in relation to a contract. And vice versa: the results of the contract risk analysis will most probably be a valuable input and feedback to the enterprise-wide process. The risk assessments at both levels will need to be based on an integration of legal methods with risk analysis methods. Some of the latter methods may be chosen from the methods surveyed by Wahlgren. Hence, it does not seem impossible to integrate these different approaches into one set of methods for legal risk management. Moreover, this integrated proactive legal method would also benefit from a convergence of preventive law and legal risk management.

However, further research will need to clarify how the different approaches to legal risk management/preventive law can be integrated and to clarify the extent to which more formal risk analysis methods make sense in the legal context. In the following section we will concentrate on how risk analysis methods can be utilized when drafting a contract.

6 Drafting Contracts based on Risk Analysis

Risk analysis could in principle be applied to many different situations. The task could be as broad as a general legal audit covering any type of risks facing an organisation. For the purpose of this paper, however, the attention is restricted to a more specific situation: How can risk analysis be used proactively when drafting a contract?

Lawyers will often base contracts on pre-existing templates, model contracts or checklists, or existing contracts which address a similar issue. This saves time and effort and may contribute to the rapid creation of a contract of adequate quality. However, one may explore whether it would be possible to use risk analysis as a complementary method which could assist in creating a contract better adapted to the situation to be governed by the contract. It may also be

helpful to have a clear picture of the risks, including those addressed in the contract, those omitted and possible risks that may evolve from the use of the contract itself.

This section discusses some of the terminological and conceptual challenges that need to be addressed before we apply risk analysis for drafting a contract.

6.1 Terminology

The terminologies of risk management and law appear as two separate vocabularies implying different conceptual frameworks. These need to be related and integrated. It may be tempting for a lawyer to choose the legal terminology, which the lawyer may argue he or she already understands in some detail, as a basis for integration, i.e. to study risk management in legal terms. However, this paper is based on a different decision; proactive legal analysis will be studied in the perspective of risk management.

The vocabulary of risk management defined by ISO will be used as a basis in order to avoid that terms used will deviate from established practice in risk management, and to ensure that legal risk management can be integrated with risk management processes conducted by experts in other disciplines. Therefore, terms related to legal risk management will only be defined differently if this is necessary in order to ensure meeting the requirements or needs of a specific legal nature. The decision to frame the analysis in the perspective of risk management is motivated by the expectation that this may allow us to understand and describe aspects of legal practice that are difficult to observe or express as long as we do not leave the traditional paths of legal reasoning.

The following working definition of legal risk management can be used as a basis for further research:

> Legal risk management is here understood as a set of co-ordinated activities to direct and control an organisation or a relation between organisations with respect to (1) legal risks and (2) other risks thatcan be “treated” by legal means.

The system could be an information system, or a system of contractual provisions – or even the integration of contractual provisions with the policies of an information system. The term legal risk in a wider sense may include all risks related to legal norms. In the narrow sense the term legal risk can be used for those risks which include a normative event (see section 6.2).

The term “risk” is in the ISO vocabulary defined as the combination of probability of an [unwanted] event to occur, and its consequences.[30] Further research will need to clarify to what extent this understanding is useful in a legal context. The usefulness of analysing consequences – in particular legal consequences – of events is beyond any doubt. However, future research will need to consider to what extent reasoning about probabilities is useful in legal

30 ISO, *Risk management vocabulary, guidelines for use in standards*, Guide 73, 2002, definition 3.1.1.

risk management. So far, proactive reasoning about probabilities – in particular quantitative calculations – is rather unfamiliar for lawyers.[31]

6.2 Risk Analysis

Particular attention should be paid to risk analysis, i.e. the systematic use of information to identify causes to, and the estimation of the probability of consequences of risks.

In a legal risk analysis we may need to distinguish between *normative* and *non-normative events*. An event can be understood as "normative" if it follows from the application of a norm, as illustrated in Figure 4.

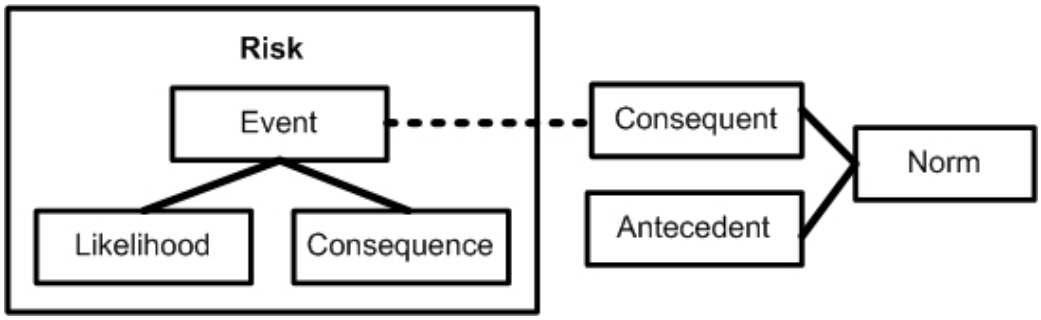

Figure 4. Normative risk events

Let us provide a simple example: In Norwegian law, the Data Inspectorate may impose a coercive fine according to the Data Protection Act Section 47 as a reaction to certain offences. As the example illustrates, the analysis of normative events is related to the question of compliance with existing legal rules. This is an obvious interface to the classical legal methods, and these may be used to assess whether the organisation or the system is compliant with the applicable provisions. However, while legal methods are valuable for assessing compliance, they give little guidance with respect to the proactive identification of facts than need to be assessed. Here the methods of risk analysis could be useful as complementary methods to support the identification of normative events.

Not all consequences that are prescribed by legal norms may be understood as "events" in the context of risk management. For instance, according to the Data Protection Act, Section 9, personal data can only be processed under certain conditions. If the conditions are not met, the processing is unlawful. The

31 For example, Keskitalo's approach to risk management does not concentrate on probabilities. Probability calculations are not necessarily irrelevant to lawyers, but it may be the case that lawyers to a certain extent are reluctant to use them. This may be illustrated by the Latin sentence *judex non calculat* ("the judge does not calculate"). However, note that there are examples of the importance of probabilities in a judicial context, *cf.* Finkelstein, Michael O., *Quantitative methods in law: studies in the application of mathematical probability and statistics to legal problems*, Free Press, New York, 1978; Eckhoff, Torstein, *Tvilsrisikoen (bevisbyrden)*, Tanum, Oslo 1943, Hov, Jo, *Rettergang III*, Papinian, Oslo 2000; for further examples see "www.worldhistory.com/wiki/P/Prosecutor's-fallacy.htm".

normative event to be considered in a risk analysis context is not included in this norm, but may follow from other norms.

Normative events may be distinguished from those that lack normative character, i.e. which are rather related to the empirically observable laws of nature or to economic processes. A normative event is the central element of a legal risk in the narrow sense. When drafting a contract we should however also take non-legal events into account. As an example, consider that a particular set of business data is communicated to a competitor, who could use the data for his or her own purposes. The consequent loss of the stakeholder's market share would in itself not be a consequence of a legal norm, but a fact related to economic mechanisms. Nevertheless, the probability of the occurrence of this event may be reduced by a confidentiality agreement, i.e. legal norms. Therefore, a methodology for legal risk analysis should specify the methods to identify those events that may be treated by legal remedies.

When drafting a contractual provision, risk management has to include both non-normative events (since these may justify certain contractual provisions) and normative events. Both can be identified at different levels.

- The *situation* to be governed by the contract may imply risks. The situation could involve normative events (e.g. the possibility for liability according to default rules) in addition to any type of factual non-normative event (e.g. the communication of confidential information leads to a loss).
- The contractual *provisions* themselves may cause risk events, e.g. to establish the possibility for contractual liability.
- The *application* of e.g. an unclear contract provision could cause additional unwanted events.

A methodology for legal risk management should facilitate a structured analysis at all of these levels for both normative and non-normative unwanted events. Since such events often will be a part of a chain of events, it is important to note which of the events has the most direct effect on the client's assets.

Moreover, the risk analysis comprises not only the identification of possible harmful events, but also an estimation of their likelihood and their consequences. In this respect, legal norms will again play a role: Laws may even reduce the consequences of an unwanted event, e.g. by offering the possibility to claim damages and to enforce a legally binding decision. Traditional legal methods will play an important role when estimating whether or not a claim for damages is likely to be successful and whether or not a decision will be enforceable.

6.3 Model-Based Legal Risk Analysis

Risk analysis is utilised – as mentioned above – in different disciplines, as enterprise management, engineering, computer science *etc*. Therefore, when the utility of new methods is to be considered for a proactive legal analysis, it is useful to concentrate on one specific domain, and to apply the methods that are developed in other disciplines when addressing this domain. For the purpose of

this paper, the emphasis will be on contractual rules focusing on the flow of information, e.g. confidentiality agreements.

It is submitted that a legal risk analysis in an ICT context would benefit from being carried out jointly by experts from different disciplines, including e.g. lawyers, economists and computer scientists. This is useful in order to jointly analyse legal risks in the narrow sense (i.e. normative events) and other risks that may occur within the same context. In some cases legal risks may be treated by non-legal treatments; in other cases it may be possible to reduce the likelihood of a normative event through non-legal remedies, e.g. an improved IT system.[32]

However, this cross-disciplinary complexity is challenging, partly due to the fact that different domains (IT and law) utilize their own vocabulary. One possible solution to this challenge lies in the use of graphical models in computer science. For example, the Unified Modelling Language (UML), the *de facto* standard modelling language for information systems, can be used for modelling hardware (engineering systems) and is commonly used for business process modelling, representing organisational structure, and systems engineering modelling.[33] In our context, particular attention should therefore be given to model-based methods. In risk analysis, these graphical models can be used both during risk identification and to document the output of a risk analysis.

An inspiration for legal risk management could be the CORAS methodology for security risk analysis, which utilises a graphical language to express notions like assets, threat, risk and treatment. The objective of introducing a graphical language is to facilitate the documentation of risks and to support communication among the participants with different backgrounds. The CORAS language is an extension of the Unified Modelling Language (UML version 2.0).[34]

The CORAS methodology and language is used to identify and treat risks for valuable assets with respect to information security in an information system. The objective is to achieve a better understanding of the risks to the assets, e.g. the probability of customer data being distributed to the public due to a computer virus infecting a server. This understanding can be utilised to reason about acceptable risks – where no action is required; and unacceptable risks – which should be treated e.g. by installing a virus scanner.

In the perspective of system theory, we can also understand a contract, a particular set of regulatory provisions or a business relationship as a system which can be analysed using the CORAS methodology. When analysing a

---

32 *As an example, see* Mahler, Tobias; Vraalsen, Fredrik, *Legal Risk Analysis with Respect to IPR in a Collaborative Engineering Virtual Organizatio*n, 6*th* IFPI Conference on Virtual Enterprises 2005, in Camarinha-Matos, Luis M. (ed.), Collaborative Networks and their Breeding Environments, New York 2005, p. 513-520, reprint in Krogh, Georg Philip and Bekken, Anne Gunn, *Yulex 2005*, Institutt for rettsinformatikk, Oslo 2005, forthcoming.

33 See for an introduction to the UML "en.wikipedia.org/wiki/Uml".

34 *Cf.* Lund, M.S., Hogganvik, I., Seehusen, F., Stølen, K.*: UML profile for security assessment.* Technical Report STF40 A03066, SINTEF Telecom and informatics 2003. The CORAS language is defined as an OMG standard, cf. OMG, *UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms*, OMG Adopted Specification, OMG Document: ptc/2005-05-02.

particular contract, we may be able to identify a number of risks, which could be treated by additional or amended contractual clauses. The use of UML in the CORAS methodology is advantageous for the primary area of this paper, i.e. risk management related to the flow of information, since graphical modelling is widely used in computer science, and facilitates a detailed analysis of information flows. However, in the context of legal risk management, the utilisation of UML also involves challenges, as lawyers are not used to graphical modelling, and are not generally experienced in the use of UML modelling tools. On the other hand, many of the graphical symbols of UML are understandable also for those not familiar with UML. Therefore, a limited use of some elements of UML may be helpful for legal risk management, particularly in the context of information law. Recent work has investigated how the CORAS methodology and language can be used to support legal risk analysis.[35] The latter research provides preliminary indications that the CORAS methodology and the graphical language indeed may be used to analyse and treat legal risks in the context of information flows. However, further research is needed to clarify to what degree and how the methodology and the language could be adapted to better address specific legal risks, and to identify where exactly the possibilities and limits for legal risk analysis lie.

7 Concluding Remarks

Methods from risk analysis and risk management can be used to enrich the legal methods in a proactive context. In a legal risk analysis, traditional legal methods will need to be employed both with respect to the risk identification and estimation and with regard to the treatment identification and analysis. However, more research is necessary in order to determine what kinds of risk analysis methods are useful for the specific needs of legal analysis.

There is a need for operative methodologies for legal risk analysis directed towards specific domains. Such methodologies should combine elements of contractual risk management based on existing legal theory with the methods for risk analysis used in other domains. For ICT-related contracts, these methods could be inspired by the CORAS methodology for security risk analysis and made operational in a similar way.

The use of methods for risk analysis in the legal domain may not only improve the ability of legal analysis to capture proactive elements, it may in addition contribute to the identification of interdisciplinary solutions to

35 Vraalsen, Fredrik, et al., Specifying *Legal Risk Scenarios Using the CORAS Threat Modelling Language – Experiences and the Way Forward*, in Hermann, Peter; Issarny, Valerie, Shiu, Simon (eds.), Trust Management, Third International Conference on Trust Management, iTrust 2005, Springer, Berlin Heidelberg 2005; Mahler, Tobias and Vraalsen, Fredrik *Legal Risk Analysis with Respect to IPR in a Collaborative Engineering Virtual Organization*, 6th *IFPI Conference on Virtual Enterprises 2005*, in Camarinha-Matos, Luis M. (ed.), Collaborative Networks and their Breeding Environments, Springer, New York 2005, p. 513-520, reprint in Krogh, Georg Philip and Bekken, Anne Gunn, *Yulex 2005*, Institutt for rettsinformatikk, Oslo 2005, forthcoming.

multidimensional problems. Hence, a legal risk management methodology that focuses on information flows needs to be directed towards the legal domain, but it should also support an interdisciplinary approach, which is necessary in the context of risk management and information law.

8 Acknowledgements

The research on which this paper reports has been supported by the IKT SOS project ENFORCE (164382/V30), funded by the Research Council of Norway.