Olav Torvund og Kirsti Pettersen(red.)

YULEX 2006

Senter for rettsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 82-7226-100-6
ISSN 0806-1912

Utgitt i samarbeid med Unipub
Denne boken går inn i universitets- og høyskolerådets skriftserie
Trykk: AIT e-dit AS
Omslagsdesign Kitty Ensby

CONTENTS

FORORD

Dette er sjette utgave av Yulex. Den gir nok en gang smakebiter på noe av det våre medarbeidere har arbeidet med i året som gikk.

2006 har vært et begivenhetsrikt år. Vi har gjennomgått organisatoriske endringer, og er nå Senter for rettsinformatikk innenfor rammen av Institutt for privatrett. Det er universitetspolitiske beslutninger som ligger bak dette. Man har ønsket å ha større grunnenheter. Instituttene har fått oppgaver som forutsetter en viss størrelse. Det som var Institutt for rettsinformatikk var for lite til å fylle en "instituttboks" i de nye organisasjonskartene.

Omorganiseringen gir nye muligheter. Vår tradisjon er å se etter muligheter, ikke etter eventuelle problemer. Vårt fagfelt har vokst kraftig siden starten i 1970, samtidig med at jurister med et mer tradisjonelt utgangspunkt ikke unngår å møte teknologiens utfordringer. Med den nye organiseringen vil det bli lettere å organisere samarbeid med miljøer som har større tyngde innen rettsområder som også vi kommer i berøring med. Vi tror at dette vil gi oss et godt og spennende nytt år.

God jul og fornøyelig lesing inn i det nye året!

Olav Torvund og Kirsti Pettersen

FOREWORD

This is the sixth issue of Yulex. It provides once again a sample of what our researchers have been working on during the past year.

2006 has been an eventful year. We have undergone organisational changes and are now a "centre" within the framework of the Department of Private Law. University political decisions lie behind this development. There has been a desire for larger organisational units. The various Departments have been given tasks that require a certain minimum size, and the NRCCL was

too small to fill the parameters of a "departmental box" in the new organisational scheme.

The organisational adjustments give new possibilities. Our tradition is to look for possibilities, not possible problems. Our field of research has grown tremendously since its beginnings in 1970 at the same time as those lawyers with more traditional points of departure are unable now to avoid meeting the challenges of technology. With the new organisational scheme, it will be easier to establish co-operation with research groups with a larger presence in legal fields with which we too come into contact. We believe that this will make the coming year both fruitful and exciting.

Merry Christmas and pleasant reading into the New Year!

Olav Torvund and Kirsti Pettersen

COMPUTERS AND LAW: SOME BEGINNINGS

Jon Bing

"Computers and Law"

The phrase "computers and law" has a comforting, old fashioned ring. It originated some time in the late 1960s, and was a rather imprecise indication of a group of issues related to "law" and "computers". Initially, there was no strong attempt to structure the field; it was a very pragmatic approach. This is demonstrated by what may be seen as the first specialised journal to emerge for the new field of research, *Law and Computer Technology,* which first issue was published in January 1968 by the World Peace Through Law Center, Washington DC, and which reported on the Third World Conference on World Peace Through Law in Geneva 1967, which featured an exhibition of computers and law, and a session on legal information retrieval.

"Computers and Law" has the advantage of embracing the two major branches within the field – first, computer technology used by lawyers for making their own work more efficient, like retrieval, decision support and in supporting the administration of justice; second, the substantive law applied to the trade and use of information technology and associated services. This dichotomy is basic to an understanding of the development of the field, and in the early days one would find the same persons and institutions working within both areas. Today, specialisation has separated them to a considerable degree.

The phrase "computers and law" may seem dated. There are versions of this phrase, as "Law and Information Technology" or "Law and Information Communication Technology", like in Centrum voor recht en informatica (ICRI) at University of Leuwen, Belgium or in the rather elegant High Tech Law Institute at Santa Clara University School of Law. The dichotomy survives also in French and related languages, like in the name of Centre de Recherches Informatique et Droit Facultés Universitaires Notre-Dame de la Paix, University of Namur, Belgium.

Many other claims have been made for naming this area of research. An early example is the German term "Rechtsinformatik", which is used to include both the main aspects. This is still used in the name of some institutions, like Institut für Rechstinformatik, Leibniz University of Hannover or University of Saarbrücken, or Instiutet för Rättsinformatik at Stockholm's University.

The Italian version is also in use, like in the L'Istituto di Teoria e Tecniche dell'Informazione Giuridica in Florence.

The English version of this term – "legal informatics" – never really caught on like its counterpart "medical informatics", but is used in the English versions of the names of institutions like Institute for Legal Informatics at the University of Zaragoza (which in Spanish is called Semniario de informática y Derecho). Reflecting technological developments, one of the new institutions at Lancashire Law School is using the phrase "law and convergent technologies", which not only includes information technology, but also nanotechnology and biotechnology.

One of the main contenders to a general term for the field is "information law", which perhaps emphasises the substantive law related to "information" – there are institutions using this in its title, for instance the Instituut voor Informatierecht, University of Amsterdam, Institut für Informationsrecht, University of Karlsruhe or Centro de Estudios en Derecho Informatico at University of Chile, Santiago.

There are also many different possibilities for variation. Harvard has its Berkeman Center for Internet and Society, which includes the Berkeman Cyberlaw Clinic, and New South Wales University has its prominent Baker & McKenzie Cyberspace Law and Policy Centre. An innovate version is the eLaw@Leiden, Centrum voor recht in de informatiemaatschappij at Leiden University.

The first book to present a course is Roy N Freed *Materials and Cases on Computers and Law,*[1] collected for a course 1968-69 at the Law School of Boston University. The material collected is diverse, from case reports through news items to academic papers. The large A4 volume has the texture of a literary collage, but firmed up through several editions. It did have the characteristic typical of the field; of bringing together issues which only glue was the computer technology. This is also the case of another early publication – Robert P Bigelow *Computers and the Law: An Introductory Handbook*. This is published by the Standing Committee on Law and Technology, established by the American Bar Association in 1968. These two books have come to indicate the "beginnings" of computers and law, but this is – of course – not the whole truth. As even this small paper will illustrate, there were many earlier attempts – and in Germany and Italy at approximately the same time, similar books were put together. However, the English language has secured these two early compilations a firm place not only in history, but also in the influence they have had for the developments in other countries.

1 Published by Freed, Boston.

They may themselves be seen as a contribution to the discussion of whether computers and law is "one" field, or one "discipline". This has been a vein running through the literature, perhaps best illustrated by Peter Seipel *Computing Law*[2] in which he with great persuasion argues that the technological part of the area – legal technology discussed in the first two sections below – are intimately fused to the issues of substantive law, and that this fusion is to be considered as one field where the parts are strongly interlinked, and that prying them apart will make it more difficult to analyse and understand. Perhaps a rather different, though related, view is that of Mads Bryde Andersen, who in his doctoral thesis on liability and computerised systems[3]qualifies what he calls "the problem of description": The systems examined for substantive law has to be analysed and understood in detail in order for the principles and terminology to be mapped onto the law. This is somewhat more than just "understanding the facts", as the systems are related to information science, and the terms used may deceive the lawyer to think they have a meaning identical to what they would have if encountered in everyday language or law. His insistence on lawyers understanding information technology sufficiently to have an independent insight for the application of law has a similar consequence.

The small survey above of some of the terms or phrases used to describe the field of "computers and law" shows diversity, and a tendency to tune the terminology to what is the current vogue in technological slang. The diversity may be an indication for this not being "one field" or "one discipline", and I will not myself venture to make any definitions. Rather, the survey will be taken for a sufficient indication of what it "all is about".

Anyway, an attempt to write a brief history of the development of this field is bound to fail. But it is nevertheless tempting. I have therefore decided to be extremely pragmatic and be guided by my own experiences, having been part of the development since entering the field as a young research assistant in 1970. I know this brief sketch will be marred by my own perspective, my own research interests, and from being located in Norway. The reader should bear this in mind to compensate for the idiosyncratic view offered.

I have decided to unravel the history by catching hold of some threads in this rich fabric, and sketch some initial developments.

2 Liber, Stockholm 1977.

3 *EDB og ansvar,* Jursit- og Økonomforbundet, Copenhagen 1988.

Let there be LITE

A retarded child and its impact[4]

In the late 1950s, a bill was passed in the legislature of Pennsylvania. Part of the bill was to change a term in the health law legislation – the phrase "retarded child" should be replaced by the more neutral phrase "exceptional child". This may seem as an example of legislative window-dressing, but obviously the amendment also indicated a new political attitude to this group of persons, and its importance should not be underestimated. There are in any jurisdiction examples of such amendments in the legislation which heralds changes in the policies within a certain area.

Pennsylvania adhered to the principle of regulatory management called "textual replacement". It dictates that any amending regulation must exactly identify which sections and sentences in the existing body of regulations should be amended. One may picture this of the amending regulation containing explicit wording which could be cut out and pasted into the specified parts of the identified existing regulations, giving as a result the new text of each amended regulation. An alternative to this principle is the "omnibus principle", where it is seen as sufficient that an amending regulation contain a section which dictate that all former regulations containing the phrase – wherever they may occur – are to be deemed amended, without specifying the relevant locations.

However, having the principle of textual replacement, the legislators of Pennsylvania had to identify where the phrase "retarded child" – or a variation of this phrase – actually occurred. This represented a tedious task, and the legislators turned towards the Graduate School of Public Health at the University of Pennsylvania for a solution. Here Professor John F Horty had been working on a manual of hospital law, and had developed indexes to support his work at the Health Law Center. Accepting the contract, Professor Horty set out to solve the problem in the time-tested way of professors: He hired a group of students to read through the legislation and indicate all passages containing the relevant phrase. The result likewise was conventional: The professor found the quality of the work wanting. He hired a new group with an equally depressing result.

It was at this stage he turned towards the Data Processing and Computer Center, which had been established in 1955, and gained co-operation for a

4 The historical background is set out in Jon Bing *et al Handbook of Legal Information Retrieval*, North-Holland, Amsterdam 1984, also available at http://www.lovdata.no/litt/index.html.

more radical approach: Solving the problem using text retrieval. To appreciate the boldness of this approach, one should consider the level of computer technology at this time. For the project, there were available an IBM 650, which was based on vacuum tubes and a drum storage of 2,000 words, and an IBM 7070, which was a transistorised version of the IBM 650, having a magnetic core storage containing 9990 numbers of ten digits each. One may compare the capacity to current examples of information technology, like a digital watch or a pocket calculator. Random access memory units like magnetic disks were not available; data not placed into the central storage units mentioned above, had to be stored on sequential tapes.

In principle, the system Professor Horty developed processed an input text to create two files. One was a "text file", containing the original text with an additional index, which gave an internal address for each element of the text – like "section 2, paragraph 3 starts at location *n* on the magnetic tape". The other was a "search file",[5] where all the different words occurring in the text were sorted in alphabetical order, giving for each occurrence the internal address of the word.

The search file could be used as a very extensive index to the text itself: Looking up any term in the search file, the internal address was specified, and the computer system could use this in accessing the index of the text file, and retrieve the word in context from the text file. The user had the impression of searching the "full text"; specifying a word like "child", the system would return with the information that this occurred, for instance, in two sections of the statutory text in the data base. And if the user asked to have these displayed (or rather, printed out), they would be retrieved, using the internal addresses as the key linking the search and text files.

Sorting the words of a text in alphabetic order could be compared, perhaps, to ordering books by authors' names in a book case. Anyone who has ventured to do this will know that new books frequently have authors with last names starting with a letter early in the alphabet, requiring you to move the last books, working yourself back towards the place where a space for the new book is needed. This metaphor may give some indication of the practical problems facing the early developers. And, of course, they did not have online systems, but had to deal with batch processing, using punched cards for input and printouts for output.

The system developed by Horty did make it rather facile to identify in which provisions of the Pennsylvania Health Law Code the word "child" and "retarded" (or grammatical variations of these) co-occurred, and the original contract

5 Also known as "inverted file" or "concordance".

could be successfully concluded. But it was rather obvious that *any* words in the stored provisions likewise and as easily could be retrieved. It is therefore justified to see this as the first successful text retrieval system, and as such it was demonstrated for an American Bar Association conference 1960. In 1963, the technology was used to build the first computerised legal information service, the LITE[6] system of the Air Force Staff Judge Advocate in Denver, Colorado. The technology also provided the basis for Aspen Systems Corporation, established 1968, which served a large number of states in maintaining their compilations of regulations in force during the early 1970s.

There are many roads to follow from Horty's initiative. In practice, it started the development of computerised legal information services, which today are provided in any jurisdiction, and with major international examples as Reid-Elisevier's NESXIS-LEXIS service, or the Westlaw and other services of the Thompson Group. But impact on research was also major, and the two major examples are European.

But before leaving the beginning, one may indicate that though lawyers are not know for being technological *avant gardists*, text retrieval was actually developed by lawyers and for lawyers, due to the need to consult the authentic text for legal interpretation. The search engines of Internet today ripe the harvest sown by the early efforts of the legal community.

European influence

Bryan Niblett was a nuclear research physicist with the UK Atomic Energy Authority.[7] He spent the 1966-67 on sabbatical in California, primarily to learn about computer programming. But as he had been called to the English Bar,[8] he also spent time digging into US research in computers and law. He came across the work of Horty, and started plans for doing something similar in the UK. On his return, he has already worked out the acronym STATUS (for STATUTe Search), and determined to develop a machine independent program, which for that reason was written in a subset of FORTRAN. Having produced the first version of the program, he run into trouble – the Lord Chancellor advised the UKAEA that for them to put all the statutes into the

6 LITE is an acronym for "Legal Information Thru Electronics", and it was launched 13 November 1963 under the inventible slogan *Let there be LITE!* The service in 1975 renamed FLITE – "F" for "Federal".

7 The paragraph is based on private communication from Bryan Niblett to the author.

8 Bryan Niblett therefore combines the two aspects of computers and law – later he became Reader of Law at the University of Kent at Canterbury, going from there to the chair of Professor in Computer Science at Swansea.

system would be an *ultra vires* act, protecting the monopoly of Her Majesty's Stationary Office (HMSO) under Crown Copyright. Therefore, the system was limited to the atomic energy regulations

The importance was not the legal service provided, but the machine independent program, which could be compiled for different computers. It provided initiatives in other institutions, and a better understanding of retrieval strategies and limitations. On this basis, activities were started in Australia, Holland and Norway. His collaborator, the former submarine officer, Norman Nunn-Price also becomes influential in the development of European legal information services, especially for the European Union.

The other major European example is Colin Tapper.[9] When working at London School of Economics 1961-65, he also became aware of the research by John Horty, and initiated studies that have become known as "The Oxford Experiments",[10] as the bulk of the work was conducted after he joined Magdalene College, Oxford (retiring as a professor). The value of Tapper's work is not only the very interesting results he provided on the design and performance of legal information services, but also the academic attitude he brought to the filed. His major objective was not to get a system up and running, but to understand how text retrieval worked, and how it best could be utilised to access the source material which mainly suffered from the shortcomings of paper-based solutions: Case law. Also, he pioneered the work on using case citations for improving performance.

The legal information crisis

Above the development of legal information retrieval has been followed from the Pittsburgh imitative, which mainly is driven by an interest in the possibilities inherent in the new computer technology. In Europe, however, another aspect was rather prominent.[11]

---

9 For a review of his work, see Jon Bing "The policies of legal information services: a perspective of three decades"; Peter Mirfield and Roger Smith (eds) *Essays for Colin Tapper,* LexisNexis UK, London 2003:147-158.

10 Cf Colin Tapper "Legal Information and Computers: Great Britain", *Law and Computer Technology* January 1968:18-19. Here is mentioned the "Office for Scientific and Technical Information" at Oxford, which was the name of the framework within Tapper continued his work from LSE. Colin Tapper is well known for his reluctance to have his photograph taken, it therefore with malicious pleasure noted that his portrait appears with the article.

11 This is argued in more detail in Jon Bing "Legal information services: some trends and characteristics", Colin Campbell (ed) *Data Proecessing and the Law,* Sweet & Maxwell, London 1984:29-45.

In 1970, Professor Spiros Simits published the book *Informationskrise des Rechts und Datenverarbeitung* (Karlsruhe). The main argument in this book is based on the growth of the European welfare states. Turning away from a legal policy where social benefits were awarded based on an assessment of need, the welfare states asserted rights for social security. This implied that a decision became legal in nature, and that an applicant could appeal. The appeal had to be processed according to the legal ideals found in how courts addressed such matters. There was a growth in specialised appeal agencies, like administrative tribunals. Also, in jurisdictions where there was a system of administrative courts, their case load increased. The appeals should be tried on the basis of the relevant legal sources. Few such sources applied to these cases apart from the prior decisions of the decision-making institution itself. Such sources were not typically included in the traditional legal publications, but were only available thorough the files of the institution. These were cumbersome to search, and consequently the time to process appeals increased.

Admittedly, this is a very crude rendering of the arguments of Simitis, but the point should be clear: There was an acute need to improve the performance of legal research in order to meet the requirements of the modern welfare state. And the solution was available in the form of legal information systems. This was strongly advocated by academic lawyers like Spiros Simitis and Herbert Fiedler;[12] and the 48th Deutschen Juristentag in 1970 recommended:

> *"Die ständige Deputation halt as für dringend geboten, über das Stadium der theoretischen Vorüberlegungen eines Einsatzes datenverarbeitender Maschinen auch für die Rechtspraxis hinaus sic nunmehr am de praktische Verwirklichung, mindestens durch de Schaffung von Datenbanken, zu bemühen, wie dies in Ausland schon weithin geschieht."*

Already in 1967, the Bundesministerium der Justiz had started planning of such a system. It is an amazing example of planning living up to the best ideals of German praxis, where the administration was supported by professors like Fiedler, Simitis and Klug, ending up in a major report of 1972 – *Das Juristische Informationssystem – Analysis, Planung, Verschläge*. On this basis, the JURIS[13] system was implemented, a system still very much alive today. The first services of this system addressed social law (the decisions of Bundessozialgericht)

12 Professor Herbert Fiedler has been very influential, and he also has a very sound basis for his work, having both a doctorate in mathematics and in law.

13 Some confusion may arise from the use of the acronym JURIS also for the US Justice Retrieval and Inquiry System, but the Bundesministerium der Justiz consulted with their American counterpart, which agreed to the German use. The US service is now discontinued.

and tax law (the decisions of Bundesfinazhof), illustrating the point of the need to address the problems of the welfare state.

We will not dwell on the development of this service, but note that it was followed by a remarkable academic activity. In the 1970s, Germany by far was the most active country within the area of computers and law. Professor Fiedler headed both Institut für Datenverarbeitung im Rechtswesen at the Gesellschaft für Mathematik und Datenverarbeitung, and Institut für Juristische Informatik at the University of Bonn. At Regensburg, Professor Willehem Steinmüller developed his basis for a general theory of computers and law, Professor Fridtjof Haft was active at the University of Tübingen, Professor Wolfgang Kilian established his Institut für Rechtsinformatik in Hannover *etc*. There are several more names that could be added to this impressive catalogue of lawyers taking an active interest in computers and law, developing its many aspects, and contributing to a rich literature.

The German example could be used as an index to what happened in many European countries. One is acutely aware of not being able in this context to even very summarily indicate these developments, but perhaps two more examples may be given.

In Italy, a similar pressure towards decisions taken by the administrative courts was felt. Here, the lead was taken by the Corte di Cassazione. Renato Borruso, one of the judges at the court, suggested a system in 1968 based on the traditional *massime* or abstracts of the decisions of the court, and the use of a thesaurus. The design of the system pursued the solutions in more traditional library-type systems, which also made it possible to realise the solution without the massive computer facilities required by the US services. The ITALGIURE-FIND system of the Centro Elettronico di documentazione of the court grew to become more than an impressive and extensive system under the inspired directorship of Vittorio Novelli, it became a driving force in Italy.

And there was a broad interest. Vittorio Frosini at the La Sapienza University in Rome had published his *Cibernetica diritto e società*[14] in 1967, in which he emphasised administrative law much stronger than in the Anglo-American literature. In 1969, Mario Losano at the University of Milan[15] coined the term *Iuscibernetica* for the field of *Macchine e modelli cibernetici nel diritto*.[16] The National Research Council established the Istituto per la Documentazione Giuridica[17] in Florence, which engaged in an active strategy of publications

14 Edizioni di Comunità, Milan 1967.
15 He is currently at the University of Piemonte Orientale.
16 Einaudi, Turin 1969.
17 Today this institution is known as L'Istituto di Teoria e Tecniche dell'Informazione Giuridica.

and conferences. The Corte di Cassazione started in 1976 a tradition, which was upheld for twenty years, of huge, international conferences spanning the whole width of the expanding area of computers and Law, the proceedings published in several volumes.

In France, Professor Pierre Catala at the University of Montpellier in 1965 organised a working group with the objective of developing a legal information service, which in 1967 was formalised as Centre d'études pour le traitement de l'information juridique (IRETIJ). This is – as far as I know – the oldest academic institution within the area of computers and law. It was associated with the problem of accessing the decisions of the appeal courts, which were not subject to systematic publishing. IRETIJ developed a system called JURIDOC, and started documenting appeal court decisions. The system was inspired by the work of Michel Bibent, whose doctoral thesis also probably is the first within the field.[18] It may be fair to say that the efforts, especially after Professor Catala left for Paris, was somewhat drained by the needs of an operational system to the disadvantage of academic research.[19] And in Paris, there was another working party established in 1967 on the imitative of Lucien Mehl, a conseilleur d'Etat and the grand old man of computers and Law in Europe (see below). The Conseil d'Etat also has some functions as an administrative court, and the imitative lead to the establishment of an information service which from 1970 became an independent organisation, Centre de recherches et développement en informatique juridique (CENIJ), which through a series of changing names and mergers with other services has become the current French information service, Legifrance. Though it is somewhat fuzzy, France again offers an example of the needs of the administrative law being a driving force behind the developments rather than the business opportunities which in the United States motivated ventures.

This aspect of computers and law will be left at this point. It is unfair to the developments that were to follow from this beginning – for instance the Swedish Law and Informatics Research Institute, which directed by Professor Peter Seipel became so very influential in the Nordic countries, or to the innovative Vienna system and the work by Robert Svoboda and others in Austria. It is also unfair to those institutions most active within this area today, for instance Professors Jos Dumortier and Marie-Francine Moens at ICRI, Leuwen or the Norma project at the University of Bologna. And it is even more unfair

18 *L'informatique applique a la jurisprudence,* Montpellier 1972.

19 Though Professor Michel Vivant, whose work in substantive information law is prominent, is also from Montpellier, but not working within the sector discussed here.

to those whose efforts even have not been mentioned. But there will be other possibilities more fully discuss these aspects.

The Council of Europe

In Europe, the Council of Europe played an essential role in the early developments. On the initiative of the Committee of Experts on the Publication of state practices in the field of public international law, a Committee of experts on the harmonisation of the means of programming legal data into computers started its work in 1969. The longish name of the committee – and I believe no one will be offended by this – rather clearly reveals that the committee was formed without a clear understanding of its objective or the means to achieve such an objective. And the committee changed its name to the more acceptable Committee on Legal Data Processing in 1974.[20] For the rest of the century, this Committee was a central forum for an exchange of ideas and experiences with respect to computers and law. The substantive law was not part of the area for this committee – but it explored legal information services and justice administrative systems as well as teaching in the area of computers and law. Often the success of international committees is measured in the number of legal instruments adopted – the Committee certainly adopted such instruments,[21] but its main achievement was the communication it facilitated between European institutions, not only at the meetings of the committee itself, but at the annual international events, which was organised in different countries. Around the committee grew a loose-knit community of experts within public administration and universities with a strong, though informal, communication.

It is not possible to understand the co-ordinated development of legal information services in the different European jurisdictions without awareness of the exchanges taking place through the network built by this committee. The committee also strongly supported academic activity, not least through the adoption of recommendations of making introduction to computerised systems a compulsory part of legal education, and suggesting a curriculum in the teaching of computers and law.

Artificial Intelligence in Law

The first paper in Europe to discuss computers and law was offered to a conference at the Institut techniques des administration publique 21 May 1957

20 Formally, this was a new committee succeeding the former.

21 An example is R(83)3 on the "protection o fusers" of legal information services.

by Lucien Mehl, the title being "La Cybernétique et l'administration". In this, Mehl discusses the problems associated with fully automated legal decisions. It may today seem somewhat premature to consider the computer as a judge at this early stage of development – but the "ghost in the machine"[22] was rather evident, one of the early contributions to the *Law and Information Technologies* raised the question "When does the computer engage in unauthorised practice?"[23]

Computers offer possibilities to explore legal reasoning by new methods. Traditionally one mentions Lee Loevinger's paper "Jurimetrics – The Next Step Forward"[24] as the start of an approach encouraging "the scientific investigation of legal problems", but he was mainly oriented towards empirical and quantitative methods related to what often is called "the sociology of law". But there was a side-track of those interested in the use of formal logic in law. This side-track actually starts some time back. George Boole, when introducing his logic basic to all computerised systems (*An Investigation Into the Laws of Thought,* 1854) chooses the following rule as an example:[25]

"Clean beasts are those which both divide the hoof and chew the cud."

which he then goes on to render as a Boolean statement, and process according to the rules of his logic. A pioneer in analysing law by logic was Layman E Allen, commencing with his paper "Symbolic logic: a razor-edged tool for drafting and interpreting legal documents".[26] In 1959, he started the journal called *Modern Uses of Logic in Law* (MULL),[27] which later was re-named *Jurimetrics Journal.*

Formal logic can be viewed as formalism similar to a high level programming language, the major difference is that a statement in formal logic cannot directly be implemented and executed by a computer. The possibility of representation of legal knowledge directly in computerised form, was in the 1970s called "radical computer use in law".[28] It was really a plea for the use of more advanced or novel methods to improve the performance of text retrieval, and

22 Arthur Koestler *Das Gespenst in der Maschine,* Fritz Molden, Wien 1968.
23 George G Lorinczi, July 1968:10-12.
24 Reprinted in *Jurimetrics Journal* 1971:3-41.
25 George Boole *An Investigation Into the Laws of Thought,* 1854, Chapter VI Section 6.
26 *Yale Law Journal* 1957.
27 The journal was published by the Electronic Data Retrieval Committee, established by the American Bar Association the same year.
28 lCf Philip Slayton "Radical Computer Use in Law", 1974, Ottawa.

the first real attempt to do this was made by Carole Hafner in 1978.[29] This was to become an area of research when artificial intelligence and law later was established, but such methods still wait to be widely deployed.[30] The papers which made a major impact internationally were based on L Thorne McCarty's TAXMAN projects, which in broad terms may be described as experiments in artificial intelligence and legal reasoning. In these projects, the objective was by modelling a set of legal norms constituting a relatively self-contained body of law insights about patterns of legal reasoning and argumentations could be achieved.

Artificial intelligence was buoyed by high expectations at the end of the 1970s. The establishment of the dispersed attempts and some major projects as the area of research called "artificial intelligence and law" can be located in time to September 1979. Bryan Niblett organised an eight day workshop at Clyne Castle, Swansea,[31] in which all those active within the area participated – the objective was "to go beyond document retrieval and explore the more ambitious task of retrieving and interpreting the law itself".[32] Here the major projects like McCarty's TAXMAN and Ronald Stamper's LEGOL were presented alongside the tradition of logic in law by Layman Allen, the empirical modelling of decisions by Reed Lawlor, and the analysis of computer programs directly representing legal rules in their code, which grew out of the German interest in "Automationsgeeignete Gesetzgebung", how to draft legislation for efficient computerisation.

The categories emerging from the Swansea conference were adopted and continued when the field was organised around the International Conference on Artificial Intelligence in Law (ICAIL). The first such conference was convened in 1987 at Northeastern University, Boston on the initiative of Carole Hafner, and is still continuing as a bi-annual event, buffered by the *Artificial Intelligence and Law* published by Springer Verlag.

29 The work was done in 1978, documented in Carole Hafner *An information retrieval system based on a computer model of legal knowledge,* UMI Research Press, Ann Arbor 1981.

30 A review of the field at the end of the 1980s is found in Jon Bing *Conceptual Text Retrieval,* CompLex 9/88, TANO, Oslo 1988.

31 This is a unique conference in the memory of the author. The participants was socially brought close together, and found ways to entertain each other in the evening. One will not forget the Schubert romances performed by Stamper, the solo violin of Costantino Ciampi, director of the Istituto per la documentazione giudica, Florence.

32 Bryan Niblett "The Structure of the Course", in Bryan Niblett (ed) *Computer Science and Law: An advanced course,* Cambridge University Press, Cambridge 1980:3.

The area has changed many times,[33] in the early 1980s, attention shifted towards expert systems influenced by Richard Susskind *Expert Sysyems in Law.*[34] A distinct area is the analysis of operational systems for legal decision support, which typically is found in public administration, and which opens the analysis and discussion of the interrelationship between the legal norms presented in conventional sources and as represented in the programs.[35] Computer-assisted methods for drafting legislation, assuring for instance consistency, constitute another branch. Lately, it may seem that the interest in electronic agents somewhat has re-vitalised the field.

Data protection

In 1967, Alan F Westin published his book *Privacy and Freedom.*[36] It is a remarkable book in many respects; the first section of the first chapter is titled "Privacy in the Animal World", and is followed by a section on privacy in the primitive societies, drawing on anthropological studies. It is, therefore, a book in which the discussion ranges broadly, addressing a number of rather different issues. But important is the "pressures on privacy created by the information processing revolution"[37] which are summarised in six points:

- The general expansion of information-gathering and record-keeping
- The development of personal dossiers by credit companies, the security files of the Department of Defense, FBI, Federal Housing Administration, *etc*.
- The acceleration of information gathering by computers
- New public programs requiring more personal data
- Computer technology facilitating the sharing of data
- The replacement of cash transactions by automatic data processing

This small summary is offered for the reader to compare to the issues current. One will find that the concerns are rather similar to those that still are with us.

---

33 A review is given by Marek Sergot *The representation of law in computer program : a survey and comparison*, CompLex 1/91, TANO, Oslo 1991.

34 Oxford University Press, Oxford 1987.

35 The pioneers here are Cecilia Magnusson Sjöberg *Rättsautomation: Särskilt om statsförvaltningens datorisering,* Nordstedts juridik, Stockholm 1992 and Dag Wiese Schartum *Rettssikkerhet og systemutvikling i offentlig forvaltning,* Scandinavian University Press, Oslo 1993.

36 Atheneum, New York.

37 Alan F Westin *Privacy and Freedom,* Atheneum, New York 1967:158.

Westin's book appeared at a time when policies were formed by the possibilities of the new mainframe computers. Terminals made it possible to access computers at a distance, there were visions of data only being recorded once, and shared among federal agencies when collected, realising savings for the taxpayer. The idea of a national information system was invoked. But rather than being greeted by enthusiasm for a more efficient federal administration, the public protested. The concern ignited by Westin's powerful prose was taken further by others; another important title was Arthur Miller *The Assault on Privacy: Computers, Data Banks and Dossiers*.[38]

One should consider that this was a time of deep political frustrations in the United States – the Vietnam War had divided the country, and the Watergate scandal in 1972 was by many seen as a political deceit. This was the age of the mainframes, the IBM/360 and 370 generation, displayed behind plate glass on the ground floors of industrial complexes and skyscrapers – still the first brick had to be lobbed through a window destroying the controlled atmosphere in the rooms where the computers were nursed by technicians in white coats. Privacy became a severe political concern; the plans for the national information system were shelved.

I have notes from a seminar in Paris, probably 1972, where Westin analyses the situation, finding that the cause is a reaction to power, and directed at computers as symbols of power. He summed it up in something like an aphorism: "You do not find computers in street corners or in free nature; you find them in big, powerful organisations."

This can be re-considered today, where the game arcade on the street corner displays pyrotechnical three dimensional computer graphics, or where you may come across a person on a footpath through the forest tapping away on the keyboard of his or her laptop. The technological infrastructure has changed in a dramatic way from Westin's initial analysis of the causes, but – as indicated above – his concerns as listed in his 1967 book, are still with us.

One of the important channels communicating this concern to Europe was the OECD.[39] This organisation, often referred to as the club of the rich countries, was established in the aftermath of the economic assistance to Europe after the Second World War, and is mainly concerned with trade issues. But as early as 1969, OECD established a "Data Bank Panel", which later was converted to the Information, Computers and Communication Policy Committee (ICCP). It is my belief that Hans Peter Gassmann, the secretary to the panel and later to the ICCP, was very influential in bringing this about. It was by no

38 University of Michigan Press, 1971

39 Organisation for Economic Co-operation and Development.

means obvious that OECD, an organisation traditionally concerned with the issues of free trade, should get involved in privacy, which many would view as a policy interest of a different nature. But national regulation protecting personal data could become an "invisible barrier to trade", as any trade implies an exchange of personal data. And with his team,[40] Gassmann brought data protection into focus. It may be argued that the international instruments that followed, which all include the consideration of free trade in goods and services, is indebted to the OECD heritage and the perspective of trade policies.

In 1970, the US adopted the Fair Credit Reporting Act, and the German state of Hesse adopted its Datenschutzgesetz, which also brought the term "data protection" into the English language. Professor Spiros Simits had assisted in drafting this legislation, and he also became a major influence in the law and policies of data protection, taking the office as commissioner in Hesse.

Such development helped bringing the policies of data protection into focus, and there were strong national activity. Sweden was the first nation to adopt a national legislation. This was by no means by chance – Sweden has the most brutal freedom of information act in existence, and there was perceived a need to harness the processing of personal data and their use.

> *A small anecdote may illustrate the point. The Greek military junta made a request to the national personal register to have access to the names of Greek nationals living in Sweden. As these generally would be political opponents, one was reluctant to make this list available, and an excused based on technical difficulties was made. A few months later, it was found that a firm importing tinned foods had made the same request. The firm planned a line of imported Greek products, and wanted the list for direct mail marketing. A routine response had been given to this request, providing the list. This is, it should be emphasised not confirmed by any source, but perhaps the point is made.*

The Swedish legislation was drafted by Jan Freese, who was to become an important figure on the international scene. With Gassmann, Freese coined the phrase "transborder data flows" in the middle of the 1970s. This became an important issue, as it focused on data protection as an "invisible barrier to trade". The ICCP started to consider an international instrument to address this issue. More or less at the same time, the Council of Europe, based on its

40 Which included Klaus Lenk, now professor emeritus at Carl von Ossietzky University of Oldenburg, and G Russell Pipe, who went on to publish the influential Transnational Data and Communications Report (TDR) 1978-1994.

tradition of human rights treaties, launched its own project. There became something of a race between the two organisations for being the first to adopt an international instrument – many of the same delegates would oscillate between the work parties in Paris and Strasbourg. The OECD effort was headed by the Australian Justice Kirby,[41] who was a stern worker – he might keep the working party till after the interpreters had left, and show up the next morning with the comments of last night typed up.[42] He was helped by Professor Peter Seipel (Sweden), and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted 23 September 1980. In Strasbourg, Frits Hondius was heading the secretariat, a kind and learned person guiding the project to its success by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted 28 January 1981.

At this time, most – but not all – European jurisdictions had national legislation. Those which sanctioned the Council of Europe treaty, also agreed not to use data protection as an argument for regulating trade between them. But if a member country itself exported personal data into a third country not bound by the treaty, other members could argue that this would put the protection of personal data at risk, and then regulate the export. During the 1980s, the European Union strongly promoted the internal market, and urged member countries to sanction the Convention to remove data protection as a potential trade barrier within this market. Member countries, however, hesitated, and the Commission decided to adopt a Directive, which would put the matter at rest – if member countries did not adopt the directive, it would eventually be directly enforced according to EU law.

The negotiations for the data protection directive started in 1990, approximately ten years after the adoption of the first international instruments. It turned out to be a drawn out struggle for the directive to find its final form, and it was only adopted in 1995,[43] indicating in its title that one of the objectives was the "free movement" of personal data.

One will easily appreciate that the years from 1990 to 1995 was critical in the development of the infrastructure of information technology. In 1990, Tim Bernes Lee was permitted by CERN to start programming the new version of his 1980 program Enquire Within Upon Everything, the project being given

41 Later to become president of the Australian Supreme Court.

42 The author draws on his personal notes, being a Norwegian delegate to the OECD working party.

43 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.

the name World Wide Web. In 1993, Marc Andreessen released the first version of his web browser, Mosaic, which made the web more easily accessible, and the web pages rich in graphics. In 1995, Digital Equipment Corporation launched Alta Vista, the first search engine based on text retrieval principles. In the five years the EU was negotiating over the directive, the world in which the data protection principles should be implemented changed in a dramatic way – one may dare to talk about a new paradigm.

Therefore, we still have a situation in which there are numerous research issues and practical challenges to data protection – ensuring that this continues to be a rather lively field.

Copyright and information technology

One of the more curios early copyright cases is White-Smith Music Publishing Company *v* Apollo Company.[44] The case concerned the copyright to two "plantation lullabies" to which White Smith had the copyright. Apollo was a company manufacturing pianolas, mechanical devices which would play the piano from "musical rolls … of perforated sheets, which are passed over ducts connected with the operating parts of the mechanism in such manner that the same are kept sealed until, by means of perforations in the rolls, air pressure is admitted to the ducts which operate the pneumatic devices to sound the notes". The issue was whether these rolls were a "copy" of the musical work in the meaning of the US (1907). The court held that it was not: "These musical tones are not a copy which appeals to the eye."[45] This case was subsequently eclipsed by Congress's intervention in the form of an amendment to the Copyright Act of 1909, introducing a compulsory license for the manufacture and distribution of such "mechanical" embodiments of musical works. This was not a solution of what Michael S Keplinger referred to as "The Case of the invisible copies".[46] It is rather trivial to observe that if a sheet of perforated piano rolls were not "pleasing to the eye", the same would hold for punched cards or tape, not to mention the magnetic storage media which were introduced.[47] And the

44 109 US 1(1907).

45 Justice Holmes remarks, "On principle anything that mechanically reproduces that collocation of sounds ought to be held a copy, or if the statute is too narrow ought to be made so by a further act, except so far as some extraneous consideration of policy may oppose." However, he did not formulate a dissident opinion, and his implied advice was followed only 70 years late.

46 *Revue International de Droit d'Auteur*, October 1970.

47 Probably first used by Mauchly and Eckert 1946 in their first attempt to produce a computer, which eventually was named UNIVAC.

basic problem in the US copyright law had still not been solved – though it represented no problem within many other jurisdictions.

> *When jointly revising the copyright acts of the Nordic countries in the late 1950s, the definition of a copy was extended to include "any device on which the work is stored". Originally this was to include sound recordings on magnetic string, but computerised devices were easily absorbed.*

In the 1960s, computer programs were considered as accessories to the very expensive computers. There were several reasons for this, one that programs simply could not be run on any other computer than for which it was written, high-level languages were still in the making[48] and compatibility was low. But IBM had considerable success with its 360-series, and decided in 1969 – perhaps somewhat stimulated by the anti-trust suit to which it was party – to unbundle hard- and software. As computer programs were separately priced, it became possible for third parties to offer competing programs. And in such a market arose the obvious issue of the protection of computer programs.

At this time, it was still unclear to what extent the US Copyright law applied to computer programs. There were several court decisions, the copyright and patent systems competing for becoming the legal framework for the intellectual property protection of computer programs. There were also strong advocates for a third possibility, a *sui generis* regime for computer programs, as it was pointed out that neither copyright nor patent was designed to accommodate the special features for protecting computer programs.

> *The author will be permitted an anecdote by the way of illustration. At one of the meetings of experts[49] to the WIPO in Geneva,[50] there had been an unusually heavy snowfall during the night. Struggling uphill to the WIPO building, one could see improvised tools being used to remove the snow in order for cars to escape from their parking lots. In the meeting, the head of the delegation of Soviet Union[51] made this into a metaphor pleading for a sui generis solution, "In Geneva, where the snow rarely falls, one may allow oneself to adapt the tools at hand for the removal of snow. If you live in Moscow, you will expect the snow to fall heavily every winter, and you will have efficient and specialised tools. And I ask*

48 The first version of COBOL was adopted 1968 by American National Standards Institute.
49 Advisory Group of Governmental Experts on the Protection of Computer Programs.
50 February 25 – March 1, 1985.
51 Vitaly Troussov, Deputy Director of the Patent Examination Department, USSR State Committee for Inventions and Discoveries

you, ladies and gentlemen, do you think computers are like the snow in Moscow or in Geneva?"[52]

WIPO actually developed 1971-77 "Model provisions on the protection of computer software" with the assistance of Professor Peter Seipel (Sweden), but these were not adopted as national legislation in any country. The model provisions were inspired by copyright, but had some elements akin to patent protection of the content of programs. In practice the discussion of alternatives came to a halt when the US adopted the 1980 amendments to the 1976 Copyright Act, extending copyright protection to computer programs. A country was free under the conventions of qualifying programs as literary works, and this made it possible nearly overnight to establish an international scheme of protection, based on the Berne and Universal Copyright Convention.

The interest in copyright was nearly exclusively limited to computer programs. For these there was a market, and there were strong commercial interests in protecting programs. This interest also found different strategies for protection; one was to introduce various devices which had to be present for the program to be executed, like an extra element for the serial plug to the printer which then was called by the program, which failed to initiate printing if the element was not found. This was the beginning of technical protection measures, the discussion of which later has escalated. Another obvious measure was only to make the program available in object form, which in turn gave rise to the doctrine of and provisions on reverse engineering in order to make it possible to develop programs functionally interacting with another program. A characteristic of copyright is that the protection allows anyone to access the information in the protected work, and use this information in the creation of new and independent works. The practice of making programs available in object form only, barred the access to the information, and reverse engineering may be seen as a reaction to this for copyright somewhat alien aspect.

There was some interest in other aspects. A joint WIPO and UNESCO[53] of 1982 concerned the "problems arising from the use of computer systems for access to or creation of works". In the recommendation it is stated that for instance uploading of a protected work to a computerised systems represents a reproduction in the terms of the conventions. The use of computers to create work attracted some attention, at this time composers would use computer

52 One will find a reference to this intervention, though stripped of the images, in the report of the meeting paragraph 22, UNESCO/WIPO/GE/CSS/3 8 March 1985:4.

53 UNESCO is the depositary to the Universal Copyright Convention.

programs as tools, and the recommendation[54] also states that this is the perspective in which to consider such use.

However, there were considerable limitations in computerised systems at this time (1982) for a real concern about the use of literary, musical or audiovisual works to be considered for computerised systems. The IBM PC had been brought out the year before, the first model did not have a hard disk, but only 5 1/4 inch floppy disks (and they really were floppy). Storage was still expensive. Only with low storage costs the volumes of data involved for storing protected works could be considered. In the early 1980s, the emphasis was on programs and the special type of programs used for gaming in the first low cost specially designed consoles brought out for the lower end of the consumer market. Also, infrastructure had to develop for the establishment for a market for protected works. This did not happen until the early 1990 as summarised above. These developments shaped the Web, and at the same time created the potential for a market in protected works which legal policies still are unfolding, and which promise an interesting future for the law of intellectual property related to information technology.

Conclusion

This paper started with an apology, and should end with one. It is a collection of loose ends, and no coherent presentation of the emergence of computers and law as a field of academic research or legal practice. In fact, this still has to be decided – though it may be convenient to bundle legal issues related to information technology together, it is still for the author uncertain whether this is for pragmatic reasons or for an underlying coherence of methods, knowledge or problems. To explore that question, an investigation needs to be much more in depth and in width than this paper permits. However, it is hoped that such a future investigations may find some morsels which are relevant in this collection of recollections, anecdotes and documentation.

54 Art 14.

OM FORHOLDET MELLOM PERSONOPPLYSNINGSLOVEN OG OFFENTLIGHETSLOVEN MV[1*]

Dag Wiese Schartum

1 Innledning

I denne artikkelen drøfter jeg forholdet mellom ny offentlighetslov[2] (lov om rett til innsyn i dokument i offentleg verksemd, heretter; "offl") og personopplysningsloven. Jeg behandler først spørsmål vedrørende de to lovenes virkeområde. Oppmerksomheten blir deretter rettet mot viktige berøringspunkter mellom de to lovene. Jeg stiller også spørsmålet om hvordan personopplysningsloven kan sies å virke inn på realiseringen av målet om åpenhet i offentlig virksomhet (jf. offl § 1), og har identifisert tre hovedgrupper av antagelser som vil bli nærmere drøftet:

- Personopplysningsloven kan ha betydning for innholdet av offentlige arkiver og hvilket materiale som det kan kreves innsyn i, se avsnitt 3;
- Personopplysningsloven kan ha betydning for i hvilken grad det kan gis offentlig innsyn i personopplysninger, se avsnitt 4;
- Personopplysningsloven har egne bestemmelser om innsynsrett for enhver, dvs. loven kan sies å utfylle offentlighetslovens innsynsrettigheter, se avsnitt 5.

Til slutt i artikkelen gir jeg en kortfattet, samlet vurdering av forholdet mellom de to lovene, med vekt på forslag som kan bidra til harmonisering og avklaring av forholdet mellom dem (avsnitt 6). Forslagene blir sammenfattet i avsnitt 7.

Gjennomgangen i dette avsnittet innebærer ingen fullstendig vurdering av forholdet mellom de to lovene. Utgangspunktet er at både personopplysningsloven og offentlighetsloven kommer til anvendelse når innsynsbegjæringer i

---

1* Artikkelen er basert på avsnitt 12.4 I Schartum, Dag Wiese og Bygrave, Lee A.: Utredning av behov for endringer i personopplysningsloven Skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet, Justisdepartementets rapportserie 2006; heretter: Schartum og Bygrave 2006.

2 Jf. Ot.prp. nr. 9 (2005–2006).

samsvar med offl § 3 innebærer behandling av personopplysninger.[3] En slik innsynssak kan for eksempel tenkes å utløse informasjonsplikt (pol § 20), og meldeplikt (pol § 31). Det vil også kunne være innsynsrett i personopplysninger på den innsynberettigedes hånd (pol § 18 annet og tredje ledd) osv. Jeg har ikke gjennomgått alle de situasjoner som kan oppstå når de to lovene anvendes i forhold til en innsynssak etter offentlighetsloven. Det betyr imidlertid ikke at slike situasjoner er uproblematiske.

2 Lovenes virkeområder mv.

Personopplysningslovens virkeområde avviker fra virkeområdet for ny offentlighetslov. Loven etablerer (med noen unntak) plikter for enhver som behandler personopplysninger, *uansett sektor*. Ny offentlighetslov etablerer plikter for staten, fylkeskommunene og kommunene samt visse andre rettssubjekter som treffer vedtak eller der stat, fylkeskommune eller kommune er involvert på nærmere angitte måter, se § 2. Dette innebærer at det ikke finnes noe del av forvaltningen eller offentlig virksomhet ellers som omfattes av offentlighetsloven uten samtidig å være omfattet av personopplysningsloven. Begge lover etablerer rettigheter for "enhver", men etter personopplysningsloven er det primært registrerte personer som har rettigheter.

Når det gjelder *saklig virkeområde*, er gjenstanden for regulering i personopplysningsloven hel eller delvis elektronisk behandling av personopplysninger samt behandling av personopplysninger som er eller skal inn i et personregister, se pol § 3. Dette innebærer at personopplysninger i papirdokumenter og andre analoge lagringsmedier som ikke er ordnet systematisk slik at personopplysninger om den enkelte kan finnes igjen, faller utenfor personopplysningsloven, samtidig som offentlighetslovens bestemmelser gjelder. Løse papirdokumenter og saksmapper med papirdokumenter mv. som er ordnet etter sakstype, kronologi og andre kriterier som ikke er knyttet til person, faller altså ikke inn under personopplysningsloven.[4] Dokumentene i en sak det skal gis innsyn i etter offentlighetsloven kan således tenkes å falle utenfor personopplysningsloven. Likevel kan begrensede deler av saken være omfattet, for eksempel fordi det er anvendt tekstbehandling for å utarbeide ett av dokumentene i en sak, eller fordi det er anvendt elektronisk kommunikasjon i tråd med fvl § 15a. Det kan virke uhensiktsmessig og tilfeldig at ulike dokumenter i én og samme forvaltningssak skal være undergitt ulike rettslige regimer vedrørende personvern.

3 Jf. dog Lovavdelingens uttalelse vedrørende personopplysningsloven § 6 (Saksnummer: 2004/04600). Uttalelsen er nærmere drøftet i neste avsnitt.

4 Se Ot.prp. nr. 92 (1998–99) s. 102.

Selv om personopplysningsloven ikke kommer til anvendelse på personopplysningene i saken det kreves innsyn i, kan loven komme til anvendelse på selve begjæringen om innsyn. Dette er i utgangspunktet tilfellet for en elektronisk henvendelse med begjæring om innsyn etter offentlighetsloven.

Gjenstand for regulering etter offentlighetsloven er forvaltningens "saksdokument, journalar og liknande register", se offl § 3. Loven bygger på samme definisjon av "dokument" som forvaltningsloven og arkivloven, dvs. "ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lytting, framsyning, overføring eller liknande", se offl § 4 første ledd. Både dokumentbegrepet i offentlighetsloven og "behandling av personopplysninger" i personopplysningsloven er teknologi- og medieuavhengige begreper. Dette gjør at det ikke finnes noen "personopplysning" etter personopplysningsloven som ikke kan tenkes å være del av et "dokument" etter offentlighetsloven.

Personopplysningsloven har bestemmelser om *geografisk virkeområde* som eksplisitt tar høyde for den internasjonale karakteren som preger deler av vår tids informasjonsbehandling, se pol § 4. Således gjelder norsk lov (bare) i to situasjoner: (i) når den som behandler personopplysningene er etablert i Norge; og (ii) når den behandlingsansvarlige er etablert utenfor EØS samtidig som det benyttes utstyr (for annet enn transmittering) som er plassert i Norge. Dersom den behandlingsansvarlige er etablert i et EØS-land, gjelder vedkommende lands personopplysningslovgivning, *også for behandling av personopplysninger som skjer i Norge*. Personverndirektivet forutsetter at et lands tilsynsmyndighet (i Norge; Datatilsynet) kan håndheve et annet EØS-lands lovgivning på sitt territorium, og landenes tilsynsmyndigheter skal samarbeide, se direktivets artikkel 28 nr. 6. Det kan således for eksempel skje at det behandles personopplysninger i Norge for en behandlingsansvarlig som kun er etablert i Spania[5] Reglene for behandlingen av disse opplysningene, herunder kravene til kvalitet, sletting, utlevering (til norske forvaltningsorganer mv.) vil normalt (i eksempelet) følge spansk lov, som Datatilsynet kan håndheve i samarbeid med spanske myndigheter.[6]

I offentlighetsloven er det så vidt vites ikke gjort forbehold om hvor rettssubjekter som kommer inn under loven[7] må være etablert, og det må derfor antas at den nye loven også vil gjelde rettssubjekter som er etablert i utlandet. Dette kan trolig være aktuelt for enkelte selvstendige rettssubjekter som kommer inn under loven. I så fall vil ny offentlighetslov gjelde, men ikke den

5 Behandlingen vil da for eksempel skje i regi av en databehandler som befinner seg i Norge, dvs. en virksomhet som behandler opplysningene på den behandlingsansvarliges vegne, se pol § 2 nr. 5.

6 Se nærmere om dette i Schartum og Bygrave 2006, kapittel 4.

7 Disse betegnes "organ" i loven, se offl § 4 siste ledd.

norske personopplysningsloven. Derimot vil personopplysningslov-givningen i landet der rettssubjektet (behandlingsansvarlig) er etablert gjelde. Selv om personverndirektivet utgjør en felles ramme for EØS-land, kan det her være forskjeller mellom landene.

Forholdet mellom offentlighetsloven og personopplysningslovgivning vil med andre ord variere avhengig av hvor rettssubjektet er etablert innen EØS. Dersom norske myndigheter for eksempel etablerer et selskap i Spania som skal arbeide for å øke tilstrømningen av spanske turister til Norge e.l.,[8] vil norsk offentlighetslov og spansk personopplysningslov gjelde. En person som det er registrert opplysninger om i Spania hos et norsk rettssubjekt som kommer inn under virkeområdet etter offl § 2, kan derfor hevde at opplysningen skal slettes etter spansk personopplysningslov, slik at det ikke kan gis innsyn i opplysningene etter norsk offentlighetslov. I andre tilfelle gjelder offentlighetsloven og personopplysningsloven samtidig. I fortsettelsen drøfter jeg bare sist nevnte situasjon.[9]

I personopplysningsloven § 6 første ledd heter det:

> *§ 6. Forholdet til lovbestemt innsynsrett etter andre lover*
>
> *Loven her begrenser ikke innsynsrett etter offentlighetsloven, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger.*

I en uttalelse fra Justisdepartementets lovavdeling[10] heter det om denne bestemmelsen at:

> *Dette innebærer at reglene i personopplysningsloven ikke kommer til anvendelse i den utstrekning offentlighetsloven eller annen lovgivning gir rett til innsyn i personopplysninger. I slike tilfeller skal det med andre ord gis innsyn uavhengig av vilkårene i personopplysningsloven kapittel II. Dette gjelder bare så langt offentlighetsloven eller annen lovgivning gir innsynsrett. I forhold til offentlighetsloven innebærer dette at personopplysningsloven ikke skal gjelde ved offentliggjøring av dokumenter som er omfattet av hovedregelen om innsynsrett i offentlighetsloven § 2 første ledd, og som*

8 Jf. den type rettssubjekter som er beskrevet i offl § 2 første ledd bokstavene c og d.

9 Det er også grunn til å foreta en nærmere grenseoppgang etter de to lovene i forhold til unntakene i pol § 3 annet ledd ("behandling av personopplysninger … for rent personlige eller private formål") og § 7 for opplysninger som behandles for formål som "utelukkende [er] kunstneriske, litterære, journalistiske, herunder opinionsdannende".

10 Saksnummer: 2004/04600, datert 16.07.2004.

ikke samtidig er omfattet av unntaksreglene i offentlighetsloven eller i annen lovgivning.

Her gis det med andre ord uttrykk for at personopplysningsloven *ikke gjelder* når innsyn skal skje i henhold til hovedregelen i offentlighetsloven. Innenfor rammene av meroffentlighet, hevder Lovavdelingen at personopplysningsloven og vilkårene i §§ 8 og 9 kommer til anvendelse, fordi innsynet i dette tilfellet beror på et skjønn og ikke en "rett", jf. formuleringen i pol § 6 første ledd ("innsynsrett"). Lovavdelingen bygger primært sin konklusjon på en fortolkning av pol § 6, noe som innebærer et tilsvarende resultat i forhold til den nye offentlighetsloven (som bygger på samme hovedregel og plikten til å vurdere meroffentlighet).

Det er grunn til å si seg uenig med Lovavdelingens fortolkning. Lovavdelingen trekker ikke direkte inn forarbeidene til personopplysningsloven. Her uttaler departementet at "bestemmelsen [§6] … understreker i *første ledd* at personopplysningsloven ikke innskrenker andre lovbestemte innsynsrettigheter".[11] Jeg forstår dette som en uttalelse om personopplysningsloven ikke kan fortolkes slik at den innskrenker lovbestemt innsynsrett. Dette er prinsipielt forskjellig fra at loven "ikke kommer til anvendelse"/"ikke skal gjelde", slik Lovavdelingen uttrykker det. Jeg velger derfor å legge til grunn at personopplysningsloven gjelder i forhold til innsyn i henhold til offentlighetsloven, også når innsyn skjer i forhold til hovedregelen i § 2 første ledd. Samtidig må imidlertid personopplysningsloven fortolkes slik at den ikke innskrenker lovfestede innsynsrettigheter. Med en slik tilnærming vil innsynberettigede personer få tilgang til like mye som etter Lovavdelingens fortolkning. Forskjellen ligger primært i en tydeliggjøring av plikten til å vurdere om det foreligger slik lovbestemt innsynsrett eller ikke.[12] Det er uansett uheldig å hevde at person-opplysningsloven får anvendelse i forhold til noen deler av offentlighetsloven men ikke andre, fordi dette gir et unødig komplisert forhold mellom de to lovene. I nedenstående diskusjoner har jeg lagt min forståelse av pol § 6 første ledd til grunn. Det er likevel primært resonnementer og begrunnelser, og ikke konklusjoner, som avviker fra det som ville fulgt på basis av Lovavdelingens uttalelse.

11 Se Ot.prp. nr. 92 (1998–99) s. 106.

12 Jf. vårt forslag til (ny) § 8 der plikten til å undersøke om det foreligger taushetsplikt er gjort eksplisitt.

3 Betydningen av personopplysningsloven for tilfanget av saksdokument som det er allmenn innsynsrett i

Personopplysningsloven kan tenkes å virke inn på adgangen til å samle inn/registrere og beholde personopplysninger. I den grad loven begrenser informasjonsinnsamling eller adgang til å lagre personopplysninger, begrenser den også det materialet som det kan kreves innsyn i.

Personopplysningsloven stiller opp visse *grunnkrav* som må tilfredsstilles for at det skal være lovlig for den behandlingsansvarlige (f.eks. forvaltningsorganer og andre rettssubjekter som kommer inn under ny offentlighetslov) å behandle personopplysninger. Dette gjelder krav til rettslig grunnlag (§§ 8 og 9), krav til angivelse av saklig begrunnede formål for behandlingen av personopplysninger (§ 11 bokstav b – c), krav til informasjonskvalitet (§ 11 bokstav d – e), krav til sikring av personopplysninger (§ 13) og krav til gjennomføring av internkontroll (§ 14). Dersom forvaltningen ikke etterlever slike krav, er behandlingen i utgangspunktet ulovlig. Et spørsmål er i så fall om innsyn etter offentlighetsloven kan omfatte personopplysninger som blir ulovlig behandlet av vedkommende. Spørsmålet kommer på spissen dersom opplysningene mangler rettslig grunnlag, jf. § 8, for eksempel dersom det gjennom nettstedet i en offentlig virksomhet samles inn personopplysninger som det ikke foreligger lovhjemmel eller "nødvendig grunn" for, og der det derfor skulle ha vært innhentet samtykke. Dersom dette ikke er gjort, er videre behandling av opplysningene ulovlig, og de skal slettes i henhold til pol § 27 første ledd som bl.a. gjelder det tilfellet at det "ikke er adgang til å behandle" personopplysningene. Unntaksbestemmelsene i § 27 som gir adgang til likevel å beholde opplysningene, gjelder tilfeller der opplysningene er uriktige eller ufullstendige, og sletteplikten fremstår derfor som absolutt. Jeg går ikke nærmere inn på en diskusjon om det kan være grunnlag for likevel å beholde opplysningene, men nøyer meg med å konkludere med at dette i beste fall er tvilsomt. Foreligger det slik sletteplikt, vil det innebære at det ikke kan gis innsyn i de personopplysninger som for eksempel er resultatet av den offentlige virksomhetens brudd på pol § 8.

Også sletteplikten i pol § 28 første ledd er viktig i forhold til eksistensen av saksdokumenter i offentlig virksomhet. Utgangspunktet her er at personopplysninger ikke kan oppbevares lenger enn det som er "nødvendig for å gjennomføre formålet med behandlingen". Opplysninger i personregistre og persondatabaser mv. skal med andre ord slettes fortløpende etter hvert som den behandlingsansvarlige (f.eks. en offentlig virksomhet) har anvendt opplysningene i tråd med innsamlingsformålet, med mindre formålet begrunner fornyet/fortsatt behandling senere. For saksdokumenter der personopplysningene inngår i en sakprosatekst, bilde mv., innebærer bestemmelsen at

hver personopplysning skal slettes, mens dokumentet for øvrig kan beholdes. Unntaket er hvis dokumentet gir et åpenbart misvisende bilde etter slettingen. I så fall skal hele dokumentet slettes, se § 28 siste ledd.

Sletting skal likevel ikke skje dersom opplysningene skal oppbevares etter arkivloven eller annen lovgivning som pålegger videre lagring. Dette siste gjelder for eksempel forskrift i medhold av helsepersonelloven.[13]

Arkiveringsplikten etter arkivloven[14] gjelder for "offentlege organ" (arkl § 5, jf. § 2 bokstav g), og dekker neppe alle slike virksomheter som kommer inn under offentlighetsloven, se dennes § 2 første ledd bokstavene a – d. I proposisjonen til arkivloven sies det bl.a. at arkiv i statsforetak skal regnes som private (ikke offentlige) arkiv. Det er derfor tvilsomt om alle slike rettssubjekter som kommer inn under offl § 2 bokstavene c og d kommer inn under arkivloven.

I offl § 10 er det etablert plikt til å føre journal for "organ" som er omfattet av loven, jf. § 4 siste ledd. For slike organ som også er regnet som "offentlege organ" etter arkl § 2 bokstav g, gjelder det et bevaringspåbud for journaler og andre registre, se arkivforskriften § 3-20 bokstavene e og f så langt arkivloven gjelder, er pol § 28 første ledd derfor ikke til hinder for at slikt materiale beholdes intakt. For offentlige virksomheter som ikke er "offentlege organ" etter arkivloven, gjelder imidlertid intet bevaringspåbud etter arkivforskriften, og personopplysninger i journaler mv. skal derfor i utgangspunktet slettes når formålet med behandlingen ikke lenger tilsier lagring.

Før jeg ser nærmere på unntaksalternativene i pol § 28, vil jeg gå nærmere inn på kriteriet i § 28 første ledd, og spørsmålet om hva som menes med at fortsatt lagring er "nødvendig for å gjennomføre formålet med behandlingen [av personopplysninger]".[15] Særlig er det viktig å bringe klarhet i hva som menes med "formål" i denne sammenhengen, og om praktisering av innsynsrett etter offentlighetsloven kan ses som et eget formål som begrunner fortsatt lagring.

I merknadene til pol § 28 diskuterer departementet tilfeller der det er behov for å utføre kontroll av en behandling av personopplysninger som i utgangspunktet er ferdigbehandlet. Departementet går i slike tilfeller ut i fra at opplysningene kan beholdes selv om "hovedformålet" er oppfylt.[16] Det synes imidlertid som om Personvernnemnda har lagt seg på en forholdsvis streng

13 Lov 2. juli 1999 nr. 64, jf. journalforskriften (forskrift 21. desember 2000 nr. 1385) § 14 som bestemmer at legejournal ikke skal avleveres til arkiv eller deponeres før 10 år etter siste innførsel i journalen.

14 Lov 4. desember 1992 nr. 126.

15 Jf. også pol § 11 første ledd bokstav e.

16 I Wiik Johansen m.fl. 2001 sies kun det samme som i departementets merknader.

praksis i spørsmålet om sletting etter § 28.[17] Jeg går ikke her nærmere inn på hvorledes grensene er trukket eller bør trekkes i fremtiden. Likevel er det grunn til å minne om at det særlig i forhold til offentlig myndighetsutøvelse er et poeng at beslutningspraksis, herunder beslutningsgrunnlag, bør kunne være tilgjengelig etter at vedtak er truffet og beslutningsformålet nådd. Særlig trekker hensynet til tilstrekkelig legalitetskontroll av fattede vedtak og forsvarlig saksutredning av fremtidige enkeltsaker i retning av at personopplysninger må kunne lagres etter at personopplysningene har vært anvendt for det primære innsamlingsformålet.

En mulighet er å se realisering av offentlighetsloven som et "fast formål" for all behandling av åpne personopplysninger[18] i offentlig virksomhet. I så fall blir dette et "evigvarende" formål, som motvirker at personopplysninger som det er innsynsrett i blir slettet. Dette er neppe en mulig løsning. For det første har den klart preg av å være en konstruksjon for å ivareta hensynet til offentlig innsyn. For det andre fører det til at personverndirektivet artikkel 6 ikke blir gjennomført i forhold til offentlig virksomhet.[19]

Personopplysningsloven § 28 annet ledd åpner for at personopplysninger kan lagres ut over den tid formålet med innsamlingen tilsier når fortsatt lagring skjer for historiske, statistiske eller vitenskapelige formål og hensynet til slike formål klart overstiger hensynet til personvern. Vilkåret er videre at opplysningene anonymiseres dersom fortsatt identifisering ikke er nødvendig. Loven må forstås slik at anonymisering skal skje dersom identiteter ikke er nødvendig for å bruke opplysningene til de historiske, statistiske eller vitenskapelige formålene som er anført som grunnlag for at opplysningene ikke skal slettes.[20]

Tredje ledd i pol § 28 åpner for å slette eller sperre personopplysninger selv om det i utgangspunktet er bestemt at opplysningene skal beholdes for historiske, statistiske eller vitenskapelige formål, jf. annet ledd. Vilkåret er at opplysningene er "sterkt belastende" for den personen opplysningene gjelder. Personvernnemnda har tolket bestemmelsen slik at sletting/sperring også kan skje selv om opplysningene er anonymiserte.[21] "Sterkt belastende" er et strengt

17 Se særlig sakene 2003 nr. 2, 2004 nr. 5 og 2005 nr. 6. Personvernnemnda synes å legge en strengere forståelse til grunn enn i departementets merknader. I f.eks. sak 2005 nr. 6 ble det bestemt at opplysninger i en vandelsattest som var innhentet i anledning ansettelse, måtte slettes etter at ansettelse hadde skjedd, fordi opplysningene i attesten senere ville være utdatert og ikke nødvendigvis gi et riktig bilde.

18 Dvs. ikke taushetsbelagte personopplysninger.

19 Jf. ordlyden: "1. […] personal data must be:
(c) […] not excessive in relation to the purposes for which they are collected and/or further processed".

20 Slik forstår jeg også Wiik Johansen m.fl. 2001 s. 208.

21 Se sak 2003 sak nr. 2.

vilkår. I tillegg må det ikke foreligge noe lovhjemlet plikt til å beholde opplysningene (jf. omtalen av særlovgivning ovenfor), og sletting/sperring må være "forsvarlig ut fra en samlet vurdering av bl.a. andres behov for dokumentasjon, hensynet til den registrerte, kulturhistoriske hensyn og de ressurser gjennomføringen av kravet forutsetter". Dette slettings-/sperringsalternativet kan derfor kun få en meget begrenset anvendelse.

Selv om den formelle adgangen til å slette/sperre personopplysninger er begrenset, er det viktig å være klar over at praksis lett kan tenkes å avvike fra lovens krav. Det er behandlingsansvarlig, dvs. den offentlige virksomheten som har de aktuelle personopplysningene, som avgjør om det skal skje anonymisering. Beslutningen skal treffes på grunnlag av meget sammensatte og skjønnsmessige bestemmelser i personopplysningsloven, på et område der det rettskildemessige grunnlaget (foreløpig) er forholdsvis tynt. Sletting og anonymisering skal per definisjon være irreversibelt, og slik beslutning skal derfor være endelig. Dersom anonymisering skjer, foreligger det ikke lenger personopplysninger og opplysningene vil ikke lenger komme inn under personopplysningsloven.

Femte og siste ledd i pol § 28 fastsetter at hele dokumentet skal slettes dersom de gjenværende opplysningene etter sletting av personopplysninger gir et åpenbart misvisende bilde. Dette alternativet har primært effekt i tilfelle der personopplysningene har inngått i dokumenter med saksprosa og annet lite formalisert innhold, og der de slettete opplysningene har vært bærende innholdselementer.

4 Betydningen av personopplysningsloven for allment innsyn i personopplysninger

4.1 Innledning og spørsmålet om formålsbegrensning

Personopplysningsloven inneholder ingen andre bestemmelser om taushetsplikt enn den i § 44, vedrørende Datatilsynets og Personvernnemdas egen taushetsplikt. Loven inneholder med andre ord ingen direkte begrensninger i allmennhetens innsynsrett i personopplysninger, og det er således offl § 13 første ledd i kombinasjon med ulike bestemmelser om lovbestemt taushetsplikt, som ivaretar de viktigste begrensninger i innsynsretten ut i fra hensynet til personvern. Personopplysningsloven kan imidlertid tenkes å innebære et *indirekte konfidensialitetsvern* som jeg kommer nærmere inn på i det følgende.

For det første krever personopplysningsloven at enhver behandling av personopplysninger "bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet", se § 11 første ledd bokstav

b. I ordrett betydning vil dette innebære at innsyn i personopplysninger med hjemmel i offentlighetsloven § 3, lovlig bare vil kunne skje dersom behandlingsansvarlig har formulert innsyn som et formål for behandlingen. Paragraf 11 må imidlertid tolkes i lys av pol § 6 første ledd der det heter at "Loven her begrenser ikke innsynsrett etter offentlighetsloven, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger". Det er lite tvilsomt at formålsbestemthetsprinsippet i personopplysningsretten ikke innebærer begrensninger av lovbestemte innsynsrettigheter, og jeg går derfor ikke nærmere inn på spørsmålet. Det er imidlertid uheldig at allmennhetens rett til innsyn ikke er tydeliggjort i personopplysningslovens bestemmelser om formålsbegrensninger. Spørsmålet har for øvrig bredere betydning enn i forhold til offentlighetsloven. Generelt må personopplysninger kunne knyttes til *ethvert* formål som er fastsatt i eller klart følger av eller i medhold av lov. Det bør derfor vurderes om dette bør presiseres i § 11, for eksempel slik det ble foreslått i Schartum og Bygrave 2006:

> **§ 11. Grunnkrav til behandling av personopplysninger**
>
> *"Den behandlingsansvarlige skal sørge for at personopplysningene som behandles*
>
> *[…]*
>
> *b) bare nyttes til uttrykkelig angitte eller lovbestemte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet" (Vår tilføyelse er satt i kursiv)"*

Offentlighetsloven § 11 inneholder en regel om merinnsyn:

> *"Når det er høve til å gjere unntak frå innsyn, skal organet likevel vurdere å gi heilt eller delvis innsyn. Organet bør gi innsyn dersom omsynet til offentleg innsyn veg tyngre enn behovet for unntak."*

Bestemmelsen gir anvisning på en bred avveining mellom hensynet til offentlig innsyn på den ene side, og behovet for unntak på den andre.[22] I behovet for unntak, inngår hensynet til personvern. Dette betyr at personvern kan tale mot merinnsyn. Samtidig skal en imidlertid være klar over at personvernhensyn

22 Bestemmelsen må trolig forstås slik at det ikke er vesentlig betydningsforskjell på "omsyn" og "behov" i lovteksten, og at det er tale om å veie to grupper av hensyn/behov mot hverandre.

også kan tale *for* merinnsyn. Dette er for eksempel tilfellet dersom innsyn begrenses til personopplysninger i en sak, og dette gir ufullstendig informasjon, jf. diskusjonen straks nedenfor av pol § 11 bokstavene d og e.

I tillegg til fastsettelse av og avgrensing til bestemte formål, må behandlingen av personopplysninger ha rettslige grunnlag. Dette rettslige grunnlaget må dekke alle aktuelle behandlingsformål, herunder formålet å gi innsyn til allmennheten, se pol § 8.[23] I tilfellet offentlig innsyn vil offl § 3 være tilstrekkelig lovhjemmel, se § 8 første ledd, første setning. Også i forhold til merinnsyn foreligger det lovhjemmel, se offl § 11. Kravet i personopplysningsloven om rettslig grunnlag kan med andre ord ikke begrense innsynsretten etter offentlighetsloven.[24]

4.2 Krav til opplysningskvalitet

Personopplysningsloven stiller krav til opplysningskvalitet mv, se pol § 11 første ledd bokstavene d og e. Personopplysningene skal for det første være tilstrekkelige og relevante *i forhold til formålet*. Når formålet er å oppfylle lovbestemte krav om innsyn i saksdokumenter, herunder i personopplysninger, kan disse kravene neppe virke i innskrenkende retning. Kravet om relevans må ses i sammenheng med kravet til spesifisering/avgrensing av innsynskrav etter offentlighetsloven, se offl § 28 annet ledd. Innsynet kan gjelde en bestemt sak, eller i rimelig utstrekning saker av bestemt art, eller journal eller lignende register. Uansett må de personopplysninger som følger av saken/samlingen av saker/journal mv. regnes som relevante, og det er neppe grunnlag for å gjøre noen begrensninger som spesielt gjelder tilgangen til personopplysninger (annet enn det som følger av regler om taushetsplikt og taushetsrett, jf. offl §§ 13 og 11). Kravet om tilstrekkelighet innebærer at det må gis så mye opplysninger at formålet med å kreve innsyn kan tilfredsstilles, noe som trekker i retning av at alle relevante opplysninger skal være omfattet av innsynet. Dette kan i konkrete tilfelle gi innsyn i *flere* personopplysninger enn det som direkte følger av innsynskravet. Dersom innsynskravet gjelder en bestemt sak som inneholder ufullstendige personopplysninger, tilsier kravet om tilstrekkelighet i pol § 11 første ledd bokstav d at opplysningene som ligger til saken suppleres av slike andre relevante personopplysninger som skal til for å gi et tilstrekkelig opplysningsgrunnlag.

23 Personopplysningsloven § 9 er ikke aktuell i forhold til innsyn fordi det alltid er taushetsplikt for sensitive personopplysninger.

24 Men personvern er et relevant hensyn når meroffentlighet skal bedømmes.

For det andre skal personopplysningene være korrekte og oppdaterte. Når det gjelder krav til korrekthet, må opplysningene slik de foreligger, være tilstrekkelig korrekte i forhold til innsynsformålet – selv om opplysningene objektivt sett er uriktige. Hensynet til tilstrekkelighet (jf. ovenfor), kan imidlertid i slike tilfelle tenkes å begrunne at andre, korrekte personopplysninger blir omfattet av innsynet. Kravet til oppdaterte personopplysninger, kan på samme måte begrunne at det gis supplerende og mer oppdaterte opplysninger enn det som ligger til en bestemt sak det er bedt om innsyn i. For øvrig tilsier både personopplysningslovens krav om ajourhold og realiseringen av innsynsretten, jf. offl § 1, at det gis tilgang til alle saksdokumenter og personopplysninger som det er innsynsrett i per dato for innsynskravet.[25]

4.3 Sammenstilling av personopplysninger

Offentlighetsloven § 9 inneholder en rett til, "med enkle framgangsmåtar", å kreve innsyn i en *sammenstilling* av personopplysninger som er lagret i organets databaser. Sammenstillingen kan både tenkes innen én og samme database, og mellom ulike databaser. Sammenstilling innebærer det en tidligere benevnte "kopling" av personregistre. I den nå opphevde personregisterloven § 11 annet ledd nr. 3 var det fastsatt at adgangen til å kople opplysninger skulle reguleres i konsesjonen. Et meget stort antall registre var underlagt konsesjonsplikt.

Personopplysningsloven har ingen særskilte regler vedrørende kopling/sammenstilling av personopplysninger. Slik behandling må imidlertid følge lovens alminnelige krav, bl.a. i forhold til opplysningskvalitet, se pol § 11 første ledd bokstavene d og e. I tillegg er det i pol § 21 regulert særlige tilfeller der resultatet av sammenstilling av opplysninger resulterer i "personprofiler". Bestemmelsen legger ingen begrensninger på hvilke profiler som kan lagres, men stiller krav til å informere de personer som mottar henvendelser eller blir gjenstand for beslutninger på grunnlag av slike profiler. Dette får derfor først betydning dersom den innsynberettigede bruker de personprofiler som sammenstilling av databasene gir til å henvende seg/beslutte slik pol § 21 beskriver.

4.4 Utlevering av personopplysninger

Offentlighetsloven § 30 har bestemmelser om gjennomføring av innsyn. Sett fra person-opplysningsloven innebærer gjennomføring av innsyn som omfatter personopplysninger, at den offentlige virksomheten *utleverer* og den

25 Personopplysningsloven § 11 første ledd bokstav e regulerer også varigheten av lagringen av personopplysninger, jf. pol §§ 27 og 28.

innsynberettigede *mottar* personopplysninger. Både for utlevering og mottak/innsamling av personopplysninger gjelder det bestemmelser i personopplysningsloven som det i utgangspunktet må tas hensyn til ved gjennomføringen av innsyn etter offentlighetsloven.

Når en innsynsberettiget person mottar personopplysninger, er det første spørsmålet om dette skjer på en slik måte at vedkommende selv blir behandlingsansvarlige og derfor må behandle opplysningene i samsvar med personopplysningslovens bestemmelser. For at person-opplysningsloven skal komme til anvendelse på den innsynberettigede, må forholdet komme inn under lovens saklige og geografiske virkeområde, jf. pol §§ 3 og 4. Dette innebærer for eksempel at utlevering av dokumenter som ikke er elektroniske og som ikke inneholder personregister, faller utenfor loven. For øvrig er utgangspunktet at loven kan komme til anvendelse. Forutsetningen er imidlertid at den innsynberettigede ikke helt eller delvis er unntatt fra lovens bestemmelser: Skjer innsynet for rent personlige eller private formål, oppstår ikke behandlingsansvar etter loven, se pol § 3 annet ledd. Skjer innsynet for journalistiske mv. formål, vil bare mindre deler av loven gjelde for den innsynberettigede som mottar opplysningene, jf. pol § 7. I andre saker kan lovens bestemmelser komme til anvendelse på den innsynberettigedes videre behandling av personopplysninger. Forutsetningen er imidlertid at opplysningene enten inngår i en *eksisterende* behandling av personopplysninger (for eksempel når innhentede opplysninger legges ut på den innsynberettigedes nettside), eller at det etableres en *ny* behandling av personopplysninger i sakens anledning (en interesse-organisasjon starter for eksempel kartlegging av hvilke personer som har deltatt ved behandlingen av visse kommunale saker). Dersom personopplysningsloven kommer til anvendelse på den innsynberettigede i rollen som behandlingsansvarlig, innebærer dette at den innsynberettigedes må etterleve en rekke krav til den videre behandling av de innhentede opplysningene.

Offentlige virksomheter som utleverer personopplysninger som ledd i etterlevelsen av offl § 3, må etterleve personopplysningsforskriftens (pof) krav til sikring av personopplysninger (i pof kap. 2). Utgangspunktet er da at "[d]en behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her", se pof § 2-15. Kravet gjelder kun *elektronisk* overføring. Unntak er gjort i annet ledd for overføring av personopplysninger til utlandet i samsvar med pol §§ 29 og 30, samt når det er "fastsatt i lov at det er adgang til å kreve opplysninger *fra et offentlig register*" (vår kursiv). Siste unntaksalternativ innebærer at det kan utleveres opplysninger fra folkeregisteret, ektepaktregisteret, kjøretøyregisteret mv. uten at registermyndigheten forsikrer seg om at mottakeren behandler de mottatte personopplysningene i samsvar med kravene i personopplysningsloven. Lignende

unntak er imidlertid ikke gjort for utlevering av opplysninger i samband med allmenninnsyn etter offl § 3 eller partsinnsyn etter offentlighetsloven § 18. Spørsmålet er ikke nærmere diskutert i kommentarene til forskriftsbestemmelsen som var del av kgl. res. 15. desember 2000 nr. 1265 der forskriften ble vedtatt.

Med forskriftens spesifikke angivelse av et unntak knyttet til offentlig register, kan det neppe konkluderes med at unntaket også gjelder etter offentlighetsloven. Konklusjonen er derfor at den offentlige virksomheten – i utgangspunktet – plikter å forvisse seg om at den personopplysningene blir utlevert til selv vil etterleve personopplysningsforskriften. Forskriften sier intet om hvorledes dette skal skje, men i kommentarene til pof § 2-15 forutsettes det at den behandlingsansvarlige som skal gi fra seg opplysninger skal få kunnskap om innholdet i sikkerhetsdokumentasjon mv. Dette er igjen knyttet til bestemte sikkerhetsgjennomganger mv. som forskrifter pålegger behandlingsansvarlige å gjennomføre. Plikten etter pof § 2-15 kan imidlertid ikke gjelde i forhold til innsynberettigede som ikke kommer inn under loven, jf. pol § 3 annet ledd om "rent personlige eller andre private formål". Bestemmelsen er imidlertid virksom i andre tilfeller, for eksempel i forhold til pressen.[26]

Plikten etter pof § 2-15 innebærer en plikt til å nekte overføring av personopplysninger *i elektronisk form* til innsynberettigede som ikke tilfredsstiller kravene i pof kapittel 2 om informasjonssikkerhet. Teoretisk sett kan dette innebære at innsynsretten må gjennomføres på måter som ikke innebærer utlevering av elektronisk materiale.

Kravene vedrørende overføring av personopplysninger til (f.eks.) en innsynsberettiget er med andre ord strenge og tungvinte i de tilfelle overføringen skjer elektronisk. Dersom opplysningene utleveres på papir eller lignende, oppstår ingen tilsvarende krav. Det er grunn til å tro at innsyn i stadig større omfang vil bli gjennomført i elektronisk form. I eforvaltningsforskriften (efvf)[27] er det i § 10 dessuten lagt til rette for at dette kan skje. Bestemmelsen slår for det første fast at det kan gis tilgang til opplysninger og dokumenter i elektronisk form dersom forvaltningsorganet fører elektronisk arkiv og den innsynberettigede samtykker eller går med på det. Paragraf 10 viser ikke til personopplysningsloven eller -forskriften, men i efvf § 13 tredje ledd bokstav g vedrørende sikkerhetsmål og sikkerhetsstrategi, er det gjort henvisning til pol § 13 og pof kapittel 2 (om informasjonssikkerhet). Dette må forstås slik at forvaltningsorganer har plikt til å fastlegge mål og strategier for å sikre

26 Se pol § 7 som bl.a. fastsetter at lovens bestemmelser om informasjonssikkerhet (§ 13) skal gjelde for journalistisk virksomhet.

27 Forskrift 25. juni 2004 nr. 988.

gjennomføringen av bl.a. pof § 2-15, herunder i samband med praktisering av "elektronisk innsyn", jf. efvf § 10.

Som tidligere nevnt har offentlighetsloven et videre saklig virkeområde enn arkivloven fordi "organ" i offl § 4 siste ledd, jf. § 2 første ledd bokstavene c og d, favner videre enn "offentleg forvaltningsorgan". Det samme gjelder forholdet mellom "organ" etter offentlighetsloven og "forvaltningsorgan" i betydningen "et hvert organ for stat eller kommune" etter forvaltningsloven. Samspillet mellom eforvaltningsforskriften og personopplysnings-forskriften som jeg nylig har redegjort for, er derfor ikke til stede for alle "organ" som kommer inn under offentlighetsloven.

5 Betydningen av personopplysningsloven for allment innsyn i annet enn personopplysninger

Personopplysningsloven inneholder innsynsrettigheter som supplerer offentlighetslovens regler om innsyn for enhver, se pol § 18 første ledd. Denne bestemmelsen gir enhver rett til å få opplysning om slike informasjonssystemer og -rutiner som behandler personopplysninger. Loven angir som utgangspunkt en gitt mengde opplysninger:

a. navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
b. hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,
c. formålet med behandlingen,
d. beskrivelser av hvilke typer personopplysninger som behandles,
e. hvor opplysningene er hentet fra, og
f. om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Anvendt på offentlige virksomheter, innebærer dette i virkeligheten en rett til å få beskrevet viktige deler av beslutningssystemer og informasjonsutveksling der offentlige organer mv. deltar. Siden det ikke eksisterer noen plikt eller fast foranledning til å produsere saksdokumenter som inneholder slike opplysninger, vil dette ofte være kunnskaper det ikke er mulig å erverve ved å kreve innsyn etter offentlighetsloven. Slik sett er bestemmelsen et viktig supplement til offl § 3.

Personopplysningslovens § 18 første ledd gjelder uavhengig av sektor, noe som innebærer at bestemmelsen ofte også vil gjelde kilder for og mottakere av personopplysninger som en offentlig virksomhet behandler. Denne innsynsretten

kan således også benyttes for å få innsyn hos aktører som offentlige virksomheter samhandler med. Også slik innebærer pol § 18 første ledd et viktig supplement til offl § 3.[28]

I § 23 gjør personopplysningsloven felles unntak fra bestemmelser om innsyn og informasjon, med i alt 6 unntakskategorier som er sterkt inspirert av forvaltningsloven og offentlighetsloven av 1970. Offentlighetsloven (av 2006) har i alt 13 unntakskategorier, hvorav noen ligner enkeltkategorier i pol § 23, mens andre unntak gjelder spesifikke typer saksdokumenter som ikke er nevnt i personopplysningsloven. Fordi innsyn for enhver etter personopplysningsloven kun gjelder beskrivelse av informasjonssystemer og -rutiner, og fordi denne loven bare gjelder elektronisk behandling og personregistre, vil det trolig ikke være mulig å få tilgang til opplysninger som er unntatt fra innsyn etter offentlighetsloven ved å kreve innsyn etter personopplysningsloven.

Personopplysningsloven gir både innsyn for enhver (§ 18 første ledd) og innsyn for den registrerte (§ 18 annet og tredje ledd). Dette innebærer at begge innsynsrettigheter utfyller andre, brede innsynsbestemmelser; særlig de i fvl § 18 og offl § 3. Dette er noe av bakgrunnen for at det i pol § 6 annet ledd er satt inn en bestemmelse om plikt for behandlingsansvarlige til å veilede om annen lovbestemt innsynsrett: "Dersom annen lovbestemt rett til innsyn gir tilgang til flere opplysninger enn loven her, skal den behandlingsansvarlige av eget tiltak veilede om retten til å be om slikt innsyn". Personer som retter spørsmål til en offentlig virksomhet som kommer inn under offentlighetslovens bestemmelser, vil alltid også ha rett til innsyn etter pol § 18 første ledd. På denne bakgrunn ville det både være logisk og rimelig dersom det i offentlighetsloven og forvaltningsloven ble tatt inn en plikt til å veilede om annen lovbestemt innsynsrett, eventuelt avgrenset til annen innsynsrett for enhver, som den i pol § 18 første ledd.

6 Kort om ivaretakelse av personvern og forekomster av personvernrelaterte begreper i offentlighetsloven

På lignende måte som personopplysningsloven fremmer offentlighet, inneholder bestemmelser i offentlighetsloven bestemmelser som ivaretar personvern. Dette gjelder primært offl § 13 som fastsetter at det ikke er innsyn i dokumenter som er omfattet av lovbestemt taushetsplikt. Unntak på grunn av

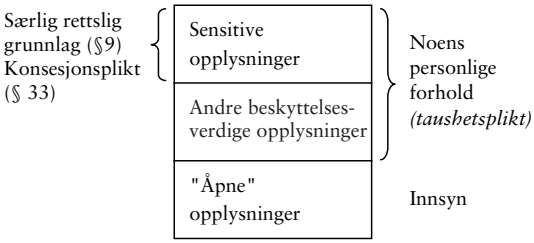
28 I tillegg til innsynsretten for enhver etter pol § 18 første ledd, har personopplysningsloven individuelle innsynsrettigheter etter § 18 annet og tredje ledd.

taushetsplikt skal også foretas av selvstendige rettssubjekter som kommer inn under offentlighetsloven[29] i samme omfang som fvl § 13 fastsetter.

For ivaretakelsen av personvern er taushetsplikt for opplysninger om "noens personlige forhold" det avgjørende. "Noens personlige forhold" er en egen kategori opplysninger som ikke uten videre passer inn i, eller har et avklaret forhold til den nært beslektete terminologien i personopplysningsloven. Begrepet ligger antagelig innenfor begrepet "personopplysning" i den forstand at det kun er tale om opplysninger om fysiske personer. Ved avgrensingen av "noens personlige forhold" er det vanlig å gå kasuistisk til verks for å undersøke hvor grensen går i forhold til "åpne" opplysninger om personer.[30] Dersom vi imidlertid legger definisjonen av "personopplysning" til grunn, genererer dette en rekke spørsmål vedrørende "noens personlige forhold" som det ikke uten videre er lett å ta stilling til på grunnlag av lovteksten:

- Gjelder taushetsplikten både for levende og døde personer?
- Må opplysningen faktisk være koplet til en person, eller er det nok at opplysningen er potensiell?
- Hvor indirekte og sammensatt kan koplingen mellom opplysningen og personen være?
- Hvor sikker må tilknytningen mellom opplysningen og personen være?
- Hvor sikker/klar må personens identitet være?

Poenget her er for det første at det er usikkert om "noens personlige forhold" er betegnelsen på en "personopplysning", slik dette begrepet er definert i pol § 2 nr. 1. Vurdert opp i mot kulepunktene ovenfor, taler mye for at "noens personlige forhold" bygger på et smalere begrep enn "personopplysning". I tillegg kommer at noens personlige forhold er betegnelsen på en kvalifisert gruppe opplysninger om personer, dvs. det foretas implisitt en todeling der noen opplysninger ikke hører til personlige forhold (og er åpne for innsyn), mens andre gjør det (og



29 Jf. § 2 første ledd bokstavene c og d. Slike rettssubjekter kommer i utgangspunktet ikke inn under forvaltningsloven, og hjemmel til å unnta på grunn av taushetsplikt er derfor satt inn i offl § 13 andre ledd.

30 Se f.eks. Lovavdelingens uttalelse vedrørende forståelsen av fvl § 13 og § 13a (Saksnummer: 1998/10047 E AS/ØØ), datert 19. november 1998.

er underlagt taushetsplikt). På en måte er "noens personlige forhold" en kvalifisering av noen opplysninger som følsomme. Likevel tilsvarer ikke "noens personlige forhold" "*sensitiv* personopplysning" i pol § 2 nr. 8. Sensitive personopplysninger hører trolig alltid til "noens personlige forhold", mens "noens personlige forhold" slett ikke alltid er sensitive i personopplysningslovens forstand. Vi har med andre ord med tre sensitivitetsgrader å gjøre, der det kun er et etablert navn på den høyeste graden og et felles navn på de to høyeste gradene. Jeg velger å kalle den mellomste kategorien for "andre beskyttelsesverdige opplysninger", og den nederste for "åpne opplysninger".

Poenget i denne sammenhengen er at offentlighetsloven bruker fvl § 13 som mellomstasjon for å angi de personopplysninger som det er taushetsplikt for. Forvaltningsloven § 13 bygger imidlertid på en begrepsbruk som passer dårlig inn i forhold til definisjonen av "personopplysning" i pol § 2 nr. 1. Samtidig gjør offl § 10 tredje ledd en direkte henvisning til pol § 2 nr. 1 (i en forskriftshjemmel). Også i § 26 tredje ledd gjøres det en henvisning som det er nærliggende å tolke som en referanse til personopplysningsloven. Det heter her at unntak fra innsynsrett kan gjøres for "personbilete som er teke inn i eit personregister". Det er nærliggende å tolke "personbilete" som et begrep som bygger på "personopplysning" i pol § 2 nr. 1, særlig fordi det figurerer sammen med "personregister" som er definert i § 2 nr. 3.

Analysen ovenfor viser at offentlighetsloven forholder seg til personopplysningsbegrepet på tre forskjellige måter:

- Til forvaltningslovens § 13 første ledd, noe som gir et uavklart forhold til pol § 2 nr. 1;
- Til personopplysningslovens definisjoner, men uten klar henvisningsstruktur;
- Til pol § 2 nr. 1 med direkte og klar henvisning.

Etter min mening er dette en klar indikasjon på at forholdet mellom offentlighetsloven og personopplysningsloven bør være gjenstand for systematiske vurderinger, bl.a. av lovteknisk karakter. Det er åpenbart behov for å rydde opp i begrepsbruken for å oppnå sammenheng mellom sentrale begreper i personopplysningsloven, offentlighetsloven og forvaltningsloven. Særlig bør dette gjelde betegnelser på opplysninger som gjelder personer. En slik samordning må også innbefatte fvl § 13 og "noens personlige forhold.

7 Allmenne vurderinger og forslag

Etter min mening er det behov for en nærmere avklaring av forholdet mellom personopplysningsloven og offentlighetsloven. I tråd med forslaget i Schartum og Bygrave 2006, antar jeg det er behov for å gjøre endringer i begge lover:

- Det bør gjøres endringer i personopplysningsloven som tydeliggjør at allmennhetens lovbestemte innsyn i "åpne" personopplysninger ikke er i konflikt med denne lovens bestemmelser.
- En bør vurdere å ta inn i begge lover en "regibestemmelse", dvs. en bestemmelse som minner om eksistensen av den andre loven, og nærmere angir betydningen av denne.
- Det bør innføres eksplisitte henvisninger mellom offentlighetsloven og personopplysningsloven som tydeliggjør de viktigste sammenhengene mellom de to lovene.
- Det bør gjøres endringer i fvl § 13 første ledd for å sikre sammenheng med personopplysningsbegrepet.
- Det er også behov for å introdusere en plikt i offentlighetsloven (f.eks. i § 28) til å veilede om annen lovbestemt innsynsrett, i alle fall om annen allmenn innsynsrett, jf. pol § 18 første ledd.
- Bestemmelsen i pol § 6 vil etter vår mening få en bedre og tydeligere plassering dersom den ble flyttet til pol § 18, eller annet sted i denne lovens kapittel III. Begrunnelsen er at dagens pol § 6 ikke primært kan ses som en lovvalgsregel, men som en regel som spesielt skal konsolidere lovbestemte innsynsrettigheter, og samtidig sikre informasjon som kan legge til rette for bruk av rettighetene.
- Det kan være grunn til å gjøre unntak fra pof § 2-15 første ledd i tilknytning til utlevering av personopplysninger som ledd i realisering av lovbestemt innsynsrett.

THE DIRECTIVE ON DATA RETENTION – BETWEEN PRIVACY AND SECURITY

Stephen Kabera Karanja

Abstract

The proposed EU law on data retention has met with serious criticisms from many quarters including data protection authorities and bodies, the European Parliament, civil liberty organisations and industry groups. Eventually, the EU Directive on data retention was adopted on 15 March 2006. This article examines the Directive's compliance on data protection rules and Article 8 of European Convention on Human Rights and asks whether a balance between security and privacy requirements have been realised. At the same time, it suggests that the issue of balance is misconceived and what is required is the understanding of the symbiotic relationship between security and privacy. The question therefore is not about "balance" but "maximising" both security and privacy in order to promote life in a democratic society.

Introduction

Privacy and security are always in tension. Both concepts are nebulous. On one hand, privacy may be interpreted in different ways in different contexts. Similarly, it may be achieved by means of different mechanisms. On the other hand, security may mean different things in different contexts. It also may be achieved by different means. The legal challenge, however, has always been how to strike the balance between the two. But recently any perceived balance between the two has been put to greater tension by emerging information and communications technologies and by governments' actions in response to rising crime and terrorism.[1] The Directive on data retention has emerged under these circumstances.[2] Though the terrorist attacks of 11 September 2001, 11

1 Ipts: Institute for Prospective Technological Studies: Security and Privacy for the citizen in post-September 11 digital age: A prospective overview. European Commission Joint Research Centre, July 2003

2 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

March 2004 and 7 July 2005 have been catalytic to adoption of the mandatory retention period provision, the genesis of the retention directive below indicates the process had started long before these events. The events have, however, facilitated a shift of paradigm from "reactive" to "proactive" modes of security protection using ICT-based systems to facilitate data collection and sharing between multiple sources in support of intelligence gathering.[3]

Using the Directive on data retention as an example, I am going to examine whether the balance between privacy and security has been achieved. In particular, I will examine the Directive's compliance with data protection rules and Article 8 European Convention for Human Rights (ECHR). At the same time, I will postulate that it is not the striking of balance which is at issue here but the understanding of the symbiotic relationship between the two as dual obligations of a democratic society each to be maximized within the constraints imposed by the other. Understood this way, policy and law making will not aim at curtailing or promoting one at the expense of the other but maximizing realisation of both obligations.

Genesis and key points of the Directive on data retention

Rules on retention of data are not new. What is new is the mandatory provision. General rules for retention of data are found in Article 6 (1) (e) of the Directive 95/46/ECwhich requires that personal data are kept in a form which allows identification of the data subject for no longer than necessary for the purposes which the data are collected.[4] Article 13, however, permits general exceptions to Article 6 on matters touching national security, defence, public safety, the prevention, investigation, detection and prosecution of criminal offences etc. These rules were intended to provide a sufficient balance between the requirements of individual privacy and the needs of law enforcement and state security.[5]

3 Ibid

4 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281/31 23.11.1995.

5 D. Rowland, 'Privacy, data retention and terrorism.' 18 th BILETA Conference: *Controlling Information in the Online Environment*, April 2003 QMW, London (2003). http://www.aber.ac.uk/law/staff/bileta2003(2).pdf (Last visted on 2 May 2005).

The rules were later translated into the telecommunication sector in Directive 97/66/EC to specifically regulate processing of personal data and privacy.[6] The Directive allowed retention of personal data relating to subscribers for purposes of billing only and to the extent that is necessary for provision of services. It also ensured confidentiality of communication and thereby prohibited use of personal data retained for surveillance purposes by security services. The Directive was, however, repealed and replaced by Directive 2002/58/EC on privacy and electronic communication.[7]

This Directive extended the retention of traffic data (e.g. records of the length, origin and destination of phone calls) for national security and law enforcement purposes. This meant that the personal data could be retained once it was no longer required for billing or other essential management purposes, provided that measures taken by Member States were proportionate and necessary. But there was no retention period agreed and Member States were granted discretion on the matter.

Consequently, Member States went ahead to provide for different retention periods in their national laws.[8] Where the legislation has been enacted, it is shown to have specified for retention of traffic data for up to 12 months, although at least one Member State preferred a 3 year retention period.[9] The present Directive 2006/24/EC is meant to harmonise Member States' provisions by prescribing a mandatory retention time frame of 6 to 24 months. The issue of retention of traffic data was initially dealt with in draft Framework Decision submitted in April 2004 which is a third pillar legal instrument.[10] In

6 Directive 97/66/EC of European Parliament and the Council on the Processing of Personal data and the Protection of Privacy in the Telecommunications Sector, in Particular in Integrated Services Digital Networks (ISDN) and the Public digital Mobile Networks. (OJ No. L 24 of 30.1.1998).

7 Directive by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communication sector. OJ L 2001/37 31.07.2003.

8 At least 9 of the 15 Member States either have, or intend to enact, legislation calling for mandatory traffic data retention, and the large majority have expressed a broad support for an EU-measure calling for mandatory data retention. While authorities in a few states like Germany and Finland remain sceptical, authorities in Greece, Denmark, Austria, Spain, Belgium, and most of the rest of Europe are supportive.

9 Privacy International: Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European convention on Human Rights, 10 October 2003. Prepared by Covington & Burling for Privacy International, at 4-5.

10 Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purposes of (…) investigation, detection and prosecution of crime and criminal offences including terrorism, 8864/1/05 REV 1 LIMITE COPEN 91 TELECOM 33, Brussels, 24 May 2005.

order to avoid issues of illegality the draft Framework Decision was replaced with the current first pillar Directive.

The retention ensures that the personal data are available for the purposes of investigation, detection and prosecution of serious crime as defined by each Member State in its national law. Retained data will not be used for the prevention of crimes or for the investigation of non-serious crimes. But Member States will still be able to require data retention for other purposes not mentioned in the Directive, including prevention.

The main feature of the Directive is the provision for mandatory time frame of 6 months to 24 months for retention of personal data, a facet not found in the previous Directives.

The Directive also limits the scope of the data to be retained. It requires telephone (fixed and mobile) and internet services to retain traffic and location data (data about phone call or email),[11] only and not the contents of communication. Data related to unsuccessful call attempts must be retained only if the data is actually stored by the service provider. The data is to be made available to law enforcement authorities when required. As pointed out by the Council, the Directive does not prevent individual Member States from additionally requiring such data to be stored.

The access and use of retained data by law enforcement and public agencies is left to the discretion of Member States to determine while being guided by international obligations on the matter. Data protection authorities will be involved in the evaluation of the application of the Directive, as well as in any amendments to the list of data to be retained. The data to be retained will be processed under the existing legislation on data protection, in particular Directive 95/46/EC and 2002/58/EC.

Critique to the Directive

The Directive was adopted after a long debate concerning the balance between security and privacy. Earlier proposals had been largely criticised by

11 For call data included the registered owner of the phone, the numbers dialled, the length of a call and, in the case of mobile phones, the location of the caller. For email it includes the registered owner of the email address and the email addresses of their correspondents. Because the stored data offers historic information it allows an individual's calling patterns to be tracked over long periods of time. Regular numbers called, and an individual's network of contacts, can therefore be identified. See http://www.opendemocracy.net/xml/xhtml/articles/3556.html (Last visited on 15 May 2006).

among others; members of European Parliament, Article 29 Working Party,[12] European Data Protection Supervisor, [13] civil liberty organisations[14] and industry. [15] But were the criticisms taken into account in the adopted Directive? Not all criticisms were incorporated. Consequently, the Directive has some obvious shortcomings as regards data processing and protection rules.

The main concern, however, is whether the new Directive can achieve harmonisation as it purports. Harmonisation is highly doubtful as the rules of retention, access to data, and data limitation will permit wide divergence in Member States national laws. In addition, the costs to be borne by the service providers when complying with the directive are enormous and the issue of financial assistance to affected enterprises to offset costs of setting up data

12 The Working Party has issued two opinions on the data retention proposal and Directive. Article 29 Data Protection Working Party Opinion /2005 on the proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic communication services and amending directive 2002/58/EC (COM(2005)438 final of 21.09.2005) WP 113. And Article 29 Data Protection Working Party Opinion 3/2006 of the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. WP 119.

13 Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final. OJ 2205/C 298/01.

14 The civil liberty organisations have pointed that despite shifting to the first pillar away from the third, the policy driving the proposal for data retention has not improved. "Despite many edits over the last two years, both the Council and the Commission proposals continue to be invasive, illegal illusory and illegitimate. The case still has not been made that retention is necessary in a democratic society and the claimed need for harmonisation is premature at best and challenges democratic process." See G. Hosein, & S.Nas, 'Briefing for members of the European Parliament on data retention'. Pivacy International and European Digital Rights (2005).

15 Many industry groups were concerned that the text adopted provides very little harmonisation. They expressed grave concerns about the flexibility that will be afforded to individual Member States, saying that it will result in compliance challenges, as well as distortion in competition within the marketplace. There was also disquiet among them about costs as they foresaw divergences because individual Member States will have the freedom to determine what, if any, financial assistance they will give to affected enterprises to offset costs of setting up data retention systems. Data retention requirements in the Directive require a considerable deployment of information technology and associated security measures. The legislation must therefore ensure the use of a comprehensive database security protocol to protect personal information in the new databases. See, J. Klosek, & S. G.Charkoudian, 'New Data Retention Rules on the Horizon in Europe'. IP Alert (2006), Goodwin Procter. http://www.goodwinprocter.com/publications.asp And, December 2005. Securing Data under the proposed EU data retention draft directive. *Cyber Security Industry Alliance*. www.csialliance.org

retention systems has been left undecided. The issue of which technical standards and organisational security measures are to apply is to be decided by individual Member States. The Article 29 Working Party is concerned that this will create divergence and has called on the Member States to co-ordinate the implementation and to define minimum standards.[16]

Although the Directive provides for a mandatory 6 to 24 months data retention period, the implementing Member State will determine the retention duration and discrepancies are expected within national laws. Individual Member States, however, are free to introduce longer retention periods under special circumstances and procedures as specified by the Directive.[17] It is not clear where Member States have longer periods whether they can opt to retain them or they must comply with the mandatory period.

The Member States will also be free to determine which national authorities have access to the retained data. As has happened in other areas such as the Schengen,[18] the authorities with access in Member States will differ. Furthermore, the Directive does not contain a requirement for Member States to draw a list of law enforcement authorities designated. There is also no obligation to record and keep audit logs of retrieval of data.[19] These omissions will create uncertainty and differences.

At the same time, the term "serious crimes" is still broad and Member States may have different interpretations of what constitutes serious crimes. It is expected that the term will apply to other serious crimes other than terrorism and organised crime. As such, the practice in Member States will diverge, which is why the Directive should have limited the provision by clearly defining and delineating serious criminal offences.[20]

The Directive will have great impact on protection of personal data but it does not contain adequate common data processing and protection rules. To augment the deficiency, it makes reference to the existing legal framework on data protection (in particular, the 95/46/EC and 2002/58/EC directives), however, this is not sufficient.[21] Furthermore, the rules on deletion do not specify how the data are to be erased. For example, in the Schengen Convention, the data are erased automatically at the end of retention period. The Directive should have specified that this will also be the case. There are also no data

16 WP 119 at 3
17 Article 12, 2006/58/EC
18 S. K. Karanja, The Schengen co-operation: Consequences for the rights of EU citizens. *Mennesker og rettigheter* Årgang 18 Nr. 3 2000, 215-222, 219.
19 See, WP 119 at 3.
20 See, EDPS Opinion OJ C 298/7.
21 Article 7, 2006/58/EC.

subject access rules to enable an individual to simply and quickly exercise rights. As Article 29 WP has pointed out 'the Directive should not entail large-scale data mining based on retained data, in respect of the travel and communications patterns of people unsuspected by law enforcement authorities.'

These omissions will make harmonisation and proportional balance between security and privacy hard to achieve.

Compliance with Article 8 ECHR

The overall policy objective of the data retention Directive is to provide for a European wide harmonisation of legislation on retention of traffic data which balances in a proportionate manner the needs of law enforcement, the fundamental rights of the citizens and the interests of the electronic communications industry.[22] But has the Directive achieved the balance in a proportional manner? Using the European Court for Human Rights case law I am going to examine the issue of proportionality here.

The protection of privacy is ensured under Article 8 of the European Convention for Human Rights (ECHR). It states that 'everyone has the right to respect for private life and family life, his home and his correspondence.' Public authorities may, however, interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society namely in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others.

The Court has given the term private life a broad meaning. In the case of *Niemitz v Germany*,[23] the Court stated that respect of private life must also comprise, to certain degree, the right to establish and develop relationships with other human beings. In the case of *Z. v. Finland*,[24] the court has asserted that the protection of personal data is of fundamental importance for a person's enjoyment of his or her right to respect for privacy and family life under Article 8. The Directive on retention of data has direct consequences for the right to establish and develop relationships with other persons and the protection of personal data and as such it may come into conflict with the enjoyment of the right to respect for private life.

22 Extended Impact Assessment: Commission Staff Working Document annexed to the Proposal for Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC {COM(2005) 438 final}. p. 7

23 [1992] EHRR 193, [29]

24 [1997] 25 EHRR 371, [96]

Retention of data amounts to interference with the respect for private life as guaranteed in Article 8(1). A number of decisions by the European Court for Human Rights affirm this. In *Amann v Switzerland*,[25] the Court found Article 8 applicable when State security services kept a record indicating that the applicant was a contact of the Soviet Embassy, after intercepting a telephone call from the Embassy to the applicant. The Court held that both the creation of the record card and storing it amounted to interference with the applicant's private life and the subsequent use of the stored information has no bearing on that finding. Similarly, in *Rotaru v Romania*[26] the Court decided that both storing and use of the information by the security services of the applicant's past political activities as a university student amounted to interference with the applicant's right of respect for private life and family life protected in Article 8(1). Following the reasoning in these cases the retention of information under the retention of data Directive will constitute to interference with private life of all communication users. The information need not to be used at all, the mere retention is enough to constitute interference.

The indiscriminate data retention under the retention Directive would also amount to interference with respect for private life. In *Klass v Germany*[27] the Court was of the opinion that because a law permitting interception of mail created a "menace of surveillance" for all users of postal services, and because that menace struck at freedom of communication, the law therefore constituted interference with the right to respect of private life.[28] The indiscriminate retention of data will create a menace in larger proportions than anticipated in the *Klass* case and strikes at heart of freedom of communication. Retention of data will also generate a record of one's private activities. It offers historic information which allows an individual's calling patterns to be tracked over long periods of time. Regular numbers called, and an individual's network of contacts and associates can therefore be identified.

It does not make any difference that the data retention Directive limits data to be retained to traffic data only and does not extend to content of individual communications. The Court has on several occasions found that the recording of numbers dialled from conventional telephones constituted interference with private life (*P.G. v United Kingdom*[29], *Valenzuela Contreras v Spain*[30] *and Malone*

25 *Amann v Switzerland* Judgment of 16 February 2000 [79-80].
26 *Rotaru v Romania* App. No. 28341/95 Judgment of 4 May 2000 [44]
27 *Klass & Others v Germany* [1993] 18 EHRR 305.
28 Ibid [41]
29 No. 44787/98 judgment of 25 September 2001.
30 [1999] 28 EHRR 483.

v United Kingdom[31]). In *Malone* case, the Court in particular observed that 'the records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone.'[32]

The right of privacy granted under Article 8(1) of ECHR is not absolute and interference can be justified under conditions set out in Article 8(2). Interference is permitted if it is in accordance with the law, in furtherance of at least one of the aims listed in Article 8(2) and is necessary in a democratic society. But the Court has cautioned that this right is to be read narrowly because it provides exceptions to a right guaranteed by the Convention. In the *Klass* case above, the Court said that "powers of secret surveillance of citizens characterised as they do the "police state", are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.[33]

The requirement that interference be in accordance with the law means that not only must there be a law in place authorising the interference, but that it should meet the standard of accessibility and foreseeability inherent in the concept of rule of law. The data retention is based on the Directive which is a law but may not satisfy the standard of accessibility and foreseeability. Universal data retention provision as in the Directive, offends the standard of foreseeability as required by the Court. Foreseeability standard requires that the State should give citizens an adequate indication of the circumstances in which the public authorities are empowered to interfere in their private lives (*Kruslin v France*[34] and *Malone v United Kingdom*). The State is not allowed to ambush the citizens but they should be allowed to regulate their conduct accordingly, so as to avoid invoking unwelcome intrusions by the State. The law should offer citizens reasonable means of avoiding surveillance in their private life. The data retention Directive fails in this respect because if citizens are to avoid surveillance the only choice they have is to stop using communication services which is not practical.

The Directive is also arbitrary because it does not distinguish between different classes of people. In *Kruslin v France*, the Court held that a law authorising telephone tapping lacked the necessary foreseeability because it did not define the categories of people liable to have their telephone tapped or the nature of the offence which might justify such surveillance.[35] The court arrived to similar decision in *Amann v Switzerland* where a decree permitting the police

31 [1985] 7 EHRR 14.
32 Ibid [84]
33 *Klass* n. 27 above at [42]
34 [1990] 12 EHRR 547.
35 Ibid [35]

to carry out surveillance did not indicate the persons subject to surveillance or circumstances in which it could be ordered. The data retention Directive blanket requirement does not differentiate those under surveillance from the rest of the population. In fact it seems that the entire society is under surveillance. The definition of "serious crimes" in the Directive is not precise either, and citizens would not know which crimes are within the scope of the Directive.

The Directive also lacks foreseeability because it is certain to come into conflict with other lawful relationships such as confidential attorney-client communications. It does not make distinction between such communications and "normal" communications. In *Kopp v Switzerland*,[36] the Court observed that a law authorising interception of telephone calls would in certain circumstances contradict other provisions of Swiss law according protection to confidential attorney-client communications. The law also lacked foreseeability because it provided no guidance on how authorities should distinguish between protected and unprotected attorney-client communications.

The requirement of legitimate aims play an important role in assessing the proportionality of a restriction and balancing of interests under the 'necessary in a democratic society' principle and the two will be considered together here. Article 8(2) requires that any interference be no greater than is necessary in a democratic society. Any interference of Article 8 must therefore correspond to a pressing social need and be proportionate to the legitimate aims pursued (*Foxley v United Kingdom*[37]). By targeting the entire society, the data retention scope goes beyond what is necessary and is not proportionate to the legitimate aims pursued. Although the aims of investigation, detection and prosecution of serious crime are legitimate, the failure to distinguish between classes of offenders and non-offenders renders the legitimate aims illegitimate. The retention is not therefore proportionate to the legitimate aims.

The Court also requires that a measure restricting individual rights to be proportional. The proportionality principle tends to place the burden of proof on the government to show that the measure or decision undertaken is not disproportional to the legitimate aims. That is, the State must put in place adequate safeguards to ensure that the interference with the rights is no greater than is necessary. The proportionality requirement enables the Court to supervise the discretion granted the State. In *Foxley v United Kingdom* the Court found that interception of a bankrupt's mail violated Article 8 because the absence of adequate and effective safeguards ensuring minimum impairment

36 [1998] 27 EHRR 91 [73-75]
37 [2000] 31 EHRR 637, [43]

of the right to respect for his correspondence.[38] The Directive does not contain adequate data processing and protection rules and no mechanism to ensure that no large-scale data mining based on retained data in respect of the travel and communication patterns of people unsuspected by law enforcement.

Proportionality also entails the issue of availability of a less restrictive alternative. Where a less restrictive alternative is present, the State should choose that one and not the most restrictive. Metaphorically speaking, a man should not use a club to kill a mosquito. The Court examines whether other less restrictive measures existed and have been used to achieve the same purpose (*Z. v Finalnd*). The Article 29 Working Party and the EDPS were not convinced that the case for data retention as required by the Directive had been clearly demonstrated. It was also not clearly demonstrated that the existing data protection laws were inadequate to deal with the threat bearing in mind that, experience in the United Kingdom on requirements of data by law enforcement were mainly for data less than 6 months old and in exceptional cases up to 12 months old. Furthermore, Member States can request preservation of data for longer time if necessary. The extension of mandatory retention period to 24 months was therefore not supported by the available evidence.

The trend internationally also went contrary to the mandatory retention periods. In the US, preservation approach is followed. Public safety officials rely on providers to preserve data and other records quickly upon notification that such information is necessary for a specific investigation, before such information is altered or deleted.[39] The situation in the US, however, may change as there are now calls for mandatory retention period law.[40] Preservation does not require a service provider to collect data for proactive investigation and detection. The Council of Europe Cyber Crime Convention[41] contains a similar preservation scheme, reflecting general agreement for now, this preservation regime strikes the proper balance between competing policy interests.

38 Ibid [43]

39 The G-8 has defined data preservation as when, a) upon lawful request by a competent authority, b) based on the facts of a specific case, c) specific historical data can be preserved to prevent its deletion, d) pending issuance of a lawful demand from a competent authority. Data preservation according to this definition does not include the prospective collection of data and does not obligate a service provider to generate data that it does not routinely require for lawful business practice.

40 The failure of some Internet service providers to retain user logs for a 'reasonable amount of time' is hampering investigations into gruesome online sex crimes, US Attorney General Alberto Gonzales said indicating that new retention rules may be on the way. http://news.zdnet.com/2100-9595_22-6063185.html (Last visited on 1 June 2006).

41 Council of Europe Convention on Cybercrime – ETS No. 185 Budapest, 23.XI.2001.

These examples demonstrate that mandatory retention was not the only way to ensure that the law enforcement have the necessary data for the purpose of investigation and detection of crime. Less alternative measures exist and are working.

The data retention Directive fails to meet some important requirements of legality and proportionality set out by the European Court for Human Rights in its case law. As such, the Directive and the laws adopted by Member States pursuant to the Directive cannot provide a proportionate balance between the demands of law enforcements and privacy requirements of EU citizens. Perhaps a new understanding of the relationship between privacy and security is necessary.

Maximizing Privacy and Security

The tension between privacy and security is not new. The complexity of the two concepts, however, has not made the discourse any easier. Both concepts are vague and society does not always agree on their meanings. At the same time, the demands of privacy and security always seem to be at variance. On one hand, we would like privacy and to be left alone to pursue our lives as we wish. On the other hand, demands for security and a safe society means that prying on our lives cannot be avoided. The issue has, therefore, been to what extent one can be left alone and what level of interference is permitted. It is also an issue of how to go about determining the balance.

In an attempt to answer the question, various concepts have been used to articulate the tension between privacy and security. At times the problem is postulated as need for "balance", that is finding a balance between the two. But I think the balance concept presents some problems because it is difficult to know where to draw the balance. 'An initial difficulty is that balancing presumes that goods ostensibly placed in the scale are amenable to being weighed against one another.'[42] 'Just as justice is not a weighable concern in legal system, neither is security.'[43] Balance can go either way, as it often does, with intractable consequences to one interest or the other. Balance can mean adding to one or subtracting from the other, improving or curtailing one. But as

42 L.Zender, 'Securing liberty in the face of terror: Reflections from criminal justice. *Journal of Law and Society*', volume 32, Number 4, December 2005 ISSN: 0263-323X, 507-533, 516.

43 O. Lepsius, 'Liberty security, and terrorism: The legal position in Germany'. *German Law Journal*, 01 May 2004 435-460, 460.

Olive Lepsius has demonstrated, 'the balancing process has become one-sided. Security concerns tend to override civil liberties.'[44]

The terminology "trade-off" has also been invoked meaning that there is need to trade-off one for the other. This entails some difficulties also because it implies one interest is of lesser importance than the other. One can be sacrificed for the sake of the other. As Lucia Zender has argued 'although the trade-off between the larger interests of the aggregate us versus the individual them is rarely made explicit, the weight of numbers hangs implicitly in the balance to tip it in our favour.'[45] After a serious security threats, such as the terrorist bombings in US, Spain and United Kingdom, we witness comments such as 'we are ready to sacrifice some of our freedoms for the sake of security'. In the circumstances, privacy is often the loser.

Further, the relationship between privacy and security has been portrayed as "competing interests" meaning that the two are always fighting for supremacy and one has to give way for the other. 'Claims to rebalance in the "public interest" or "national interest" are laid down as trump cards against which any individual claim to liberty cannot compete.'[46]

At other times, privacy is expressed as an "individual right" while security is viewed as a "collective interest". Collective interests are usually accorded greater value than individual rights when the two are in conflict. Presented this way, privacy tends to always lose to security.

I think the conflict between privacy and security is worsened by the way their relationship has been postulated over time. There is need to rethink and develop new concepts to articulate the relationship between the two positively. As I see it, the relationship between privacy and security is symbiotic. That is, although the two are different, they have a close beneficial relationship, in the sense that you cannot have one without the other. Both security and privacy are important and fundamental concepts both for individuals and collectively for society but neither are amenable to quantification.[47] A democratic society needs both privacy and security. Security is needed in order for the society to protect itself from individuals and groups that might harm it through crime, fraud, terrorism, and serious irresponsible behaviour. Privacy also is needed for individuals and society to be protected from an overprotective, domineering, controlling, invasive society.[48]

---

44 Ibid 459.
45 L. Zender, n. 37 above , 513.
46 Ibid 513.
47 D. Rowland, n. 5 above.
48 G. G. Scott, Mind your own business: The battle for personal privacy. (New York: Insight Books Plenum Press, 1995).

The question is how can the two values be realised at the same time? Perhaps, a better concept to employ would be "maximizing" which means increasing as much as possible. That is increasing security as much as is required and similarly increasing privacy as much as is needed. Ben Hayes has observed that there is no "balance" between security and civil liberties – just less of each other.[49] He wondered how can there be a "trade-off" between (collective) liberties and (collective) security if both are in decline. He concludes that 'defence of civil liberties and democracy requires that positive demands are placed on the agenda.'[50] The trend is that communication technologies will continue to advance and demands for security and law enforcements will also increase. In such circumstances, the best responses are also to increase the demands for privacy and not to erode it. As such, a democratic society has a dual obligation to maximize security and privacy within the constraints imposed by the other in order to protect and promote life in the society.

The data retention Directive is an example of how the EU institutions have failed to maximize both security and privacy. Despite, numerous suggestions from data protection authorities and experts, civil liberty organisations and industry, pointing the need to maximize both values, the EU institutions did not deal with the challenge adequately. The end result as the analysis of proportionality above indicates is that security was given priority over privacy. Proportionality was sacrificed.

The approach used by the Court supports the "maximizing" thesis. The enquiry of the Court aims at finding a proportionate balance, not by destroying one value and building the other but by maximizing both values. The requirement for adequate safeguards is the main building block for a solid balance and the Court is not satisfied unless the presence of adequate safeguards is demonstrated. Perhaps, if legislators and policy makers adopted a "maximizing" view on security and privacy the existing tension between the two could be reduced.

Conclusion

The tension between privacy and security has never been greater. Technological advancement and demands of law enforcement continue to extend the coexistence of privacy and security to the limits. The Directive on data retention has

49 Hayes, B.. There is no "balance" between security and civil liberties – just less of each. In *Essays for civil liberties and democracy in Europe* .(ECLN Essays no. 12. 2005) www.ecln.org (Last visited on 26 May 2006).

50 Ibid at 6.

shown how difficult it is to strike a proportionate balance between the two. Perhaps it is time to rethink and redefine the relationship between privacy and security in positive terms. By understanding the symbiotic nature of privacy and security, it is possible to maximize the two values instead of pitting them against each other.

USER INVOLVEMENT IN E-GOVERNMENT SYSTEM DEVELOPMENT PROJECTS: WHAT CAN BE LEARNED FROM THE PAST?

Arild Jansen

Abstract

The aim of this paper is to take part in the discussions on how the Scandinavian IS research tradition in information system research may contribute to eGovernment developments and implementations. Although this tradition does not represent a coherent set of principles and methods for system development, they share some common ideas and goals related to user involvement, participatory design and democracy at the work place. Even if some of the most basic ideas are inherent in our understanding of the IS field to day, many of the lessons from the past may have been forgotten. Some do also claim that the dominant understanding of eGovernment nicely conforms to the perspectives and goals of the New Public Management paradigm. I will rather argue that advanced development and use of ICT can support the ideals and goals of the Scandinavian approaches to IS; we should not least have a greater focus on studying the consequences of various approaches to system design, implementation and use.

Key words

eGovernment development, Scandinavian information system development tradition, participatory design, user involvement

Introduction

Scandinavian research projects in system development have traditionally put a strong emphasis on user participation and support for different interests as a strategy for increased work life democracy, and also for the society at large. However, as important goals are to develop well-functioning, user-friendly and high-quality system. The basic assumption is that one only can achieve long-term benefits by combining these different goals and by managing the

clashes of interests and contradictions that necessary will appear in system development projects.

However, what impact has this tradition had on the development and implementation of information systems in public sector? Or has the influence of the New Public Management paradigm been dominating, in its focus on market orientation, service provision to customers and high performance through competition?

This paper will not be able to fully answer these questions, but may stimulate to a debate on how the knowledge and experiences gained in the past Scandinavian IS research effort can contribute to progress in this new field.

The structure of the paper is as follows. Chapter 2 summarizes the basic ideas of the Scandinavian school(s) of IS research. Chapter 3 visits the debate on the relation between eGovernment and New Public Management, followed by a discussion of the role that Scandinavian IS approaches may have in the eGovernment era.

Scandinavian traditions in system development research

System developments has, from the outset been an expert-dominated and top-down oriented activity from problem description to implementation, use and maintenance, frequently referred to as "phase-driven" or the "Waterfall" development method. This approach is characterized by system-theoretical thinking, often based a functional analysis of the system to be modeled and designed and implemented. However, it became early clear that this approach had a number of weaknesses.

The Scandinavian tradition in information system research has its roots the early action-oriented research projects and efforts in late 60thies and 70thies. Important inspirations came from the socio-technical research by the Norwegian Industrial Democracy project that started in 1960 as cooperation between the Norwegian Federation of Trade Unions (LO) and the Employers organization (NAF, later renamed NHO). But first of all this tradition is linked to the NJMF-project (Norwegian Iron and Metal Workers), in cooperation with Kristen Nygaard and Olav Terje Bergo (Nygaard og Bergo 1974), followed by the Swedish Demos-project and the Due-project in Denmark (se e.g. Ehn og Sandberg 1979, Bansler 1987, 1989, Bjerknes, Ehn og Kyng 1987), Bjerknes, Dahlbom et al 1990, Iivari 1991, Bjerknes and Bratteteig 1995). Although these projects had partly different goals and perspectives, they can be characterized as action research, having a socio-technical orientation and strong user- involvement in all phases, and aiming at democratization at the workplace.

These and other projects were the inspiration and empirical background for the textbook "*Professional System development"* by Andersen et al (1986), in which they emphasizes the relation between development work and management, between process and product and between planning and evaluation, and the need for communication at all levels in the system development processes.

Another important and very interesting contribution is textbook "*Computer and controversy. The philosophy and Practice of Systems Design*[1], written by Bo Dahlbom and Lars Mathiassen, in which they reflect over the profession of system development and its essential ideas, and not least, discuss some of the fundamental contradictions that is inherent in the practical work. Starting out by addressing our understanding of systems, information and the use of computers as tool for problem solving, and by drawing on various philosophers, they spell out three different frameworks for system development work in distinguishing between *hard, soft, and dialectica*l system thinking. Following from that, they outlined three corresponding paradigms for system development. The first one, *construction,* suggests a rational and analytical strategy, while the *evolution* approach focuses on uncertainty and suggests an experimental strategy for problem solving. In the third approach, *intervention* the problem is no longer given, and development cannot be seen as some thing isolated from the life of the organization, and accordingly, system development must be seen as an integral part of organizational change. Furthermore and perhaps the most pioneering, they discuss the many dimensions of quality of technical artifacts, as e.g. functional, aesthetic and symbolic quality, and points to the power, politics and ethics in defining quality.

eGovernment – more than the emperor's new clothing?

Computers have been applied for administrative applications for quite a while and even in Norway, computers were used for governmental tasks already in 1957. During the next decades to come, computers and later on ICT including Internet have being used in a large range of tasks; thought the concept of EGovernment was not used until Internet was in use. EGovernment is today becoming a global phenomenon that is consuming the attention of politicians, policy makers as well as ordinary citizens.

There exits a number of different definitions of eGovernment in the literature. Some are rather narrow, focusing on using ICT, particularly the Internet,

1 In the preface to this book, the Scandinavian IS tradition is not explicitly mentioned, but many of the ideas are inherent in this tradition. The authors have been an integral part of this Scandinavian IS community for many years.

as e.g. "the use of technology to enhance the access to and delivery of government services to citizens, business partners and employees", (Deloitte Research 2000, p4.) Others view eGovernment more broadly as efforts to transform government. Such examples can be:

> *"The use by the government of Web-based Internet applications and other ICTs, combined with processes that implement these technologies, to a) enhance the access to and delivery of government information and services to the public, other agencies, and to government entities; or b) bring about improvements in government to operations that may include effectiveness, efficiencies, service quality, or transformation"*
>
> US government 2002

EGovernment is thus far more than a technological phenomenon. It is transformative in nature, affecting the management of human, technological, and organizational resources processes. Consequently, the implementation of eGovernment systems will be monumental change effort, which clearly shows that eGovernment to day is qualitatively different from the more isolated ICT-system in the past.

EGovernment and New public Management – a perfect marriage?

The above definitions emphasize eGovernment as a transformational endeavor and that it is an international phenomenon which not at least a number of consultant companies world wide are heavily involved in. This has inspired some commentators to ask if there is a close a link between eGovernment and the New Public Management paradigm (NMP). New Public Management is a management philosophy used by Governments since the 1980's to modernize their Public Sector (Wikipedia 2005). Based on public choice and managerial schools of thought, new public management seeks to enhance the efficiency of the public sector and the control the government has over it. The main hypothesis in the NPM-reform is that more marked and active management in the public sector will lead to more cost-efficiency for governments, without having negative side effects on other objectives and considerations.

NPM can among others be characterized by: i) a customer rather than citizen orientation focusing on high quality services that serve narrow interest of the citizens, ii) performance orientation, iii) lean and highly decentralized structures, iv) emphasis on accountability upwards, v)use of divisional structures breaking down former unitary bureaucracies (Bruening 2001). He claims that this type of reform has a techno-optimistic, analytic flavor and seems to

reinforce the effects NPM is having on the organizations throughout the industrialized world.

Homburg (2005) points to that about a decade ago, a new kind of rationalization or reform was introduced in public sector by the use of modern ICTs (especially Internet technologies). Initially, it was focused on improving and reengineering internal processes, but later it also included the redesign of external relationships in order to improve public administration's accessibility and quality of service provision. He analyses two different sets of trajectories: one based on an external perspective; on the relationship between government and citizens, and another with an internal focus, referring to the changes that could occur within and between bureaucratic organizations.

However, the ways such principles are implemented show great heterogeneity, and Homburg discusses 4 different patters: i) markets government, ii) participatory government, iii) flexible government (e.g. virtual organizations) and iv) deregulated government. He thus claims that "underlying to all patterns of practices, is a notion of departure from the classic public administration paradigm. Especially the notion of decentralization conflicts with public management of strict hierarchy and rules, and centralization by integration. Furthermore, the basic mechanism of the (hierarchical) accountability route is complemented with a product-oriented (opposed to process-oriented) accountability structure, which tries to capture citizens' perception of quality of public services" (ibid, p 549). However, he continues, the means used to achieve this may vary from different contact with citizens, market mechanisms and more organic relationships.

His analysis seems to indicate that eGovernment services in practice, in its focus on transformation of the public sector, mark a deviation from the classical public administration paradigm. However, it shows no unambiguous relationship or marriage between eGovernment and a specific form of public management, rather that there are many different scenarios or trajectories. This is also what is found in other studies; that the use of ICT may affect public management in many ways (e.g. George and King 1991).

EGovernment and the Scandinavian tradition: is there any relation?

It thus seems to be evidence for claiming that EGovernment is far more than realizing NPM. If we look at the work on eGovernment in the EU Commission, they focus on these overall objectives for eEurope (Com 2003):

- A public sector as e.g. open and transparent, that is understandable and accountable to the citizens, open to democratic involvement and scrutiny.

- A public sector that is at the service of all, being inclusive and exclude no one from its services
- A productive public sector that delivers maximum value for taxpayers money

These goals may, at a general level conform to the ideas and thinking of Scandinavian IS traditions. However, that is not to say that all eGovernment solutions have consequences we may support from a work life democracy perspective. There are powerful pressure groups, not least from the consulting industry that are pushing strongly for implementing their solutions in rather standardized ways, similar to what we see in the private sector. The strong emphasis on evaluations, benchmarking and ranking (e.g. Com 2003, Capgemini 2005 etc) does not necessarily encourage user involvement and participatory design. The question is then: what role can the Scandinavian IS approaches have in such processes?

Greenbaum (1995) summarizes the main motivations for conducting participatory design as *pragmatic* (improving system design), *theoretical* (e.g. for communication benefits of the involved parties) and *political* (e.g. further workplace democracy). On a more concrete level, these reasons for stronger user involvement are normally given as: i) improving the knowledge upon which systems are build, ii)allowing for experimenting and learning before the solutions are finally implemented and put into use, iii) enabling people to develop realistic expectations and reducing resistance to change, and iv) increasing workplace democracy by giving the member of an organization the right to participate in decisions that are likely to affect their work

However, the way IS systems are being developed and used have been changed during the last 15-20 years, and many will maintain that the above arguments are no longer valid, e.g. because modern system development methods are different from those used in the past, in providing various opportunities for involvement. Internet and Web-based systems tools have changed the way systems are developed. Furthermore, we have a much more knowledgeable and skilled work force related to IT than in the past. There has been a move from internal systems aiming at rationalization to external (customer-oriented) systems aiming at improving the quality of public services, which implies the users to a large extent are not as employees, but as citizens. One can also argue that new legislation, such as the Working environment act in Norway provide means for involvement and participation at various levels.

On the contrary, it can also be argued that greater involvement and participation in all phases of development and deployment are even more necessary now, e.g. because:

- We see greater changes in organization than before; the traditional organizational patterns are being challenged in that the borders between private and public sector is continuously being challenged.
- What differs from the past is the change of focus from stand-alone system to large-scale integration of various systems and restructuring, and a shift from focus on the users to consumers and citizens. Systems are getting more and more complex through closer interaction and integration, as basis for radical restructuring of the public sector at large
- There is an increasingly tendency to outsourcing and globalization. We thus see new types of conflicts and contradictions, which best can be handled through participation on various levels.
- The different threats related to digital divide calls for professionals that can support the various groups of citizens that do not have a strong voice on their own

I am not arguing that we should return to the ideology-driven debates and actions of the "good old days". But we should critically assess the experiences from the past and use them as inspiration and knowledge base for new thinking and initiatives.

User participation, where and how

User participation is not a panacea in the context of eGovernment. It is not obvious how and where participation best may take place. Marginalization and cultural bias are favoring dominant groups in access and decisions were the important topics in the participatory design activities. And who are the real users? This simple framework may illustrate that there are many different constellation and stakeholders when new ICT-solution are to be implemented:

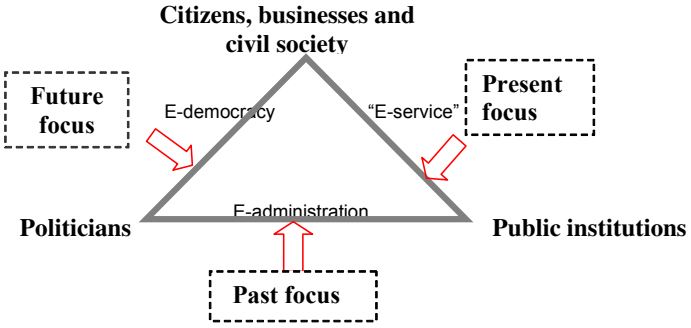


Figure 1: A framework for eGovernment

The above figure aims at illustrating that while one in the pioneering period mostly worked along the horizontal line, and the users were mostly the employees, the focus to day are most related to service provision, and the users are outside the organization (primarily as customers). We are now gradually seeing more efforts toward the "e-democracy" dimension, though mostly as small scale experiments, involving various groups of citizens. It is rather obvious that this wide range of projects types require quite different system development strategies, depending on the goals and perspectives. Thus, in the individual projects, we will have to organize projects such that all involved parties will have their voice heard.

Følstad, Jørgensen et al (2005) have studied user involvement in eGovernment development projects in Norway. They found that there seems to be a broad agreement on the importance of user involvement, at least among the project leaders. However, actual user involvement is often conducted according to the participant practice of the industrial democracy, emphasizing formal procedures rather than the processes and methods advocated within the traditions of HCI. The most frequently deployed user involvement is user representation in project teams, rather than e.g. usability tests and user group analysis. One conclusion from the study is that there seem to be an explicit need of more structured processes for user involvement activities for eGovernment projects.

Oostveen and van den Besselaar (2005) discusses different methods for engaging users in systems design, and ask: To what extent can we use lessons and methods from participatory design, as e.g. being active in the specification and design process, to include a variety of political views and social interests in the social-technical shaping of future trajectories of large-scale of large-scale eGovernment systems. They claim, based on experiences from to large projects, that such traditional methods does not apply for various reasons: i) the models and methods are based on small scale projects, ii) the number and variation of user groups are quite different, and iii) it involves not (only) users as citizens and civil servants, but also politicians on various levels. Their conclusion is that a combination of methods from technology assessment approaches with participatory design practice can be successful, but is not yet practiced enough.

Different levels of participation

Bjerknes and Bratteteig (1995) point to that there are many different arenas of participation and democracy, and they describe these four:

1. The *work situation* level, in which the use of technology depends on the nature of work tasks, and the ICT systems are viewed basically as *concrete tools*. It is possible to influence through participation in the individual development projects, which used to be the traditional type of involvement.
2. The *workplace or organization* level, which depends on how different activities are coordinated and integrated in the organization. Focus is not only on individual systems, but their interlinkage and integration, where the information (technology) architecture and infrastructure are designed, including choices of standards and type of software. Important issues will be the degree of (de)centralization (as e.g. in the national wide systems in public sectors as Tax administration, National Health Insurance offices, etc.) To ensure the employees influence on their work organization, it is necessary to address the whole organization.
3. The *interorganisational level,* in which the focus is on the relation between an organization and its environment, as e.g. the external users (customers), cooperating agencies, private businesses. Important issues are how to design technical and organizational infrastructure, and how changes in the environment can and will affect the internal structure of the organization. In Norway, such examples are cross-sect oral ICT initiatives as common solutions for businesses, collaborative use of registers, (including a common Meta database), the reorganization of National Insurance Administration, Directorate of Labour and social welfare into one unit, the PKI (public Key Infrastructure) initiatives, etc. At this level, user involvement and participation are complicated issues, involving many stakeholders and interests.

Are other strategies more adequate?

Should we choose a political or an ethical road to democracy?

The ACM (Association for Computer Machinery) has its Code of Ethics and Professional Conduct[2], in which a commitment to ethical professional conduct is expected of every member. E.g. § 2.5 reads: "Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks". Another approach is chosen by the North America[3] based organization Computer Professional for Social Responsibility, which

2 ACM home page: http://www.acm.org/constitution/code.html
3 CPSR do also have chapter outside US, e.g. in Europe, see http://www.cpsr.org/

through individual participating members have been able to provide substantial contribution to important areas within the field. Is this the way to go?

Bjerknes and Bratteteig (op. cit.) expressed in their article a concern about a shift in locus from being seen as the realm of systems design as such to a notion of responsibility testing on individual ethics. They see the danger that user participation in system development activities is a mean or the only means. They argue that the political dimension should be reintroduced. The change of power structures in society during the last decades is an important challenge for system developments research that cannot be dealt without discussing the political dimension, on various levels.

Eevi Beck (2001), in her provocative article in SJIS *P for political* claim that "in a world made global by ICT, political concerns remain on the minds of many, PD (participatory design) must encompass work motivated political conscience which is expressed through of approaches and conducted at multiple points throughout the processes of computer development and adoption, not only participatory design". She calls for a community of professionals that develops a stronger demand for analysis of societal and ethical consequences of ICT developments, adoption and use.

Conclusions – a value-laden research agenda is still needed

My intention with this paper has been to take part in a discussion on how the Scandinavian tradition in information system research may contribute to eGovernment developments and implementations. It is not argued that the Scandinavian IS tradition represents a coherent set of principle and methods for system development, but that it shares some common ideas and goals related to socio-technical thinking, user involvement and democracy at the work place. Without aiming at raising the whole debate of the emancipator dimension of user involvement or digital divide in general, I will argue for a greater focus on studying the consequences of various approaches to system design, implementations and use. We accordingly need to study how user involvement is practiced in various types of eGovernment projects and what impact different approaches have had.

I believe that specific challenges are related to outsourcing strategies, where top-down, specification-driven projects are dominating. Referring to Dahlbom and Mathiassen (1993), I will maintain that we also need experimental and evolutionary approaches, allowing for "failures" without dramatic consequences. Not least, we need a better understanding of the problems associated with defining quality as an objective and measurable entity, as well as the efforts it takes to change the culture in an organization.

References

Andersen, N.E. et al (1986) *Professionel systemutvikling* Teknisk forlag, a.s. København.

Bansler, J. (1987) Systemutvikling. Teori og historie i et skandinavisk perspektiv. Studentlitteratur, Lund.

Bansler, J. (1989) *System Development Research in Scandinavia. Three Theoretical Schools*. I New Technology, Work and Employment Vol 4, NO 2, 1989.

Bjerknes, G. og T. Bratteteig (1995) *User Participation and Democracy: A Discussion of Scandinavian Research on System Development*. I Scandinavian Journal of Information System, Vol 7(1),

Bjerknes, G., B. Dalhlbom et al., red. (1990) *Organisational Competence in System development* . Studentlitteratur, Lund.

Bjerknes, G., P. Ehn, M. Kyng red. (1987) *Computers and Democracy.* Aldershot, England Avebury.

Boehm, B. (1976) *Software Engineering*. IEEE Transactions on Computers, Vol. C-25 (12), Dec. 1976.

Boehm, B. (1988) A Spiral Model for Software Development and Enhancement. IEEE Computer. May 1988.

Borland, R.J. and R.J.Hirschheim (1987) *Critical Issues in Information Research* John Wiley & Sons

Broening, G. (2001) *Origin and theoretical basis of New Public Management*. International Public Management Journal 2001 4(1): p 1-25

Capgemini (2005) *Online Availability of public services: How is Europe Progressing?* European Commission DG Information Society, Bruxelles.

Checkland, P. (1981) Systems Thinking, Systems Practice. Chichester. New York Basic Books

Ciborra, C. eds. (1996) *Groupware and Teamwork*. Chichester, UK: John Wiley.

COM (2003) *The Role of eGovernment for Europe's Future*. Communication from the Commission to the Council, COM (2003) 567 Final. Brussels 26.9.2003

Dahlbom, B. and L. Mathiassen (1993) *Computers in Context*. Basil Blackwell

Ehn, P. og Å. Sandberg (1979) Føretaksstyrning og Løntagermakt. Prisma, Falkøping.

Emery, M (1993) *Participative Design for Participative Democracy*. Centre for Continuing Education, Australian National University.

George, J & J.King (1991) *Examining the Computing and centralization debate*. CACM, vol.34(7), July 91.

Greenbaum, J. (1995) *Windows at the workplace*. Monthly ReviewPress, N.Y.

Greenbaum, J., & M- Kyng, eds. (1991) Design at Work . Hillsdale, N.J. Lawrence Erlbaum Ass

Grønlund, Å og A. Ranerup eds (2001) Elektronisk förvaltning, elektronisk demokrati. Studentlitteratur, Lund.

Grønlund, Å. Eds. (2002) *Electronic Government: Design Visions and Management*. Idea Group Publishing. 2002

Grudin, J. (1988) Why CSCW fails: Problems in the design and evaluation of organisational interfaces: *Proceeedings of the CSCW'88* Conference on Computer Supported Cooperative Work, 85-93. New York. ACM

Gustavsen, B. (1992) Dialogue and Development. Arbeidslivscetrum &Van Gorcum. Assen/Matricht

Hirschheim, R., & Klein. H-K. (1989*) Four Paradigms of Information Systems Developments*. Communications of ACM 32, no 10, 1199-1216

Heeks, R. (1999) *Reinventing government in the information age*. London and New York Routledge,p 9-12.

Holbeck Hansen, E. , Håndlykkel and Nygaard (1976). System Description and the Delta Language . Norsk regnesentral, Oslo

Homburg, V.(2005) E-government and NPM: A perfect Marriage?. **Proceedings of the 6th international conference on Electronic commerce.** Pages: 547 – 555, Year of Publication: 2004, ISBN:1-58113-930-6 In **ACM Int. Conference Proceeding Series; Vol. 60** archive, http://portal.acm.org/citation.cfm?id=1052289

Iivari, J. (1991) A paradigmatic analysis of contemporary schools of IS development. I *European Journal of Information Systems* Vol 1, No 4, pp249-272

Mathiassen, L. (1982) Systemutvikling og Systemutviklingsmetode. DIAMI PB 136, Mat. Inst. Århus.

Mumford, E. (1975) Industrial Democracy and Systems design. I Mumford og Sackman (1975) *Human Choice and Computers* . North Holland

Mumford, E. (1983*) Designing Human Systems*. Manchester Business School, Manchester ,England

Nurminen, M. (1987). Different Perspectives. What are they and How can they be used. Dockerty et al. (red.1987) Systems design for Human Development and Productivity. IFIP 1987, North Holland.

Parnas, D.L. og Clements, P.C. (1985) A Rational Design Process: How and Why to Fake It. I H Ehrig et al. (red. 1985) Formal Methods and Software development Springer-Verlag.

Nilsson A. & A. Ranerup (2001) Improvisatorisk førendringsarbete – nye arbeidsett med gruppeprogramvara In Grønlund og Randerup (red): Elektronisk förvaltning og elektronisk demokrati, 2001. Studentlitteratur, Lund.

Schuler, D. and A. Namioka (red.) *Participatory Design. Principles and Practices* Lawrence Erbaum Ass. Publ. New Jersey. 1993

Thorsrud, E. og F. Emery (1970) *Mot en ny bedriftsorganisasjon*. Universitetsforlaget, Oslo

US government (2002) *The e-government act of 2002*. HR 2458. http://csrc.nist.gov/policies/HR2458-final.pdf

Wikipedia (2005) http://en.wikipedia.org/wiki/Public_Sector

LOVGIVNINGSPROSESSEN BAK REGISTRERINGSPLIKT FOR KONTANTKORT TIL MOBILTELEFON[1]

Thomas Olsen

Innledning

Lov om elektronisk kommunikasjon (ekomloven, 2003:83) og forskrift om elektronisk kommunikasjon og elektronisk kommunikasjonstjeneste (ekomforskriften, 2004:401) pålegger tilbydere av offentlige telefontjenester å registrere alle sluttbrukere på en måte som muliggjør entydig identifisering. Loven og forskriften avløser lov om telekommunikasjon (teleloven, 1995:39) og forskrift om offentlig telenett og offentlig teletjeneste (offentlignettforskriften, 1997:1259) og utgjør nå det sentrale regelverket for elektronisk kommunikasjon. Mens det lenge har vært klart at tilbydere av teletjenester har hatt plikt til å registrere abonnementskunder av fast- og mobiltelefoni, har den rettslige situasjonen og praktiseringen knyttet til registreringen av kontantkortkunder vært mer usikker og sprikende. Ekomloven og ekomforskriften gjør det nå klart at registreringsplikten også gjelder kontantkortkunder.

Denne artikkelen ser nærmere på lovprosessen og begrunnelsen for innføringen av registreringsplikt for sluttbrukere av telefontjenester i Norge. Foranledningen for artikkelen er at jeg høsten 2005 rapporterte om bakgrunnen for den rettslige reguleringen av kontantkort i Norge til en sammenliknende undersøkelse i OECD-landene. Undersøkelsen, som vil bli kort skissert under, viser at OECD-landene har svært ulik tilnærming til spørsmålet, og kun et fåtall av landene har gått til det skritt å pålegge registreringsplikt. Når det gjelder situasjonen i Norge, kunne man forvente å finne prinsipielle drøftelser om adgangen til å benytte uregistrerte og anonyme teletjenester i forarbeidene til ekomloven. Det er ikke tilfelle. Gjennomgangen av lovgivningsprosessen bak ekomloven og ekomforskriften viser at spørsmålet ikke ble tydeliggjort i

1 Artikkelen er tidligere publisert i Lov&Data nr. 85, mars 2006, s. 1-6. Artikkelen er her oppdatert i forhold til vedtagelsen av datalagringsdirektivet 15. mars 2006. (Directive 2006/21/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC).

høringsforslagene til lov og forskrift, slik at det derfor ikke ble anledning for høringsinstansene til å kommentere spørsmålet.

Registreringsplikt av kontantkort reiser prinsipielle spørsmål om adgangen til å kommunisere anonymt i samfunnet. Det er velkjent at bruk av mobiltelefon etterlater såkalte elektroniske spor etter blant annet lokasjon og omgangskrets[2]. Likevel er det grunn til å tro at mobiltelefonen fremdeles er i sin spede barndom, og at transaksjonsopplysninger fra mobiltelefon på sikt vil kunne gi et svært detaljert bilde av vårt bevegelsesmønster, hvem vi kommuniserer med og våre forbruksvaner. Konvergerende teknologier (Internett og telefoni) og nye anvendelsesområder for mobiltelefonen (f.eks. betalingsløsninger), gjør at det er viktig å legge til rette for hensiktsmessig grad av identifisering overfor dem man kommuniserer med.

Spørsmålet om identifisering og registrering har også forbindelse med andre former for kommunikasjon. Er det for eksempel ønskelig og gjennomførbart å kreve identifisering og registrering for bruk av internettkafeer eller for å benytte ulike former for IP-telefoni? Tilsvarende spørsmål tvinger seg også frem i forbindelse med samferdsel - i hvilken grad skal det være adgang til anonym ferdsel på veiene ved passering av fotobokser og bompengeringer?

Et annet spørsmål som har fått betydelig mer oppmerksomhet i lovgivningsprosessen, er adgangen (og eventuelt plikten) tilbydere har til å lagre opplysninger om bruk av teletjenester (trafikkdata). Dette spørsmålet må sees i lys av parallelle prosesser som Politimetodeutvalgets arbeid[3] og forslag til nytt EU-direktiv om lagring av tele- og internettopplysinger i kriminalitetsbekjempelsesøyemed. EUs datalagringsdirektiv[4] ble vedtatt 15. mars 2006 til tross for sterk motstand fra personvernmyndigheter og rettighetsorganisasjoner. En interdepartemental arbeidsgruppe ble nedsatt kort tid etter for å utrede de nasjonale mulighetene som direktivet gir. I korte trekk pålegger direktivet tilbydere av nettverk og tjenester for elektronisk kommunikasjon å lagre transaksjonsopplysninger i minimum seks måneder, maksimum to år. Direktivet går dessuten langt i å kreve identifisering og registrering av sluttbrukere.

Selv om det er nær sammenheng mellom identifiserings- og registreringsplikt for abonnenter og lagring av abonnenters trafikkdata, er det etter min mening viktig å holde disse to spørsmålene fra hverandre. Ved å se nærmere

2 Se f.eks. Teknologirådet: "*Elektroniske spor og personvern*", 2005, og Norsk Regnesentral: "*Elektroniske spor*", 2005.

3 Se NOU 2004:6 "Mellom effektivitet og personvern – politimetoder i forebyggende øyemed".

4 Directive 2006/21/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

på lovgivningsprosessen bak ekomloven og -forskriften kan man få mistanke om at spørsmålet om registreringsplikt nærmest er tatt for gitt, og at det ble forutsatt at det skulle være adgang for politiet til å innhente allerede lagrede transaksjonsopplysninger. Dette er uheldig. Etter min mening er en identifiserings- og registreringsplikt ikke en forutsetning for lagring av transaksjonsdata, og man må vurdere konkret hvilke krav som må stilles til identifisering og registrering for at formålet med lagring av transaksjonsopplyninger kan oppnås.

Nærmere om OECD-studien og kontantkort

Studien er finansiert av personvernmyndigheten i Canada (Office of the Privacy Commissioner) og gjennomføres av Centre for Policy Research on Science and Technology (CPROST) ved Simon Fraser University[5]. I Canada er det foreløpig ikke registreringsplikt for kontantkort, men det diskuteres om en slik plikt bør innføres av hensyn til blant annet kriminalitetsbekjempelse og innbyggernes sikkerhet. Studien, som altså kartlegger reguleringen av kontantkort i alle OECD-landene, har som mål å danne et faglig fundert utgangspunkt for diskusjon og utvikling av en velegnet policy for registrering av kontantkort. Kjernen i denne diskusjonen er om adgangen til anonym kommunikasjon med mobiltelefon bør innskrenkes av hensyn til blant annet kriminalitetsbekjempelse og sikkerhet. Den canadiske personvernmyndigheten hevder at det så langt er klar mangel på dokumentasjon som viser at registreringsplikt reduserer kriminalitet eller medfører store fordeler for kriminalitetsbekjempelse eller nasjonal sikkerhet.[6]

Fordelene som gjerne assosieres med kontantkort, er at det gir en veldig god og direkte kontroll med kostnadene med å bruke telefon siden ringetiden er forhåndsbetalt. Dette betyr også at det ikke er behov for kredittvurdering slik det er for andre telefonabonnement. Forhåndsbetaling betyr også at det ikke er noe behov for tilbydere å vite hvilken kunde som benytter hvilket SIM-kort, noe som har gjort det mulig å tilby uregistrerte (anonyme) kontantkort.

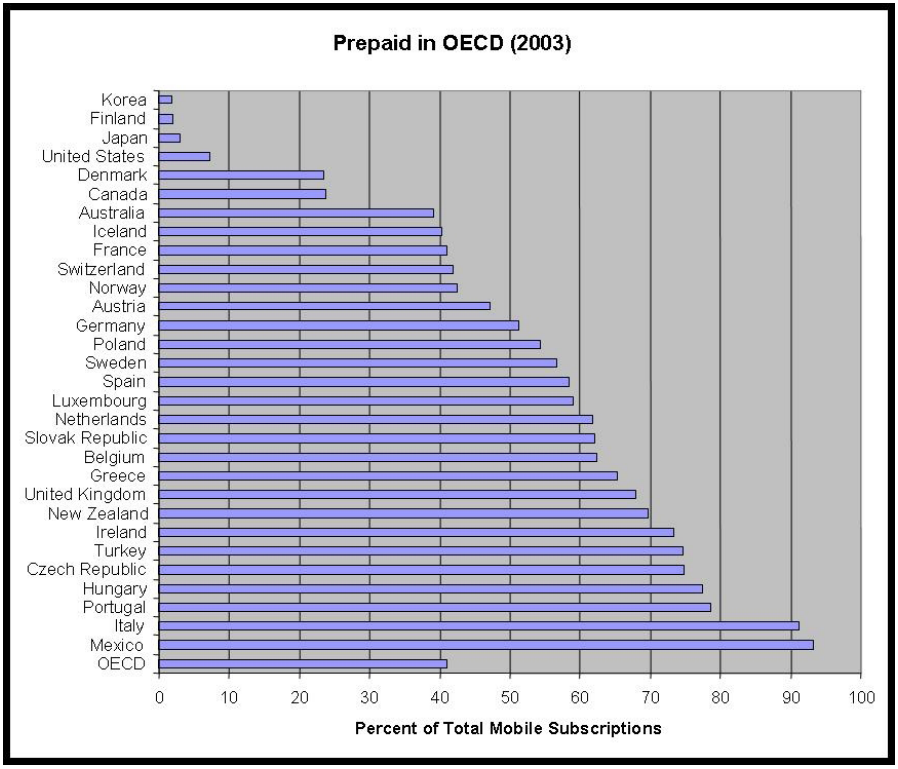
Undersøkelser[7] viser at andelen kontantkort blant alle mobilbrukere i Norge i 2003 utgjorde ca. 42,5 % av totalt ca. 1,8 millioner mobilabonnenter. Dette tilsvarer omtrent snittet for samtlige OECD land samme år hvor kontantkort

5 Se http://www.sfu.ca/cprost/prepaid/.

6 Se pressemelding av 27. januar 2005: http://www.privcom.gc.ca/media/nr-c/2005/nr-c_050127_10_e.asp/.

7 OECD Communications Outlook 2005.

utgjorde 41,0 % av totalt ca. 304 millioner mobilabonnenter. Grafen under illustrer andelen kontantkort i de ulike OECD-landene.



Figur 1 Percent of Total Mobile Subscriptions

Av de 26 OECD-landene som responderte på CPROST-undersøkelsen, er det 9 land som har innført registreringsplikt for kontantkort: Australia, Frankrike, Japan, Slovakia, Sveits, Sør-Afrika, Tyskland, Ungarn og Norge. Flere av landene har innført registreringsplikt relativt nylig. Japan innførte registreringsplikt i 2005 som følge av en rekke telefonbedrag mot eldre. Sør-Afrika har hatt lovgivning som påbyr registrering siden 2002, men reglene trådte ikke i kraft før i slutten av 2005. I Australia, Sveits og Sør-Afrika er det ingen håndheving av registreringsplikten.

Kartleggingen av OECD-landene viser at det er få studier som direkte støtter registreringsplikt for kontantkortabonnementer. Kun i Tyskland har man identifisert en studie som forsøksvis evaluerer effektivitetsgevinsten av registreringsplikt i

forbindelse med kommunikasjonskontroll og etterforskning av kriminalitet. Når det gjelder studier som fraråder registreringsplikt, har flere tyske organisasjoner hevdet at registreringsplikten er grunnlovstridig, både i forhold til borgernes personvern og i forhold til økte kostnader for tilbyderne. Enkelte forskningsrapporter i Nederland fraråder også registreringsplikt.

Lovgivningsprosessen frem til innføringen av registreringsplikt i Norge

Bakgrunnen for ny lov om elektronisk kommunikasjon

Formålet med den nye ekomloven er ifølge lovens § 1-1 «å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse, samt stimulere til næringsutvikling og innovasjon». Loven er ment å regulere hele området for elektronisk kommunikasjon, og å åpne for ytterligere liberalisering slik at den sektorspesifikke konkurranseregu-leringen etter hvert kan avvikles og markedet i større grad overlates til generell konkurranseregulering.

Loven tar sikte på å implementere EUs såkalte «reguleringspakke» for elektronisk kommunikasjon, som bl.a. består av fem direktiver vedtatt i 2002 med implementeringsfrist 25.7.2003. I forhold til registreringsplikt for kontantkort står direktivet om personvern og elektronisk kommunikasjon (kommunikasjonsdirektivet) i en særstilling[8]. Kommunikasjonsdirektivet har som formål å harmonisere lovgivningen i EU/EØS for å sikre et ensartet nivå for fundamentale rettigheter og friheter, spesielt personvern, i forbindelse med behandlingen av personopplysninger innenfor sektoren elektronisk kommunikasjon for derigjennom å sikre fri flyt av personopplysninger og av utstyr og tjenester for elektronisk kommunikasjon i EU/EØS-området.

Kommunikasjonsdirektivet var ennå ikke vedtatt da forslaget til ekomloven ble lagt ut på høring. Dette har blant annet ført til at mange av bestemmelsene i direktivet er blitt gjennomført i ekomforskriften. Direktivet tar ikke stilling til spørsmålet om registreringsplikt direkte, men gir klart uttrykk for at man innenfor sektoren skal bestrebe seg på å samle inn og behandle så få opplysninger som mulig (minimalitet), og at sluttbrukere så vidt mulig skal tilbys anonyme eller pseudonyme tjenester. For eksempel er det i fortalen til

8 Direktiv 2002/58/EF av 12.7.2002 om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor. Fristen for implementering i nasjonal rett var 31.10.2003.

direktivet (premiss 30) understreket at kommunikasjonsnett- og tjenester bør konstrueres slik at de begrenser mengden av personopplysninger til et absolutt minimum. I forhold til problematikken med spesifiserte fakturaer er det i fortalen (premiss 33) gitt en oppfordring til medlemsstatene om at det "utvikles valgmuligheter som f.eks. andre betalingsmuligheter som gir anonym eller strengt privat tilgang til offentlig tilgjengelige elektroniske kommunikasjonstjenester, for eksempel telefonkort og mulighet for å betale med kredittkort". Ved gjennomføringen av regelverket i norsk rett kan det synes som om de grunnleggende prinsippene om minimalitet og anonymitet ikke er blitt viet særlig mye oppmerksomhet, spesielt ikke i spørsmålet om registreringsplikt for kontantkort.

Forarbeidene til ekomloven

Høringsutkastet til ny lov om elektronisk kommunikasjon, inneholdt ingen bestemmelser som berørte spørsmålet om registreringsplikt direkte.[9] Høringsforslagets § 2-12 (5) gir riktignok en vid adgang for myndigheten til å gi forskrifter om taushetsplikt og om plikt til tilrettelegging for kommunikasjonskontroll, men spørsmålet om registrering av kontantkort er ikke kommentert. Ikke uventet var det derfor heller ingen av høringsinstansene som tok opp dette spørsmålet.

I Ot.prp.nr.58 (2002-2003) (*Om lov om elektronisk kommunikasjon*) er plikten om tilrettelegging for kommunikasjonskontroll flyttet fra § 2-12 (5) til ny § 2-8:

> *"§ 2-8. Tilrettelegging for lovbestemt tilgang til informasjon*
>
> *Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres.*
>
> *Myndigheten kan gi forskrifter om tilretteleggingsplikten etter første ledd, herunder om plikt til å lagre trafikkdata i en bestemt periode."*

Ifølge Ot.prp.nr.58 (2002-2003) er bestemmelsen en videreføring av den gjeldende forskriftsbestemte tilretteleggingsplikten som er fastsatt med hjemmel i teleloven § 3-4 (1) h), jf. forskriften av 23. juni 1995 nr. 39 om offentlig telenett og offentlig teletjeneste § 2-11.

---

9 Se http://www.odin.no/odinarkiv/norsk/sd/2002/publ/028021-080057/028021-080056/dok-bn.html.

Datatilsynet har i brev til Stortinget ved samferdselskomiteen kommentert bestemmelsen om tilrettelegging for lovbestestemt tilgang til informasjon. Tilsynet bemerker i brev av 28.3.2003 at forslaget til § 2-8 gir myndigheten hjemmel til å gi forskrift om tilretteleggingsplikten, "herunder om plikt til å lagre trafikkdata i en bestemt periode".[10] Ifølge Datatilsynet var muligheten for å pålegge lagringsplikt ikke kommentert i høringsnotatet, slik at tilsynet og andre høringsinstanser ikke har hatt anledning til å kommentere spørsmålet.

Datatilsynet ble senere oppmerksom på at forslaget til ny § 2-8 i Ot.prp. nr.58 (2002-2003) kunne oppfattes videre enn det tilsynet var klar over ved oversendelse av brevet av 28.3.2003. Et nytt og utdypende brev ble derfor oversendt 3.6.2003.[11] Tilsynet bemerker her at § 2-8 om tilrettelegging for lovbestemt tilgang til informasjon ifølge merknadene til bestemmelsen skulle være en videreføring av gjeldende rett. Tilsynets oppfatning var at dette innebar en plikt for tilbydere av offentlig elektronisk kommunikasjonstjeneste til å tilrettelegge nett og tjenester for ordinær kommunikasjonskontroll for politiet. Det fremgår av brevet at Datatilsynet finner det ukjent og overraskende at en videreføring av gjeldene rett også innebar en plikt for tilbydere til å registrere kontantkort. Siden spørsmålet ikke ble kommentert i høringsnotatet, bemerker Datatilsynet at det er uklart hva departementet mener skal videreføres som gjeldende rett.

Reglene om tilrettelegging for lovbestemt tilgang til informasjon er kommentert i St.meld.nr.32 (2001-2002) (*Om situasjonen i den norske mobilmarknaden*), pkt. 5.1:

> *"Gjennomføring av kommunikasjonskontroll og påfølgjande behov for registrering av abonnentar og teletrafikk fører til vanskelege avvegingar i forholdet mellom personvern og andre samfunnsinteresser. Når Stortinget ved endringslov til straffeprosesslova (lov 03.12.1999 nr. 92) har gjeve reglar om når og på kva måte kommunikasjonskontroll lovleg kan gjennomførast, må dette lede til at sektorlovgjevinga sine krav til tilbydarane vert utforma og praktisert slik at dei ikkje er til hinder for at krava etter straffeprosesslovgjevinga kan verte oppfylte. Dette må også gjelde for reglar gjeve av styresmaktene på området for personvern om lagring og behandling av personopplysningar.*
>
> *Etter Samferdselsdepartementet sitt syn medfører plikten til tilrettelegging for lovleg kommunikasjonskontroll etter telelova § 3-4 h og offentlignettforskrifta § 2-11 til at mobiltilbydarane må registrere*

10 Se http://www.datatilsynet.no/upload/Dokumenter/saker/2003/hoeringstillegg.pdf.
11 Se http://www.datatilsynet.no/upload/Dokumenter/saker/2003/ekom2.pdf.

sine kontantkortabonnenter på lik linje med sine ordinære abonnentar. Dette er gjennomført av Telenor Mobil AS, mens andre tilbydere som til dømes NetCom GSM as har praktisert ei ordning med frivillig registrering av persondata for sine kontantkortabonnenter. Tidlegare kunne det vere ein viss tvil om det låg føre tilstrekkeleg heimel for registreringsplikta i telereguleringa. Etter ein endring i teleloven § 3-4 d, jf. Ot.prp.nr.87 (2000-2001) og Innst.O.nr.121 (2000-2001) meiner Samferdselsdepartementet at det nå ikkje ligg føre tvil om registreringsplikta."

Tilbydernes praksis tyder også på at det har vært tvil om adgangen til å registrere kontantkortabonnenter. I følge Christian Dahlgren[12] har NetCom frem til vedtakelsen av ekomforskriften den 18.2.2004 og de nærmere retningslinjene fra Post- og teletilsynet (se under) ikke registret andre kontantkortkunder enn de som selv frivillig registrerte seg. I begynnelsen av 2004 hadde derfor Netcom ca. 250.000 kunder som ikke var registrert. Telenor, derimot, har alltid krevd registrering av sine kontantkortabonnenter, men fordi informasjonen ikke har fungert som faktureringsinformasjon, ble de oppgitte opplysningene aldri kontrollert mot folkeregisteret.

Jeg er senere blitt kjent med at Post- og teletilsynet i 1999 fikk vurdert om telekommunikasjonslovgivningen var til hinder for at tilbydere av mobiltelefontjenester selger forhåndsbetalte SIM-kort med uregistrert abonnement. Forsker Jens Petter Berg ved Institutt for rettsinformatikk vurderte i en betenkning av 25.1.1999 lovligheten av registreringsplikt i forhold til teleloven, personregisterloven, EUs personverndirektiv og EMK artikkel 8. Bergs konklusjon var at teleforskriften § 2-11, jf. teleloven § 4-6 (2) hjemlet registreringsplikt, og at en slik plikt var lovlig i forhold til personregisterloven. I forhold til EMK artikkel 8 var Bergs vurdering at forbrukerhensyn alene neppe kunne være tungtveiende nok til å lovliggjøre registreringsplikt. Men dersom registreringsplikten begrunnes med hensyn til politiets og påtalemyndighetens behov ville dette være lovlig også etter EMK artikkel 8.

Ekomforskriften

Ved vedtakelsen av ekomforskriften den 18.2.2004 er det ikke lenger tvil om at det er registreringsplikt for kontantkort, jf. § 6-2 (1):

"Tilbyder av offentlig telefontjeneste skal føre oversikt over enhver sluttbrukers navn, adresse og nummer/adresse for tjeneste. Oversikten

12 Christian Dahlgren, *Elektroniske spor fra mobiltelefoner - om politiets bruk og teleoperatørenes lagring av trafikkdata*, CompLex 4/04, s. 12, Oslo 2004

skal inneholde opplysninger som muliggjør entydig identifisering av de registrerte, jf. § 6-3 annet ledd."

Forslaget til ekomforskrift ble sendt ut på offentlig høring den 4.7.2003. I kommentaren til bestemmelsen er det uttalt at en tilsvarende bestemmelse ble sendt ut på høring fra Post- og teletilsynet 5.7.2002 i forbindelsen med utkast til endringer i offentlignettforskriften og nummerforskriften. Det vises i høringsforslaget også til St.meld.nr.32 (2001-2002), jf. over. I sitt høringsvar til forslag til ekomforskrift savnet Datatilsynet en presisering av hva som menes med entydige "identifikasjonsopplysninger", da normal forståelse av begrepet typisk vil være 11-sifret fødselsnummer. Tilsynet bemerket også at den anså konsesjonen for behandling av personopplysninger om abonnenters bruk av teletjenester som en tilfredsstillende regulering av bruk av fødselsnummer.

Datatilsynets utgangspunkt har her vært at fødselsnummer bare innhentes i den grad tilbyderen av teletjenester anser det som nødvendig for å innhente kredittopplysninger om en kunde i forbindelse med inngåelse av abonnementsavtale. Fødselsnummeret vil ikke være nødvendig for gjennomføring av tjenesten ellers, og må slettes etter at kredittopplysningene er hentet inn.

Gjennomføring av registreringsplikten

Post- og teletilsynet (PT) har i brev av 29.9. og 8.11.2004 presisert hvordan registreringsplikten skal gjennomføres.[13] Kravene er oppstilt etter en dialog mellom representanter fra tilbyderne, Økokrim, Politidirektoratet, Oslo Politidistrikt og PT.

Av PTs brev av 29.9.2004 fremgår det at Økokrim og politiet ønsket en streng identitetskontroll etter mønster fra hvitvaskingsloven, slik at kunden må møte opp personlig og fremlegge legitimasjon før det etableres et kundeforhold. PT har imidlertid stilt seg tvilende til om tilsvarende krav skulle gjelde for ekomloven og ekomforskriften. Tilsynet har derfor lagt seg på en linje hvor minimumskravet for kvalitetssikring er at de registrerte opplysningene kan kontrolleres opp mot opplysingene i Folkeregisteret. Telefontjeneste skal imidlertid ikke kunne benyttes før bruker/eier er registrert på en entydig måte. Hvordan dette kravet oppfylles, er opp til tilbyderne, f.eks. ved at det legges frem legitimasjon ved utsalgsstedet eller at første samtale går til et kundesenter hvor registrering foretas.

Etter en fristutsettelse har PT satt følgende krav til tilbyderne:

13 Se http://www.npt.no/iKnowBase/FileServer/200400631-32.pdf?documentID=31653/.

- Alle nye sluttbrukere av offentlig telefontjeneste, inkludert kontantkortkunder, skal registreres i samsvar med kravene innen 1.2.2005. Fra samme dato skal uregistrerte kontantkortkunder ikke lenger ha mulighet til å fylle på sine kontantkort.
- Alle sluttbrukere av offentlig telefontjeneste skal være registrert i samsvar med kravene innen 1.8.2005. Fra samme dato skal de nummer hvor bruker ikke er identifisert på en entydig måte og registrert, stenges for normal trafikk.

PT har fulgt opp tilbydernes etterlevelse av kravene og sendte i begynnelsen av november 2005 brev med pålegg om retting i forbindelse med manglende registrering av kontantkortkunder til Chess og Lebara Mobile. Tilbyderne trues med dagsmulkter på kr 50.000 per dag for overtredelse av påleggene.[14]

Nærmere om « tilretteleggingsplikten for lovbestemt tilgang til informasjon »

Omfanget av tilretteleggingsplikten er i Ot.prp.nr.58 (2002-2003), s. 93, beskrevet som "kommunikasjonskontroll som gjennomføres av politiet etter reglene i straffeprosessloven kap. 16a" og dessuten "oppfylling av utleveringspålegg etter straffeprosessloven § 210 når utleveringspålegget gjelder informasjon om sluttbruker og elektronisk kommunikasjon."

Dahlgren (2004:17) argumenterer for at tilretteleggingsplikten gjelder enhver lovbestemt tilgang til trafikkdata. Dette betyr i så fall at tilretteleggingsplikten omfatter den informasjon som utleveres etter fritak fra taushetsplikten fra PT eller retten, etter samtykke eller nødrett og de data som beslaglegges etter nektet utlevering. Derimot kan det ikke innfortolkes noen plikt til å lagre trafikkdata i tilretteleggingsplikten.

Adgangen til å lagre trafikkdata følger av Datatilsynets konsesjon om behandling av opplysninger om abonnementers bruk av teletjenester, samt ekomloven § 2-7 om kommunikasjonsvern. I følge konsesjonens pkt. 2 kan det bare behandles opplysinger "som er nødvendige for gjennomføring og fakturering av tjenesten". Konsesjonen er taus om behandling av opplysninger knyttet til bruk av kontantkort. Siden kontantkort er forhåndsbetalt, skulle det ikke være nødvendig å lagre trafikkdata fra disse for annet enn transaksjonsformål. Dahlgren (2004) finner imidlertid i sin avhandling at tilbyderne i praksis lagrer opplysninger om bruken av kontantkort ut over dette. Resultatet er at politiet

14 Se http://www.npt.no/iKnowBase/Content/paalegg_chess.pdf?documentID=46406/ og http://www.npt.no/iKnowBase/Content/paaleg_lebara.pdf?documentID=46407/.

har mulighet til å kreve utlevering av trafikkdata som ikke skulle vært lagret. Konsesjonen er taus om lokaliseringsdata, og Dahlgren (2004) stiller derfor også spørsmål om tilbydernes lagringspraksis er i overensstemmelse med lov og konsesjon på dette punktet.

Avsluttende bemerkninger

Redegjørelsen viser at registreringsplikten for kontantkort i Norge er blitt innført så å si uten tilløp til debatt eller belysning av prinsipielle spørsmål angående retten til personvern og anonymitet. Etter min mening er det uheldig ikke å skille klarere mellom opplysninger om brukeren (abonnementsopplysninger), og opplysninger om bruken av elektronisk kommunikasjon (trafikkdata). I ekomforskriften § 7-1 (1) siste setning er trafikkdata definert som "data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring". Ot.prp.nr.58 (2002-2003) presiserer dette ytterligere: "Med trafikkdata menes for eksempel data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, data, omfang, varighet og underliggende tjeneste".

Artikkel 29-gruppen har i sin Opinion 113/2005 til forslaget til direktiv om lagring av transaksjonsdata understreket behovet for å klargjøre i direktivet at det ikke skal være plikt til identifisering når identifisering ikke er nødvendig for fakturering eller andre formål for å gjennomføre en kontrakt.[15] I forarbeidene til ekomloven er spørsmålet om registreringsplikt og krav til abonnementsopplysninger nærmest tatt for gitt, mens fokuset har vært på å redegjøre for reglene om politiets og påtalemyndighetens adgang til lagrede trafikkdata, samt innføring av nye regler for lagring av trafikkdata til bruk for politiet.

En kan også stille spørsmål ved hvor ønskelig det er med gjennomføring av kommunikasjonsdirektivet i ekomloven og ekomforskriften. Flere sentrale aktører (eksempelvis PT, Telenor, Netcom og Datatilsynet) bemerket i høringen til ekomloven at direktivet fortrinnsvis burde gjennomføres ved en egen lov, eventuelt gjennom personopplysingsloven, personopplysningsforskriften eller en egen forskrift til personopplysningsloven. Resultatet er blitt at bestemmelsene er forholdsvis vanskelig tilgjengelig blant regler av mer konkurransemessig og teknisk art. I tillegg må aktørene forholde seg til flere tilsynsmyndigheter med overlappende ansvarsområder: Datatilsynet gir i dag konsesjonen som

15 Opinion 113/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(200543)8 final of 21.09.2005), http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf.

blant annet hjemler lagring av trafikkdata og fører tilsyn med tilbydernes behandling av personopplysninger etter personopplysningsloven, mens PT har tilsyn med reglene som gjelder registreringsplikt, kommunikasjonsvern, samt fritak fra taushetsplikt for tilbydere etter forespørsel fra politiet.

Det synes også å være et stort sprik mellom regelverk og tilbydernes praksis i forhold til registrering av kontantkortabonnenter og lagring av trafikkdata. I forarbeidene til ekomloven kom det for eksempel overraskende på mange aktører, også Datatilsynet, at en videreføring av gjeldende regelverk innebar registreringsplikt av kontantkortabonnementer. Undersøkelser av tilbydernes praksis for lagring av trafikkdata viser at dette ikke alltid skjer innenfor konsesjonens og regelverkets rammer. Dahlgren (2004) antar at dette først og fremst skyldes et uoversiktlig rettskildebilde, til dels sterkt motstridende interesser og tekniske løsninger som ikke er tilpasset lovgivningen.

Spørsmålet om registreringsplikt handler også om hvilken grad av sikkerhet man skal ha for at brukeren er den han eller hun gir seg ut for å være. De nærmere prosedyrer og rutiner for registrering bestemt av Post- og teletilsynet og tilbydernes oppfølgning av dem bør antakelig evalueres jevnlig. Dersom prosedyrene for registrering gjør det enkelt for kriminelle å unnlate å oppgi riktig personalia, vil dette undergrave hovedformålet med registreringsplikten. Det er i så tilfelle grunn til å stille spørsmål om fordelene med en slik ordning oppveier den ekstra belastningen for tilbyderne og brukerne.

ANTI-SPAM LEGISLATION BETWEEN PRIVACY AND COMMERCIAL INTEREST

Dana Irina Cojocarasu

Abstract:

This article aims at assessing how appropriate the current European Union legislation is to serve as a tool for Member States in their fight against spam. In my view, spam is to be seen as an anomaly, occurring both in the context of data processing and in the commercial practice. Therefore it is important to analyze this phenomenon in the context in which it occurs and to examine the balance of interests reached by the anti-spam legal provisions pertaining both to e-commerce and personal data protection.

Introduction

Although most of the average computer users could recognize a spam message when they receive it in their e-mail box, very few of them might accept the challenge to define or to explain it. Their dilemma is perfectly excusable, as there is, up until this moment, no universally agreed definition of spam, although more and more international initiatives and action plans to combat it are launched[1] . The various definitions provided are more functional and working definitions. Moreover, although the Community legislation refrains from using the term spam as it is, other official documents use it[2].

For the purpose of this article I will try to identify clearly the distinctions between the e-mail spam and the e-mail marketing (even the one involving some unsolicited commercial communications) as well as between the practices involved in spam and the legal ways of collecting and processing personal data.

---

1 See for example http://www.oecd.org/department/0,2688,en_2649_22555297_1_1_1_1_1,00.html for the OECD work on spam and also http://www.itu.int/osg/spu/spam/ for the International Telecommunication Union activities in combating spam (last visited July 16th 2005)

2 See for example; the Presidency Paper, "*Unsolicited communications for direct marketing purposes or spam*", Council of the European Union, Brussels, 24 November 2004, 15148/04, Article 29 Data Protection Working Party's "*Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection*-" 21st November 2000, 5063/00/EN/FINAL WP 37

Official EU documents define *spam* as "the practice of sending unsolicited e-mails, usually of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has had no previous contact"[3]. Other definitions point out apart from the unsolicited and the commercial character some other different features commonly associated with spam: the fact that the "e-mail address has been collected in a public space on the Internet"[4] or that the sender disguises or forges his identity"[5]. Finally, a more recent view of the European Commission, after the opt-in regime for unsolicited commercial e-mail messages was introduced by the Directive on privacy and electronic communications[6] , states that "in short, [spam] is commonly used to describe unsolicited, often bulk e-mails. The new Directive does not define or use the term 'spam'. It uses the concepts of 'unsolicited communications' by 'electronic mail', 'for the purposes of direct marketing' which taken together, will in effect cover most sorts of 'spam'. Therefore, the concept of 'spam' is used in this Communication as a shortcut for unsolicited commercial electronic mail"[7]

As it can be seen from these definitions, the most common traits of the practice being discussed here refer to the commercial character, to some circumstances involving the collection of the e-mail address and to the fake identity of the sender. While these are essential traits, they provide little guidance as to the distinction between spam and e-mail marketing involving unsolicited communications.

Essentially, the purpose of most spamming is the commercial marketing activity, although the content of spam e-mails can vary. At the same time, this activity involves a personal data processing, as it needs, as an absolute prerequisite, the collection and use of e-mail addresses[8]. Thus, spamming is potentially directed indiscriminately towards each and every individual that owns one such address.

---

3 DPWP: "*Privacy on the Internet* (2000), 5063/00/EN/FINAL.

4 DPWP "*Opinion 1/2000 on certain data protection aspects of electronic commerce*"(5007/00/EN/final) , page 3 http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2000/wp28_en.pdf (last visited July 16th 2005)

5 Serge Gauthronet and Etienne Drouard "Unsolicited commercial communications and Data Protection", January 2001.

6 "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", Official Journal L 201, 31/07/2002, P. 0037- 0047

7 COM(2004) 28 final, op.cit.

8 Although spam can be distributed also through sms messages, facsimile machines and automated calling machines, due to the limited size of this thesis I will limit my analysis to e-mail spam messages.

In my view, spam is to be viewed as an anomaly, both from the perspectives of commercial practice and data processing. As I will argue in this article, the e-mail addresses can be considered in the overwhelming majority of cases (even when they belong to legal persons) as personal data[9]. Therefore, the collection, use and third party disclosure of the e-mail addresses carried out as part of the spam activities represent not only commercial practices (calling for the application of the E-commerce Directive[10]), but can be seen also as involving a processing[11] of personal data. While as a rule, personal data has to be collected and processed "fairly and lawfully" and while e-mail marketing is a legitimate business with a series of unquestionable advantages both for the marketer and the prospect customer, as an exception, the spamming activity speculates on existing legal, technical or enforcement difficulties in order to reach the expected commercial benefits while short-circuiting the established rules.

Instead of choosing to fragment the normative provisions into easily definable concepts, my goal was to look at spam in the business context in which it occurs.

That requires first of all to clearly identify the investigated business practice and to point out the ethical and behavioral differences between the legitimate e-mail practices and spam.

Subsequently, I will provide some arguments justifying why e-mail addresses are to be regarded as personal data and I will discuss why unsolicited commercial communications represent a concern for individual privacy.

The third and the most extensive part of the article will present the anti-spam legal framework in force in the European Union. Since this framework comprises provisions pertaining both to e-commerce and data protection, I will examine whether or not these provisions converge towards a coherent approach and the impact this has on the efficiency and the effectiveness of the anti-spam solution.

The evaluation of the efficiency and the effectiveness will take into account three elements: the business practices that are commonly associated with spam, as a factual argument, the interests of the actors involved, that generates the dynamic of the relations established between direct marketers and potential receivers of the commercial messages as well as the reflection of these two elements in the relevant legal provisions of the E-Commerce Directive and the 2002 Privacy Directive. Therefore, the conclusion reached is not based only

9 In the interpretation given to the term "personal data" by article 2(a) of the Directive 95/46/EC.

10 Directive 2000/31/EC;

11 In the interpretation given to the term "processing" by article 2(b) of the Directive 95/46/EC.

on a limited legal text dissection, but includes arguments relating to social psychology, marketing, economic theory.

2. E-MAIL MARKETING AND SPAM PRACTICES- Differentiating features:

The technological advances employed "in the interest" of the individuals inevitably reshaped the way in which they organize their daily lives, the way they perceive themselves and their needs and the way in which they do business with each other.

One of these changes relates to the dual impact of the digital technologies on the individual's ability to interact with the environment in which he lives. On the one hand, they expanded the choices available and brought diversity in both products and lifestyles. On the other hand, through enabling at the same time the acquisition, retention and secondary dissemination of vast amounts of data, they made it more difficult for the individual to assert with certainty what information about him is available and who controls it, much less how it got out of the private sphere into the public domain.

This change can be illustrated by the advertising techniques currently employed by the marketers. Traditional media of dissemination of advertising messages was rigid and it didn't allow very much to customize the content to the profile of a certain group or individual. Conversely, marketing techniques used by the advertisers today allow them to target the advertising campaigns to smaller groups of people, based on customers' interests, as identified or inferred previously by the marketer through examining on-line activities. Targeted advertising is therefore made possible by the use of personal information. Therefore the marketer's interest in knowing as much as possible about their potential clients is obvious.

Marketers are interested in the efficient allocation of their resources, and this implies not spending on advertising products or services that either are not of interest to a particular consumer group, or are not presented in a manner suited to appeal their level of understanding and interest.

At the same time, the costs of a direct marketing campaign through e-mail, automated calling machines, sms, facsimile are much smaller then those involved in indirect marketing techniques, through television, radio, brochures. The companies do not actually pay to get the personal information from the customers (they still sell their products and services to the customers for the price they set). Moreover, there are no intermediary costs involved in the printing, distribution, mailing of the commercial messages, which can reach the potential customers directly. Simultaneously, the marketers are provided instantly

with the feedback of their activity, once the members of the target group chose either decide to buy or to discard the commercial messages received.

As shown above, personal information represents an asset for the marketers. However, the practices involved in the collection, use or transmission of the e-mail addresses[12] to third parties set the dividing line between e-mail marketing, as legitimate practice, with proven benefits both for the customers and marketers, and spam as nuisance and anomaly having "reached worrying proportions"[13].

1. the means to collect the e-mail addresses

It is possible for the interested parties[14] to get hold of possible customers' e-mail addresses:

a. directly from the owner of the address, who agrees to disclose his address in order to receive certain types of commercial communication – this is a typical situation of permission based marketing. This method sets the basis for long-term commercial relation between the parties based on trust and mutually beneficial.
b. indirectly, without the knowledge of the e-mail address owner,
   - *who is unaware that his address will be used in the future for direct marketing*. For example, the user posts his address in a public space on the Internet, for purposes different than that of receiving commercial communications from different marketers. However, spamware tools can be employed in order to automatically navigate websites, newsgroups and chat rooms and collect the e-mail addresses found there. Whereas the "collection of e-mail addresses from public spaces on the Internet for the purposes of unsolicited commercial e-mail " has been considered "contrary to the existing community legislation"[15], studies have shown that the addresses posted on public spaces of the Internet are the main source of the spammers thus exposing their owners to the

12 At this point my analysis is based on the assumption that e-mails are personal data. This assumption will be argumented in detail in the following section.
13 COM(2004) 28 final .
14 I will use the term "marketer" to designate the person that uses direct marketing, as prescribed by the law and the various codes of good practice, and the term "spammer" in order to designate the person that does not comply with the same rules, while engaging in direct marketing.
15 DPWP(2000), 5063/00/EN/FINAL, op.cit.

greatest amount of spam[16]
But another example can be provided for the same situation: the insufficiently attentive user that was misled by the wording or the design of the webpage and was not aware that he gave his consent (especially when the marketer uses a pre checked box or a negative option statement[17]). While this technique does not in theory amount to spam, as somehow consent was asked and given, marketers are recommended not to use this strategy, as the image they create in the eyes of the customers will be negative[18] and the results doubtful[19] .

- *who is unaware that that his address is being harvested at all*. This technique is clearly typical for spam. Such a "brute force" attack on the mail server, where the software used by the spammer sends spam messages to all possible combination of letters that could form an e-mail address, could generate a tremendous amount of spam, even to addresses that hadn't been shared anywhere[20]. There is little that can be done by an individual user when faced to this sort of spam, unless he chooses a more complicated e-mail, more difficult to detect through "dictionary attacks".

2. The transmission practices

are, in my opinion, the main trait differentiating e-mail marketing from spam. Although both practices involve electronic unsolicited commercial messages,

16 "*Why Am I Getting All This Spam?"* Unsolicited Commercial E-mail Research, Center for Democracy & Technology March 2003, available at: http://www.cdt.org/speech/spam/030319spamreport.pdf (last visited July 28, 2005).

17 For example by checking a box, calling or writing the marketer if the customer does NOT want to be on a mailing list.

18 "It is in the interest of business to be able to use legitimate commercial e-mail and be associated with ethical e-mail marketing using industry codes of conduct such as these guidelines. Unfavorable attitudes generate consumer skepticism and can lead consumers to take actions that are catastrophic to businesses" ICC Guidelines on Marketing and Advertising using Electronic Media, 2004.

19 "*The negative option statements was relatively inefficient, whereas the yes/no format proved to be more efficient: more honest way of asking for permission than a negative format , more conducive to building customer relationships. Consumers see the direct yes no format as an invitation, whereas the negative option as a challenge*": George R. Milne (1997), study regarding consumer's willingness to provide marketers with personal information and permission to rent this information given in varied permission formats. The author commented also that as customers become more aware of the transfer practices, they may come to expect that marketers will be more straightforward in their communications.

20 According to CDT (2003) study, see footnote 16.

marketers and spammers use different strategies to get their message through to their potential customers.

First of all, spamware programs can automatically generate false headers and false return address information[21]. This practice is banned by the existing legislation and the applicable codes of practice, both in Europe and in the US[22].

Also, mailing tools used by spammers are capable of sending bulk e-mail without going through a specific mail server or ISP[23], which avoids the trouble of being detected or having their accounts terminated due to the way they exhaust the bandwidth. Although marketers send as well the same e-mail advertising message to a great number of potential customers, they usually belong to the same cluster or are considered to have a special interest in the product or service being advertised. "If marketers failed to identify proper target groups and send unsolicited e-mail to massive audiences, negative effects could be tremendous"[24], potentially facing the contempt of both the customers and the business community (complaints to upper administrative bodies, black listing).

Spam is also repetitive, and arguably very difficult to stop, since the unsubscribe links do not work[25]. According to the OECD Paper on Spam[26], spammers either open free e-mail accounts which they abandon before getting caught, or load in multiple accounts, so that when one of them is terminated, another one becomes automatically active. The marketers' practice has to involve as a fundamental requirement, the possibility for the customers to opt out from receiving further commercial messages.

Taking into account the e-mail harvesting methods used, it is easy to realise that spam messages are untargeted and indiscriminate as to the potential receiver. In fact, a big part of the nuisance caused by spam to the users is represented by the discomfort of constantly having to spend time and effort,

21 *Background paper for the OECD workshop on spam"*, DSTI/ICCP (2003)10/FINAL, 2003.

22 See for example Recital 43 of 2002/58/EC Directive and Section 5(a) of the US CAN-Spam Act, as well as article 3 of the ICC Guidelines on Marketing and Advertising using Electronic Media, 2004, Section 2.1 of the European Code of Practice for the use of personal data in Direct Marketing, FEDMA 2005.

23 Serge Gauthronet and Etienne Drouard (2001), op.cit, page 32.

24 Susan Chang, Mariko Morimoto "An Assessment of Consumer Attitudes toward Direct Marketing Channels: A Comparison between Unsolicited E-Mail and Postal Direct Mail" Michigan State University April 1, 2003 available at http://www.inma.org/subscribers/papers/2003-Chang-Morimoto.doc (last visited 2005-07-28).

25 In fact, users are advised not to click on the unsubscribe links (if they are provided), as they will only thereby confirm that the address is valid, used…and good to spam further.

26 *Background paper for the OECD workshop on spam"*, DSTI/ICCP (2003)10/FINAL, 2003.

as well as money in order to get rid of unsolicited, useless[27] emails. On the matter, the Guidelines[28] issued by the International Chamber of Commerce recommend in article 9 to all marketers, that in case they do send unsolicited commercial e-mails as part of their marketing strategy, they should "have reasonable grounds to believe" that the consumer targeted will find the offer of interest for him.

3. the content

From the point of view of the content, there are similarities between spam practices and e-mail marketing. Although spam can include scams (humanitarian or phishing), pornographic content or viruses, the great majority of it is still aiming at advertising products and services. What differs often is the quality and the truthfulness of whatever "special offer" is being presented there.

4. the position of the receiver with regard to the unsolicited communication received

The overwhelming majority of customers don't like receiving spam. It's unsolicited, unwanted, useless and unstoppable. It imposes unjustified costs on the targeted end-users without bringing any benefit. Some distinctions should be made here regarding the terms used. While the offers received from a company that sold you a computer might be seen as "unsolicited", there is a high likelihood that they are "wanted", and "useful" (even if I don't choose to buy the products or request the services, I can be thus informed about the latest products available and even compare prices and find out whether a better offer is available on market for something I'm interested in). According to EASA[29], once the individual has given his consent to the use of his contact details for marketing purposes, all the subsequent communications he receives from that source are deemed to be "solicited" even if the individual is not aware of the future content of these communications. While I don't argue the level of

27 Studies quoted in the OECD Paper on SPAM claim that even a very low response rate (0.001%) is enough to make spamming profitable (see page 9) due to the low costs involved in producing and sending them.

28 "These Guidelines (…) are an expression of the business community's recognition of its social responsibilities in respect of marketing activities and communications. The Guidelines have been updated in light of experience acquired, and ICC, conscious of the ongoing development, commits itself to regularly review them to ensure their continued viability"

29 "Recommendations for the issue paper for the EU Workshop on unsolicited commercial communications or spam", November 4th 2003, page 4 available at, http://www.easa-alliance.org/news_views/en/position_spam%20issue.pdf (last visited July 28, 2005).

expertise in this Communication, I don't agree with the interpretation of the meaning of the verb "to solicit"[30]. While the commercial communications subsequent to a manifestation of consent cannot be seen as spam, they are and remain unsolicited, but they deemed to be accepted, wanted, useful (for as long as the consent is not revoked through the exercise of the right to opt-out). In my view, you cannot solicit something and not know what you will receive as the result of your solicitation.

It can be argued that the customers had to deal with unsolicited commercial communications as a result of direct marketing long before the Internet came into play, and this is one of the risks inherent to having multiple choices in terms of offers for similar products and services. The marketers become more aggressive in bringing their offer in the attention of the public. However, the level of consumer annoyance when faced with unsolicited e-mails is, for some consumers, higher than in case of other forms of unsolicited direct marketing (brochures in the mail, for example)[31]. The receivers have to bear the online service costs according to the time spent online, risk loosing important mail due to limitation in the storage space of their e-mail boxes, and waste time sorting out the important e-mails from the unwanted ones.

These are inconveniences that the end users have not faced before and the cumulative social and economical impact of this unfair business practice, spam, calls for special measures to limit and if possible put a stop to it.

Unsolicited Commercial Communications - A Concern For Individual Privacy?

Few people would doubt that a social security or a personal ID number are personal data, as well as the credit card number or bank account and the information that can be drawn from it (spending patterns, purchases made, solvency). However, the e-mail address is more difficult to qualify due to its intrinsic features and its function. I will discuss these aspects in the following lines.

Formally speaking, an e-mail address is formed by two parts, separated by the @character. The host name identifier, located on the right part of the @ sign rarely constitutes personal data when the e-mail service is free of charge and accessible worldwide (take a.b@yahoo.com or a.b@gmail.com). Exceptionally, in case the e-mail address belongs to a business, the right part of the@ sign can

30 To make solicitation or petition for something desired, to seek to obtain by persuasion, entreaty, or formal application, synonyms: to ask for, to request, to seek

31 see Susan Chang, Mariko Morimoto, op.cit, page 6

allow the identification, due to the fact that it coincides most of the times with the website address and most likely the trademark of the business. For example, a business registered as "INCODATA", has http://www.incodata.ro/ as a website address and office@incodata.ro as a contact e-mail address.

On the left side of the @sign, a group of characters (letters and numbers most if the times) describes "the name" with which a user is known by the e-mail service. While it is true this name is unique for every e-mail account opened within an e-mail host server, there is no technical obligation that the identifier be the actual name of the individual opening an account, and there are no limitations regarding the number of on-line identifiers (e-mail addresses) that a person can have. At the same time, the e-mail account can be accessed from any computer connected to the Internet, no matter where it is geographically located.

The most important criteria in order to qualify certain data as being personal is its ability to lead, directly or indirectly to the identification of the individual to whom they belong[32]. In the law literature this criteria has been contextualized by reference to the relevant agent of the identification, the ease, the precision or the validity of the identification[33]. What is important here is that the identification was seen as leading to a "flesh and blood" person, and not to a simple on-line identity, that does not necessarily coincide with the legal[34], off-line one. Due to the features identified above, it is questionable that by employing "all means likely reasonably to be used"[35] the e-mail address is able to convey in itself the real, off-line identity of its rightful owner.

Some indications that e-mail address is seen as personal data can be traced both in law[36], and in official documents[37], but no further justifications are provided. As I see it, one reason for this might be that it is a real, actual person (legal or natural) who suffers the costs (pecuniary or not) associated with any misuse of the e-mail address. But is this reason enough?

---

32 See article 2(a) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of the individuals with regard to processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/ 1995 P. 0031-0050

33 Lee A. Bygrave, "DATA PROTECTION LAW, Approaching its rationale, Logic and Limits", Kluwer Law International, 2002, page 42

34 By legal identity I mean the one recognized by the law, and confirmed by identity cards, birth certificates, administrative acts and so on

35 see Recital 26 of the Directive 95/46/EC

36 see Recital 26 read in accordance with Recital 15 and article 2(b) of the 2002 Privacy Directive.

37 for example, Presidency Paper (2004) (15148/04), op.cit., and DPWP *Opinion 1/2000* (5007/00/EN/final).

I found most interesting and relevant to the discussion about privacy concerns related to the unsolicited commercial e-mails that, according to Bartel and Hoy (2000)[38], privacy concerns among on-line consumers appear when the information usage is not expected by the consumer, either because he was not aware that his personal data was used, or that the use was different from the one originally intended. The authors correlate their empirical findings with the ones reached by Cranor, Reagle and Ackerman (1999) [39], that evidentiated the fact that when consumers were asked to provide their e-mail addresses, the information was not perceived as sensitive and therefore did not produce privacy concerns. However, the "fear of unfamiliar" caused by the inability to trace back the circumstances in which the marketer acquired the e-mail address increased their concerns[40] .

Overall, Bartel and Hoy (2000) estimate that their findings confirm earlier studies suggesting that privacy is a measure of the control of the transactions between the individual and others. When the transaction is immediate and involves only an exchange between a consumer and one entity, the consumer will feel more in control and thus, less concerned about privacy.

On the other hand, when the transaction extends to multiple entities (as it is often the case when e-mail lists are traded between marketers), the consumer experiences loss of control and therefore an increased concern for privacy.

The empirical studies quoted above show that the most significant privacy concern of the individual faced with the massive phenomenon of spam is the lack of control over the use of his personal data, including here the related interest in attentional self determination. While the legislation recognizes privacy as a fundamental human right[41], its scope and ambit are difficult to define through the adoption of uniform and universal standards, as different individuals value differently their own privacy, thus building their own hierarchy of rights. Therefore, they are willing to sacrifice one for the sake of the other according to cognitive and emotional resolutions, that are hard to anticipate and even harder to generalise.

---

38 Kim Bartel Sheehan and Mariea Grubbs Hoy " Dimensions of privacy concerns among online consumers" Journal of public Policy and Marketing(2000), 19 spring, 62-73

39 Lorrie Faith Cranor, Joseph Reagle, and Mark S. Ackerman "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy AT&T Labs-Research Technical Report TR 99.4.3" available at http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm (last visited, August 03 2005)

40 Bartel, Hoy, op.cit, page 68

41 see article 8(1) of the European Convention of Human Rights.

However "while privacy protection is an individual concern, its effective enforcement may only come through collective action"[42].

The Efficiency Of The Anti-spam Solution Provided By The European Legislator

Up until now the spam is not dealt with by the European legislator within one specially designed normative instrument. The rules regarding unsolicited commercial communications can be found mainly in two European Directives: the E-Commerce Directive (2001) and 2002 Privacy Directive. However, as I will show below, not only these directives safeguard different interests of the actors involved in the commercial communications, but impose different and even contradictory obligations on the marketers. Due to the limited length of this article, the relevant provisions of the Directives will not be analyzed separately in detail; I would rather focus on discussing the cumulated efficiency of the anti-spam normative tools made available by the European legislator.

For the purposes of the analysis I adopted a broad interpretation of the term "efficiency", including not only an evaluation of the costs of enforcing the system vs. the practical results achieved, but also a balance of the practical results vs. the basic aims of the legal framework; the latter evaluation might be otherwise included under the term "effectiveness".

In essence, I will try to provide a possible answer to two questions:

1. Do the different mechanisms provided by the E-commerce Directive, on the one hand, and Privacy and Data Protection European Directives on the other converge towards a unitary solution or do they clash?
2. Is this solution (Or are the two mechanisms) fit for the purpose it (they) aim(s) at?

1. Different mechanisms –one solution?

Comparing the provisions of the E-commerce Directive (articles 6 and 7) with the provisions of the 2002 Privacy Directive (mainly article 13), the first point that becomes obvious is that they employ different mechanisms in the fight against spam, and therefore establish different duties for the marketers that

42 see Ann Cavoukian, Information and Privacy Commissioner Ontario, "*Privacy as a fundamental human right vs.an economic right: an attempt to conciliation" 1999* available at: http://www.ipc.on.ca/userfiles/page_attachments/pr-right.pdf (last visited July 18th 2005).

wish to interact with potential customers through e-mail commercial messages and to send unsolicited messages.

The E-Commerce Directive leaves it up to the Member States to permit or to forbid unsolicited commercial communications through e-mail (art.7(1)) and imposes on the marketers a mandatory consultation of the opt-out registers in which natural person might register themselves(art.7(2)). The 2002 Privacy Directive divides the obligations of the marketers depending on the legal personality of the receiver (natural or legal person): an opt-in mechanism when the e-mail address belongs to ***natural persons*** (art.13(1) and 13(3) in accordance with art.13(5)), and a different regime, as chosen by the Member States (art.13(5)), for ***legal persons***. As hybrid between the opt-in and the opt-out regime, the rule commonly referred to as ***soft opt-in***, distinguishes further between the type of relations that exist between the marketer and the prospected customer (art.13(2)).

Therefore, the dilemma of a marketer conducting businesses on-line and wishing to start a targeted advertising campaign through e-mail, consists first of all in determining which of the two directives to follow so as not to suffer the consequences arisen from being labelled a spammer.

Following the **E-Commerce Directive**, a marketer will be bound to the jurisdiction that applies to him[43], with the associated controversies regarding the meaning of the phrase "established on its territory" and the associated risks of forum shopping.

The E-commerce Directive imposes on the Member States the obligation to ensure that the customer has the opportunity to request the termination of commercial communications by subscribing to an opt-out list. Bear in mind however that these registers ought to be set only for natural persons that object to receiving such contents in their inbox.

Secondly, a marketer should "regularly" check for the opt-out registers mentioned above (art.7(2)). The question that arises is how thorough is this control expected to be? The legislator chose regularity as a criteria, but a check-up scheduled every six months according to self determined rules of practice is just as "regular" as a check-up done before every marketing campaign, although they are the expression of different levels of diligence from the marketer. Since the expected outcome of this safeguard is to make sure the wishes of the customer are respected, what is truly relevant here is neither the time frequency not the pattern-like occurrence, but the "*bona fides*" behaviour of the marketer in making sure that his commercial message does not conflict with an express wish of the customer.

43 according to article 3(1) of the E-Commerce Directive

Reflecting the preoccupation for gaining and enforcing consumer confidence in e-mail marketing, the E-commerce Directive imposes also transparency obligations on the marketer, regarding both the commercial character of the e-mails and the identity of the business sending them. Section 2 of the Directive and especially article 6 instantiate the "transparency requirement" hinted at in Recital 29 of the same Directive. *In concreto*, all commercial communications should be "*clearly identifiable as such*"[44], specify the person (legal or natural) whose products or services are being advertised[45], and clearly state any special conditions(promotions or offers, competitions or games) that are associated with the products or services being advertised[46]. These are general, basic conditions to be fulfilled by any commercial communication, solicited, or unsolicited by the customer (for example when a former client asks the firm to communicate him updated information about related products or services, as well as when, during an ongoing business relation, one of the parties communicate to the other some new services that it just started to provide). Although not explicitly targeted at spam messages, the provisions in article 6 tackle two of the most common features of spam: the disguised commercial character and the forged sender information. The requirement is restated in art. 7(1) that deals directly with unsolicited commercial communications.

Having presented the E-commerce Directive mechanism addressing the unsolicited communications, I will direct my attention to the relevant provisions of the 2002 Privacy Directive.

The new[47] rules regarding unsolicited commercial e-mails make a basic distinction between the commercial e-mails sent to natural persons and the commercial e-mails sent to legal persons.

The first rule requires the marketer to obtain prior and informed consent of the natural person targeted (art.13.1) before the sending of the first message. Similarly, a separate consent needs to be obtained for any secondary uses of the e-mail address obtained[48]. The natural person should also be given the possibility to stop at any point in time, free of charge and in an easy manner, further commercial communications.

The second rule concerns "subscribers other than the natural persons" (art.13(4)) whose "legitimate interests" have to be sufficiently protected in this respect (unsolicited commercial communications). The provision is rather

44 article 6(a)
45 article 6(b)
46 articles 6(c) and 6(d)
47 The former Privacy in Telecommunications Directive (97/66/EC) had in art. 12 opt-out rules for unsolicited commercial e-mails, similar to the ones in the E-Commerce Directive.
48 Such as selling or renting the e-mail address to a third party.

broad and unclear, since no further guidance is provided on relevant issues such as: what legitimate interests are being referred to in the context, what are the criteria that serve in the assessment of the "sufficiency" of protection, whether or not unincorporated companies, or structures without legal personality (such as daughter companies or virtual organizations), as well as sole traders should be included under the umbrella of "subscribers other than the natural persons" *Ad litteram* they should, as these entities are not and do not accomplish the functions on a natural person, but Member States have found different solutions to steer clear of the ambiguities in the European text.

Four examples will serve my purpose of illustrating how different the national implementation of the Directive can be:

Due to the provisions of article 19 (3) of the Basic Law (Grundgesetz) [49], in Germany the same level of protection was awarded to both natural and corporate e-mail addresses.

In UK[50], the term "individual subscriber" was interpreted broadly so as to include not only natural persons, but also "unincorporated partnerships and sole traders", in the first case because the unincorporated partnership is not a legal person, in the second case since the legal and the natural person coincide. In other words, it is forbidden to send commercial e-mails in the absence of informed and specific prior consent not only to e-mail addresses belonging to natural persons, but also to business e-mail addresses in the two mentioned situations.

In Belgium[51], it is possible to send unsolicited commercial communications to addresses like info@company.be or customer.services@company.be or contact@... office@..., as long as, according to the circumstances, it is obvious that they belong to a legal person.[52]. Contrarily, once a company creates to its employee business addresses like name.surname@company.be , the address is to be considered as belonging to a natural person, despite its use for business related communications. It is the marketer's responsibility to appreciate in each case, before sending the commercial e-mails, what kind of address (belonging

49 http://www.datenschutz-berlin.de/recht/de/bdsg/summary-gutachten.pdf , page 2, (last visited, August 1, 2005)

50 see further, http://ico-cms.amaze.co.uk/DocumentUploads/New%20rules%20on%20email%20marketing.pdf (last visited, August 1, 2005)

51 According to the "Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique", 4.04.2003, published in the MONITEUR BELGE- BELGISCH STAATSBLAD on 28.05.2003, page 29292" http://www.iab-belgium.be/Media/pdf/kb040403.pdf (last visited, August 1, 2005)

52 "Des publicités non sollicitées par courrier électronique peuvent être envoyées à ces adresses, dans la mesure où, en raison des circonstances, il est manifeste que ces adresses concernent des personnes morales"

to a natural or a legal person) is the one targeted, and the evidentiary burden (with regard to applicability of this exception) rests on him. One additional and essential condition is that a marketer is not allowed to send unsolicited commercial communications to legal persons in order to advertise products and services addressed actually to natural persons[53].

The fourth and the last example is the French approach. Following negotiations between the CNIL and the representatives of the direct marketers in France, in a decision in 17th of February 2005, CNIL ruled that natural persons can receive commercial e-mails without their prior consent on their nominative professional e-mail addresses if these unsolicited e-mails are related to the function they fulfil within the company[54]. In other words, the director of informatics systems within a company can receive "special offers" for hardware on its nominative business e-mail address, but not offers for summer vacations on some exotic islands.

The third rule in the 2002 Privacy Directive (article 13.2) deals with existing business relations, involving both natural and legal person subscribers. Basically, marketers that obtained the e-mail addresses from their customers can continue to use them for sending commercial e-mails advertising their own similar products and services. Similar safeguards regarding the possibility for the customer to object to the communication should also be provided.

This short description of the two mechanisms introduced by the European legislator as a legal tool to shield the Member States in the fight against spam already highlighted some of the discrepancies. My goal is to explore the possibility for them to aggregate into a unitary solution, if this possibility exists, or to underline the contradictions that prevent them to become such unity.

The two mechanisms have certain features in common:

First of all, they both use the term "unsolicited communications", and expressly (E-commerce Directive) or implicitly (2002 Privacy Directive) refer in terms of the content only to the commercial communications. As such, they regulate a larger sphere of behaviours that if they would have to address only spam and not legitimate e-mail marketing as well. At the same time, only part of the content commonly associated with spam is covered, since as I mentioned in

53 "En outre, les produits ou services offerts à travers les publicités ainsi envoyées doivent viser des personnes morales, et non des personnes physiques. En effet, un annonceur ne saurait se prévaloir de l'exception pour envoyer à des adresses de personnes morales des publicités visant en réalité des personnes physiques, contournant ainsi l'obligation de solliciter le consentement préalable de ces dernières"

54 Les personnes physiques puissent être prospectées sans leur accord préalable à leur adresse électronique professionnelle, «au titre de la fonction dans l'organisme (…) que leur a attribué cette adresse.

the Introduction, spam e-mail messages are only in part commercial in nature, but can include political, religious, humanitarian and illegal material (viruses, child pornography).

Secondly, they both outlaw the sending of commercial e-mail messages when the identity of the sender or of the person on whose behalf the sending is done is hidden or disguised (article 6 (b) of the E-Commerce Directive and article 13(4) of the 2002 Privacy Directive). Both the interest in gaining client confidence and the privacy interest on having insight on the identity of the data processor justify and are well served by this requirement.

Thirdly, they both reveal the need to look after the manifested wishes of the potential receiver, although the manner of expression and the role of such manifestation differ.

Somehow surprisingly, this is about all the two legal texts have in common. The rest of the provisions, when they are faced one against the other, reveal either cross references or contradictions.

The first cross reference is again related to the terminology used in the two directives. The E-commerce Directive contains in article 2(f) the definition of "commercial communications" and it seems that although the 2002 Privacy Directive does not expressly refer to the E-commerce Directive, it uses the term alike. The same can be said about the term "direct marketing" used by the Privacy Directive in both the text of article 13 and in the related Recitals (41, 42, 43, 45). Although the Recitals mention some of the features of the direct marketing, such as the low costs involved in sending those (40), some media through which the direct marketing message can be conveyed, no definition is provided.

The second cross reference concerns the level of protection awarded to legal persons. A partial reference is made in Recital 45 of the 2002 Privacy Directive, to those States that would chose to set up an opt-out register for **legal persons,** that they should apply the provisions in article 7 of the E-Commerce Directive. Again, the terminological reference is misleading, since the scope of the terms "legal person" (Recital 45) and "recipients other than natural persons"(article 13(4)) is different.

The broadest cross reference between the two texts is to be found in article 7 of the E-Commerce Directive, stating that the provisions found in the E-Commerce Directive are "without prejudice to Directive 97/7/EC and Directive 97/66/EC". This is an indirect reference to the 2002 Privacy Directive, as it mentions the former Privacy Directive (Directive 97/66/EC), that was repealed

by the 2002 one[55]. In this context, given the fact that the 2002 Privacy Directive changed in the most part the content of the provisions referring to unsolicited commercial communications, it is questionable if the reference can still be considered valid. Taking into account the opposition to the current Privacy Directive in the business circles, as well as the incompatibility that would result from the application of both provisions, it is my opinion that the reference can no longer be seen as justified.

The E-Commerce Directive does not address however the issue of the initial collection of the e-mail addresses by the marketers and does not distinguish further regarding the different types of business relations that the marketer and the targeted e-mail address owner might be in. Although the references to "other requirements established by Community law"[56] (additional to the E-commerce Directive provisions) cannot be ignored, still it is my opinion that some rules regarding the initial collection of the e-mail addresses should have been also included in a directive aiming to set up the general framework in which e-commerce activities are supposed to take place. These rules could have referred not to the issues pertaining more to personal data protection, but at least to the sources from where the collection of the e-mail addresses can occur. All the more reason to instantiate the rules for unsolicited commercial communications to the possible pre-existing relations between the service provider and the receiver: is the receiver a customer already? Is it a visitor to the website, who provided the e-mail address just in order to take part in a competition? Is he simply an Internet user with whom the marketer had no previous contact? Of course, all of them are granted the general right to opt-out to receiving commercial communications, however such an instantiation would still provide useful guidance to the marketers as to how to behave in order not to be associated with a spammer

From the point of view of the content, the E-Commerce Directive does not include even a general obligation for the marketers to personalise the content of the commercial e-mails sent according to the receiver's profile, although such a distinction is claimed[57] to exist between the legitimate direct marketing and spam.

These deficiencies are partially covered by the 2002 Privacy Directive, at least at the level of express provisions, still the role they accomplish and the

55 According to article 19 of the 2002/58/EC Directive: "References made to the repealed Directive shall be construed as being made to this Directive"

56 Article 7(1), E-commerce Directive.

57 See the ICC Code of Conduct.

values they serve are different from the ones likely to be found in an E-commerce Directive.

The 2002 Privacy Directive introduces the notion of "informed, prior consent" of the receiver as the only factor legitimizing the sending of commercial e-mails. Therefore as opposed to the E-Commerce Directive, an e-mail marketer risks being labelled as a spammer from the first message sent without a clear manifestation of consent[58], and not at a later point when it overlooks the wishes of an end-user.

The 2002 Privacy Directive also changes the manner in which the natural persons can object to and stop further commercial e-mails as well as the actors involved. In the E-Commerce Directive, it was the Member State's obligation to set up easily accessible registries in which the natural persons could register their objection. The marketers had only to make sure they check them "regularly". According to the rules in the 2002 Privacy Directive the objection is to be sent directly to the marketer (through unsubscribe links) and has to be handled by the marketer himself.

It is unclear how the Privacy Directive envisages the functioning of an opt-out registry for legal persons and what rules would apply regarding timeliness of the recordings, the authority of the mother company to decide over the commercial e-mails received by the daughter company or the situation of the business entities lacking legal personality.

To sum up and answer the question in the title of this subsection, I find little grounds to consider the provisions in the two directives as representing one legislative solution in the fight against spam, but rather as being two separate parts of a legal framework that is supposedly in place to deal with spam.

2 Fitness for the purpose

Without doubt, the opt-in regime introduced by the 2002 Privacy Directive changed some of the provisions of the Directive 97/66/EC that proved inefficient in the fight against spam. It attempted and partially succeeded in unifying the legal regime applicable all throughout Europe bringing a plus of legal certainty. Previously, through making use of their autonomy to chose either an opt-in or an opt-out[59] regime for unsolicited communications[60], the Member States fragmented the unity of the legal market failing to reach a common

58 Clearly a point found objectionable by the majority of marketers

59 See an overview of the option of the European countries between opt-in /opt-out regime in May 2002 at http://www.euro.cauce.org/en/lchaos.html (last visited 20 Aug. 05).

60 According to article 12 of the Directive 97/66/EC.

anti-spam approach. Therefore, the behaviour of the same marketer pursuing an e-mail marketing campaign and targeting e-mail holders without their prior consent, could have been regarded at the same time as spam in his own country (if that country implemented the opt-in regime) and a legitimate marketer in countries that implemented an opt-out regime. Additional difficulties were raised by the impossibility to link sometimes the e-mail address to a certain country and by the difficult detection of the right opt-out register to check.

At the same time, the newly introduced opt-in regime addressed the issue of the initial collection of the e-mail addresses, one of the problems commonly associated with spam. The previous opt-out regime legitimised the sending of the first commercial e-mail. It represented a weak defence against spam, as the commercial e-mail, once sent and received by the end-user, rarely allowed for subsequent removal (and the activation of the unsubscribe link, if present, did nothing more than confirming the address as valid, thus leading to more spam). At the same time, the opt-out regime placed additional burden on the end-user, making him responsible to stop the flooding of his address with unwanted mail (so he had to spend time and energy both in removing the existent unwanted content, and to take action to stop further messages). As the role of the end-user changed following the introduction of the opt-in regime (he is now the initiator of the commercial dialogue), it has become arguably easier to set the anti-spam filters to let in only the content that was expressly and knowingly agreed by the user.

The opt-in targets also the uselessness of the spam messages. It is improbable that the user will give his prior and informed consent to something that he might later on claim as useless, and in any event, a legitimate marketer, as opposed to a spammer, would have a defence and a justification for having sent that particular content to that particular e-mail address, through stating the circumstances in which the consent was asked and received.

By changing the procedure through which the end-user manifests his will not to receive further commercial e-mails and relying not a third administrative party but the two parties involved (the sender and the receiver), the provisions in article 13 created a standard requirement for the inclusion of a workable opt-out link[61], considering that most spam messages do not allow the receiver to refuse receiving the spam e-mails. Of course, a good point regarding the prohibition of disguised or concealed sender identity was maintained in the intention to outlaw the practice used by spammers to hide their tracks either by using a third party e-mail address as an alleged sender address or to use a fake address and abandon it immediately after.

61 As reflected in the existing FEDMA and ICC Codes of Conduct.

The most important critique that can be brought to the current anti-spam legal provisions is that they attempt to treat two separate activities as being one and the same. The definitional inconsistency called for the compromise solution of the soft opt-in as a way to alleviate the concerns of direct marketers regarding regulatory overkill. In my opinion, a clear definition of both terms ("commercial communication" and "direct marketing") would have been of increased importance, especially since official documents use the term "spam" as being synonym with "unsolicited commercial electronic mail" with reference to article 13 of the 2002 Privacy Directive[62], but attention, documents issued before and after 2002, by the marketing associations set clear parameters distinguishing the two activities. In this context it seems misguided to borrow the terminology from one context and try to fit it into another while changing the scope of the activities comprised therein.

The effect of this inconsistency of approach is best reflected in the different regime applicable to the commercial e-mails sent to legal persons. An approach consistent with the stated synonymy between spam and unsolicited commercial communications would have justified one single regime for both natural and legal persons. Several reasons concur to my opinion:

While the difference in regime between business-to-business and business-to-consumer relations if well founded in general[63], businesses and consumers alike suffer the negative consequences of spam, and the legal personality is absolutely irrelevant from the spammers' point of view. The definition of spam does not relate the spam features with the legal personality of the potential receiver. Therefore, an opt-in regime for legal persons would have condemned the spam in general as business practice and as illegal personal data processing no matter to whom the e-mail addresses belongs, considering the overall detrimental effect[64] and not associate it solely to the "distress" caused to the individuals.

Since the European legislator did not provide a clear distinction between e-mail marketing involving also unsolicited commercial communications and spam, using instead the etiquette neuter terms consecrated by the business practice and literature, special cautions were required in order not to short-circuit legitimate communications that are intrinsic to the e-commerce practice.

62 COM(2004) 28 final.

63 Being a reflection of the more general principles of equity and the protection of the contractual weaker party.

64 "Spam has negative impacts for consumers, businesses, Internet Service Providers (ISPs), legitimate e-mail marketers and virtually anyone else who uses e-mail for any reason ", Cristina Bueti "ITU Survey on anti-spam legislation worldwide" (July 2005), available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf

To sum up, the European anti spam solution seems to be, for the most part, an appropriate tool against spam as it tackles some of the most important features of the commercial communications that can be regarded as spam. However, the definitional issues and the inconsistency regarding the level of protection for legal persons cannot be overlooked.

Conclusions

The provisions that are supposed to represent the European anti-spam legislative tool are scattered throughout various Directives whose applicability is called by unclear references. SUA, Japan, Australia to give just a few examples, have enacted special legislation to deal with the particular issues involved by spam. In Europe, however, it seems that general principles of data processing, 3 articles dealing with the unclearly defined notion of "unsolicited commercial communications" and several provisions dealing with consumer protection are supposed to provide the national enforcement authorities[65] with sufficient legislative guidance in order to ensure an efficient fight against spam[66]. This option translates in fact in supplementary difficulties in identifying the relevant provisions as well as in finding the way they fit in a "Lego" like framework.

It cannot be ignored that the E-Commerce Directive and the 2002 Privacy Directive establish different regimes for unsolicited commercial communications. In this situation, either we consider that the provisions of article 7 of the E-Commerce Directive have been implicitly and partially abrogated by the enactment of the 2002 Privacy Directive[67], and they remain in force only in what regards the legal persons[68], or they are both in force and refer however to different business practices[69].

---

65 Either courts, or administrative bodies such as consumer protection authorities or data protection units (see the Anti-Spam Law Enforcement Report (May 2005), OECD, available at http://www.oecd.org/dataoecd/18/43/34886680.pdf (last visited 21 August 2005) for a list of authorities with responsibilities for enforcement of laws related to spam.

66 I am not questioning the role of the codes of conduct, what is in focus now is the legislative answer.

67 this idea seems to be conveyed by the First Report on the Application of the E-Commerce Directive (COM(2003) 702 final) which states that "*the issue of unsolicited commercial communications via e-mail has now been dealt with at Community level by Directive 2002/58/EC*" (section 4.3)

68 See Recital 45 of the 2002 Privacy Directive.

69 Surprisingly, the idea is conveyed by COM(2003) 702 final, stating that the issue of unsolicited commercial communications is being dealt with now by the 2002 Privacy Directive, as this issue has "increasingly become a problem for consumers and business alike" , see page 10.

There are legitimate grounds to believe that the provisions in article 7 of the E-commerce Directive, as much as they contain divergent points from the 2002 Privacy Directive, are still in force and a relevant piece of the framework. First of all, although the 2002 Privacy Directive repeals expressly Directive 97/66/EC, it refers to the provisions of article 7 of the E-Commerce Directive without questioning their validity. Secondly, international fore [70] treats the E-Commerce provisions as a piece of the European anti-spam answer.

Other reasons relate more to the circumstances in which the Directive was enacted. Gauthronet and Drouard (2001)[71] argue that the European anti-spam legislation was "a reaction to American privacy issues" and "the relevant law was in place before the phenomenon ever emerged in Europe", while "the research conducted for this study reveal that Europe has not yet experienced an acute outbreak of unsolicited commercial e-mail or of spam".

If this is the case, the provisions in E-commerce Directive can be seen as a general framework[72] stating the expected behaviour of all the marketers that do send unsolicited commercial communications and not a spam targeted norm per se. On the other hand, article 13 of the 2002 Privacy Directive is seen as a "victory" in the fight against spam[73].

It is this "victory" that I question.

Due to article 4 of the Directive 95/46/EC, the provisions of the 2002 Privacy Directive (and therefore the opt-in rules) do not apply when the data controller is not established in a Member State or does not make use of equipment located in a Member State. Therefore, the solution found by the European legislator does little to protect the end-users from the spam coming from outside the European Union, which according to some studies[74] accounts for the most part of spam.

Several impediments that prevent the European response to spam to become an appropriate tool to be used in annihilating spam have been identified above. They relate to definitional inconsistencies, to clashes between legal

70 http://www.itu.int/osg/spu/spam/legislation/legislation_europeanunion.html.

71 See Serge Gauthronet & Etienne Drouard, op.cit, at 82, "Unsolicited commercial communications and Data Protection", January 2001.

72 See Recital (10) of the E-Commerce Directive stating "In accordance with the principle of proportionality, the measures provided for in this Directive *are strictly limited to the minimum needed* to achieve the objective of the proper functioning of the internal market…"

73 "We Did It! ***EU Parliament "Opts In"*** Commercial Email in ***European Economic Area*** will not be allowed without ***recipients' prior consent***, states the European Coalition Against Unsolicited Commercial Email , http://www.euro.cauce.org/en/index.html (last visited 20 August 2005). It is relevant that the quoted source considers unsolicited commercial email (UCE) as being "more commonly known as "spam"".

74 See for example ITU survey (2005), op.cit.

texts equally applicable, to differences in regime not justified by the practices involved in spam and to the insufficient level of protection for the legal persons that become victim of this unethical, unfair and generally detrimental business practice.

De lege ferenda, the anti-spam normative solution could benefit from an explicit and coherent definition of the two different business practices: e-mail marketing and spam, and I believe the European legislator should not refrain from "calling things for what they are", instead of using the unclear term of "unsolicited commercial communications".

Since the 2002 Privacy Directive is a norm designed to address spam, whereas the E-Commerce Directive can only be seen as a general framework setting the rules for the unsolicited commercial communications that cannot be qualified as spam, the soft opt-in rule would be better placed in the E-Commerce Directive than in the 2000 Privacy Directive. Spam appears only exceptionally in already existing businesses relations. At the same time it would send a signal to the e-mail marketers that they cannot abuse existing business relations and would make sure that the customer has a viable alternative to the aggressive practice of the spammers. Moreover, the privacy legislation in general does not instantiate different principles and levels of protection based on the existence of a business relation between data subject and the data controller.

Similarly, unifying the legal anti-spam provisions applicable to both natural and legal persons would first of all reflect better the business reality that spam does not discern between the e-mail addresses of the individuals and those of businesses, and secondly would relate the banning of spam not only to the emotional distress caused to the individuals but to the overall costs and negative consequences that impinge on the Internet communications in general.

I do believe that legislation is a powerful mechanism and a guarantee that non-pecuniary values such as equity, autonomy, privacy, non-discrimination are protected. I can see several reasons why the market should not be permitted to set alone the "price" of personal information, absent all regulatory constraints.

First of all, there will always be an information asymmetry between customers and marketers, which will prevent the formers to perceive the real level of privacy intrusion made possible by the current technology as well all the uses to which different pieces of personal information could be put – rational factors that can contribute to identifying the true value of the personal data disclosed.

Secondly, privacy is threatened by the aggregated effect of small violations, therefore the privacy preferences of the individual might be different for a particular intrusion and for privacy as a whole.

Thirdly, most individuals view privacy as a long term, abstract gain, whereas the benefit resulted from personal data disclosure is usually tangible and immediate. This again prevents an equitable remuneration for the disclosure, and only an illusion of informational self determination.

Quite normally, the legislation is only part and parcel of a broader range of measures targeted against spam. Co-regulation, the use of self-regulatory mechanisms in order to translate the general normative rules into more detailed codes of conduct, may respond better to the complexities of spam then if only laws would be relied on.

However, even the most detailed rules of conduct cannot supplement the pro-active involvement of the end-user himself. No one would argue that being a part of the "off-line" society means learning a series of preventive conducts and not relying only on laws guaranteeing the protection from various wrongs caused by the others. Similarly, actions aimed at raising awareness about the threats and the reasonable behaviour when exploring the "on-line world" can only be in the interest of the users. This is probably where future efforts of the international and national bodies alike should be directed more in the future, especially considering the increasing number of Internet users worldwide.

* * *

This article was written in January 2006 and it summarizes the results of the research that I carried out for the completion of the Master thesis in Information and Communication Technology Law at the University of Oslo, 2004-2005.

CONTRACTUAL RISK MANAGEMENT IN AN ICT CONTEXT – SEARCHING FOR A POSSIBLE INTERFACE BETWEEN LEGAL METHODS AND RISK ANALYSIS[1]

Tobias Mahler and Jon Bing

Introduction

In Richard Susskind's book *The Future of Law,*[2] 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 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 questions 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

---

1 An earlier version of this paper was published in the Scandinavian Studies in Law Volume 49, A Proactive Approach, edited by Peter Wahlgren, Stockholm Institute for Scandinavian Law, 2006, p. 340-357. Reprinted with kind permission of Peter Wahlgren.

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

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.

Motivation

The phrase "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 to direct and control an organisation with respect to "risks" of a nature to be specified.[3] 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, negative effects on the 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 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).[4] 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.[5] It has been stated that legal risk methodologies "are in their infancy, compared to technical and commercial risk methodologies."[6]

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

3 ISO, *Risk management – vocabulary – guidelines for use in standards,* Guide 73, 2002, definition 3.1.7.

4 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).

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

6 Burnett, Rachel, *Legal risk management for the IT industry*, Computer Law & Security Report (2005) 21, p. 66.

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[7] 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[8] or contracts.[9] Focusing on compliance may require certain risk management methods, which may differ 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

7 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.

8 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.

9 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.

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"[10] 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).

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:[11]

- 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).

This can also be resented by a simple flow diagram:

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

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

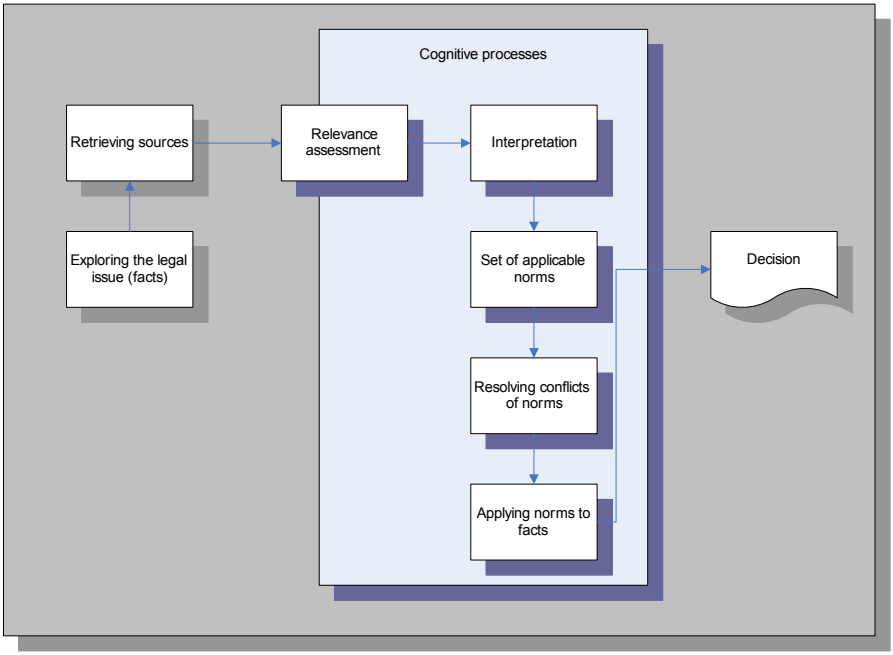


Figure 1 – Legal decision process

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[12] 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 statures 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.[13] Hyperlinks will be part of the retrieval tools, enhancing the traditional way of linking sources through citations.

The sources will typically be texts.[14] 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.

---

12 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.

13 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.

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

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 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.[15] 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.[16]

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.[17] 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

15 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.

16 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.

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

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.

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

Taxonomy

The term "risk management" can be defined according to the vocabulary for risk management in standards, provided by the International Organisation for Standardisation.[18]

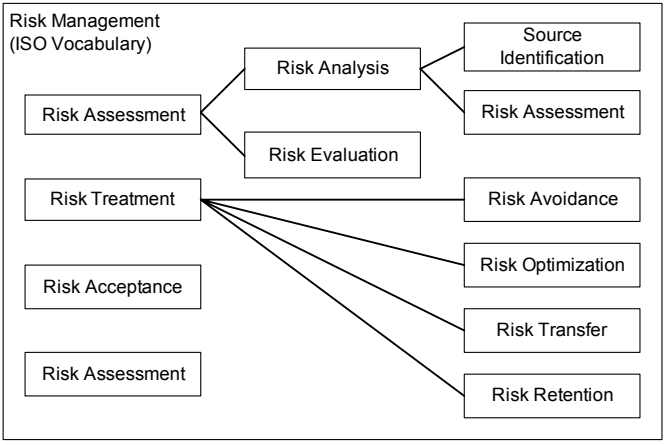


Figure 2 – ISO risk management vocabulary

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

Risk management is understood by the ISO[19] 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.[20] The risk value is thus calculated based on the probability and the consequence values. A closer analysis of this and other definitions of risk will have to determine whether this definition is appropriate for the legal domain.[21] 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;
- 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.

Risk management literature does not always use the above terms consistently. In particular, many experts understand the term risk analysis much broader, i.e. to include also risk evaluation, acceptance and treatment. Hence, risk management may also be conceptualized as a continuous process that involves many risk analyses, which each include all or most of the elements presented above. In this paper we utilize this wide understanding of risk analysis.

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

19 ISO, *ibid*, definition 3.1.7.
20 ISO, *ibid*, definition 3.1.1.
21 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.

with respect to financial products and their interplay in portfolios.[22] 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.*[23]

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,[24] 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. Similarly, 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 0.

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

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

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

24 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.

introduces some of the current Scandinavian[25] legal 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 1960s and 1970s, also draws on the experience from preventive medicine.

Methods for legal risk analysis

Peter Wahlgren[26] 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.

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.[27]

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

25 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.

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

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

Legal Risk Management

Iversen[28] 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.[29] 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

28 Iversen, Jon, *Legal Risk Management,* Thomson, Copenhagen 2004.
29 Iversen, Jon, *ibid*, p. 85.

which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined."[30] 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:

- 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.

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:[31] 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 effective-

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

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

ness 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[32] and corporate governance, the two concepts do not contain major contradictions.

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 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.

32 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.

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.

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.

Terminology

The terminology 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 with 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 manage risks with respect to (1) legal risks and (2) other risks that can be "treated" by legal means.

The phrase legal risk could be utilized in a wider sense to include any risk in which the event involves the application of a legal norm. However, such a definition may cover too many risks with only remote relation to legal norms. Therefore, we should establish a notion of legal risk in a narrower sense where we require that the norm in addition has to have a significant impact on the risk value. This is illustrated in the UML class diagram[33] in Figure 4. The norm's significant impact on the risk level means that the existence of the norm contributes to an increase in likelihood or consequence value, or both. This is to say that without the norm, the risk value would be significantly lower.

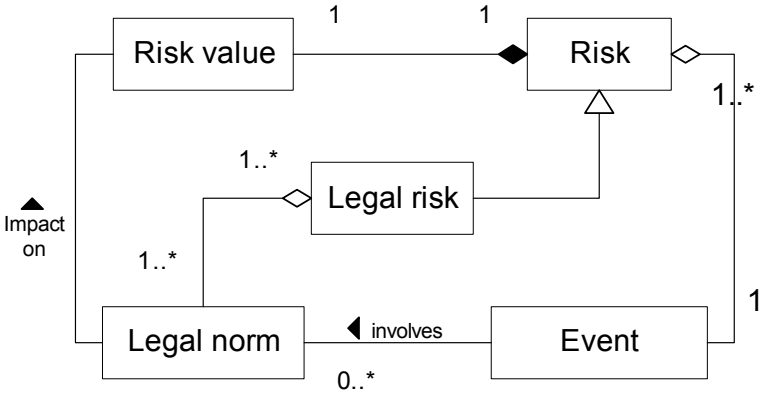


Figure 4 – Legal Risk

33 The Unified Modelling Language (UML) is the *de facto* standard modelling language for information systems and can be used for modelling hardware (engineering systems) as well as for business process modelling, representing organisational structure, and systems engineering. A class diagram describes the types of objects in a system and the various kinds of static relationships that exist among them, cf. Fowler, Martin, *UML Distilled: A brief Guide to the Standard Object Modeling Language*, 3rd edition, Addison-Wesley, Boston et al., 2004.

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 "risk" is in the ISO vocabulary defined as the combination of probability of an [unwanted] event to occur, and its consequences.[34] 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 risk management. So far, proactive reasoning about probabilities – in particular quantitative calculations – is rather unfamiliar for lawyers.[35]

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. As mentioned above, this includes the identification of legal risks as defined above.

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 legal risks is at least partly 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 legal risks.

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

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

35 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 http://www.worldhistory.com/wiki/P/Prosecutor's-fallacy.htm.

Data Protection Act, Section 9, personal data can only be processed under certain conditions. If the conditions are not met, the processing is unlawful. Unless this has direct negative consequences, this rule alone does not imply a legal risk. Nevertheless a legal risk may follow from other norms.

When drafting a contract we should however also take other risks into account. As an example, consider that a particular set of business data could be 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. a legal rule. 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 legal and other risks (since these may justify certain contractual provisions). Both can be identified at different levels.

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

A methodology for legal risk management should facilitate a structured analysis at all of these levels for both legal and other risks. 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.

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 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 legal risk through non-legal remedies, e.g. an improved IT system.[36]

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 also used for business process modelling, representing organisational structure, and systems engineering modelling.[37] 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.

36 *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.

37 See for an introduction to the UML http://en.wikipedia.org/wiki/Uml.

The CORAS language is an extension of the Unified Modelling Language (UML version 2.0).[38]

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 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

38 *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.

methodology and language can be used to support legal risk analysis.[39] 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.

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 multidimensional problems. Hence, a legal risk management methodology that focuses on information flows needs to be directed towards the legal domain,

39 Mahler, Tobias and Fredrik Vraalsen, *Legal Risk Management for an E-Learning Web Services Collaboration*. In: Sylvia M. Kierkegaard (ed.): Legal, privacy and security issues in information technology - volume 1. Proceedings of the First International Conference on Legal, Privacy and Security Issues in IT (LSPI), held in Hamburg, Germany, 30.04.2006 - 02.05.2006. Oslo: Complex 2006 (3): 503-523. 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, p. 69-79.

but it should also support an interdisciplinary approach, which is necessary in the context of risk management and information law.

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. We would like to thank the members of the ENFORCE project for valuable comments.

DETERMINANTS FOR DATAFLOW

NORM AND ACTION: CAUSATION IN LAW, AND CAUSATION FROM LAW TO ACTION

Georg Philip Krog

How law may be a determinant for cross-border circulation of intangible data and communicational behaviour in global computer networks will in the following brief note be elucidated by the rules of international adjudicatory authority. Consider the following.

If, on the one hand, a legal relationship arising from cross-border circulation of intangible data in global computer networks is disqualified to count as a member of a sovereign State's adjudicatory law system, the parties inherent to the legal relationship may disobey the law without sanctions, and may therefore feel free to carry out actions or omissions even though they logically either are prohibited, obligated, exempted or permitted.

If, on the other hand, a legal relationship arising from cross-border circulation of intangible data in global computer networks is qualified to count as a member of a sovereign State's adjudicatory law system, intelligent individuals who are assumed to have the capacity to control their conduct, are invited to carry out their actions or omissions in accordance with the law, or may disobey the law and be subject to adjudicatory authority, coercive sanction and possibly some form of liability.

Hence, the source for statements about causation from law to action differ depending on whether the legal relationship is qualified or disqualified to count as a member of a sovereign State's adjudicatory law system.

I shall give some general remarks on how the rules determining the international adjudicatory authority of sovereign States´ courts may be the cause for and determine the circulation of intangible data and people's conduct.

One must inquire how a legal relationship can be qualified or disqualified to count as a member of a sovereign State's adjudicatory law system and subject to its adjudicatory authority. This question requires the structure of legal causal statements to be clarified and separated from issues of legal policy.[1] Questions

1 This does not imply that causal connections established in accordance with these criteria are sufficient for a legal relationship to become a member of a sovereign State's adjudicatory law system, since other criteria may be necessary as well.

pertaining to causal notions as determinant of international adjudicatory authority require clarification and identification of the structure of legal causal statements for the relation between 1) the object of action and the factual basis of the cause of action, 2) the object of action and the legal basis of the cause of action, and 3) the cause of action and the forum. The law may construe these relations in a number of combinations and by different types of causal relationship where verifying the existence of causal connection may involve counterfactual speculation to determine that an individuated act or omission was at least a sine qua non.[2] The degree required for the strength of the cause is a matter of legal policy.

Furthermore, one must inquire how a person strategically may construe her activities along legal statements of causal notions in order to qualify or disqualify her activities to count as a member. This question requires one must first seek to clarify whether it is possible to make a causal statement about the logic for how transmission and retransmission of data come about or is prevented in the computer network, its component parts and their interconnections. Second, this causal description of data transmission may be insufficient to define the causal relation between communicants and the result of their relation, that of which they relate in and have related to each other, which in turn signify change or preservation of various positions in relation to various interrelational and informational aspects of time, quality and quantity. An appropriate characterization of the relation between communicants and their sequence of action and reaction may need to be supplied with deontic logic. The direction of behavioral events may exhaustively be characterized by the theory of normative positions upon which one may formulate a complete characterization of all possible normative positions of obligations and permissions of the persons involved, not only the single agents, but also relations between agents, in order to investigate the normative relations between two agents, or between agents and States´ law systems By doing so, communicants may secure and ensure themselves of clear, precise and certain direction of behavioural events within the sphere of or delimited to a selection of territorial connections to the exclusion of other potential connections.

This completes my quick and incomplete look on how law, elucidated by the rules of international adjudicatory authority, may be a determinant for cross-border circulation of intangible data and communicational behaviour in global computer networks.

2 Such as e.g. initiation of physical sequences, the provision of reasons or opportunities for action.

Why rules on international adjudicatory authority are the starting point for such a determination, I shall succinctly state in abbreviated form.

In the following I shall explain how the agent's uncertain normative position is a pre-condition for and gives the agent the incentive to determine her normative position within the framework of a consistent set of normative instructions.

How these rules may affect dataflow and behavior is difficult to grasp due to the complexity of the component parts of the rules and their connections. However, the connections between the component parts must be presented in a certain order.

Determination of normative positions

For so long as there is no uniform and exhaustive norm-system of common rules on international adjudicatory authority, separate and distinct from national procedural rules, different sovereign States´ norm-systems may concurrently attribute adjudicative authority over the same legal relationship.

In turn, the sovereign States´ norm-systems have adopted separate and distinct legal norms[3] where upon the resolution of any given court litigation has the prospect of different outcomes, and hence, legal uncertainty as to an agent's normative position.

For this reason, the facts and the rule of law relied on as the basis of any action may, through constitutive rules, be classified to count as a member of the term provided for in the antecedent of the rule regulating the adjudicatory authority of a norm-system (jurisdiction *ratione materiae*).[4]

In turn, cclassification of the facts to count as a member of the antecedent is necessary for a court to assert whether the facts may be qualified as having a relevant connection to the place provided for in the consequent.[5]

3 E.g. lack of national procedural rules, rules *of service abroad of legal documents*, substantive law, rules of conflicts of laws, rules governing the admissibility of an action, *rules on the moment of session of a case, rules on recognition and enforcement of judgments etc.*

4 The norm-systems may concurrently reject the legal relationship from being a member of any norm-system conferring adjudicative power since the facts and the rule of law relied on as the basis of an action may, through constitutive rules, not be classified to count as a member of the term provided for in the antecedents (jurisdiction *ratione materiae*).

5 The norm-systems may concurrently decline adjudicative competence to a court at the place provided for in the jurisdictional consequent since the facts (classified to count as a member of the antecedent) may be qualified as not having a relevant connection to the place provided for in the antecedent.

In turn, qualification of the facts to have a relevant connection to the place provided for in the consequent is necessary for a court to attribute adjudicatory authority over the legal relationship.[6]

Concurrent[7] classification of the facts to count as a member of a multiplicity of norm-systems´ respective adjudicatory antecedents, and concurrent qualification of the facts to have a relevant connection to the place provided for in the adhering consequents of the respective antecedents (positive conflicts of competence) is *necessary* and may be the cause for a plaintiff to initiate[8] court proceedings in parallel proceedings before different States´ courts against a defendant for the same cause of action and object of action (forum-shopping) [9], and thus necessary and the cause for courts to attribute adjudicative authority over the same legal relationship (competing competence).[10]

A multiplicity of competent courts concurrently empowered by the plaintiff's initiation of parallel court proceedings before different States´ courts to give or deprive effect to something is necessary and the cause for the competent courts to select the applicable law (*lex causae*) in accordance with the rules of conflicts of laws in lex forum.

The selection of different applicable laws to determine the subject-matter is necessary and the cause for the object of the legal relationship, to which the plaintiff seeks to give or deprive an effect, logically either will be prohibited, permitted or free [11] by way of what legal consequences the normative positions established or created in the respective judgements entail.

The situation of a multiplicity of competent courts in the same legal relationship, parallel proceedings before the courts of different States with differing applicable laws in accordance with each competent and adjudicating courts´

---

6 Inaccessibility to justice for the plaintiff to assert his alleged rights, and, on the other side, lack of necessity for the plaintiff to arrange for his defence, and finally for the legal relationship as such, the non-production of a norm in which the legal relationship potentially could be a member.

7 In general, the legal basis of sovereign state power to adjudicate may be either self-imposed by a state, voluntarily accepted agreements between states, or imposed on a state from a supranational authority.

8 The norms conferring adjudicative power in civil proceedings do not impose themselves on their own account. Thus, the court is not empowered to initiate court proceedings itself and seize the case on the basis of its own initiative.

9 Some norm-systems coordinate the exercise of judicial functions in such a way that adjudicative competence is delimited to one court. This may also occur within a norm-system.

10 If all norm-systems are inapplicable (negative conflicts of norm-systems), the same legal relationship is independent of all courts (negative conflicts of competence).

11 In relation to an incompetent court, the action or omission is free. This does not imply that his actions and/or omissions are free to carry out since they may be regulated, but simply implies that a court will not adjudicate them.

rules of conflicts of laws, and separate enforcement of each judgement, either in the forum state or another state than the forum state, is necessary and the cause for judgments to establish or create irreconcilable normative positions entailing mutually exclusive legal consequences which logically either are prohibited, permitted or free (conflicts between decisions).

Conflicts between decisions are necessary and are the cause for the parties´ legal uncertainty and coordination problems, i.e. which courts are competent? Which laws apply? Which laws is the action or omission in breach of or accordance with?

The agent's uncertain normative position is a pre-condition for and gives the agent the incentive to achieve the fundamental object to avoid or preclude, to the greatest extent possible, a multiplicity of competent courts in the same legal relationship, fragmentation of proceedings by parallel proceedings before the courts of different States and conflicting decisions entailing mutually exclusive legal consequences.

Subsequently, the investigation of how a person in relation to the rules of international adjudicatory authority ex ante can develop and provide an easily identifiable action plan to qualify or disqualify herself to count as a member of a sovereign State's adjudicatory law system, and there upon secure herself of legal certainty of normative positions, can only reliably and reasonably be identified by clarifying the structure of legal causal statements separated from issues of legal policy. Upon clarification of legal causal statements, the person can activate or abstain from activating, or permit or prohibit, facts which the law system will qualify to count as relevant legal causation.

PREVENTION IS BETTER THAN CURE: FOSTERING THE GROWTH OF DYNAMIC NETWORKED ORGANISATIONS THROUGH THE USE OF PROACTIVE LEGAL MEASURES

Emily M. Weitzenböck[1]

Introduction

With the growth of information and communications technology (ICT) – not least the Internet – new forms of communication and entrepreneurial co-operation are emerging. Networked organisation, strategic web, strategic/co-operative alliance, virtual organisation: these are but some of the different terms used to describe the novel forms of economic organisations.[2] ICT facilitates speedy, instantaneous collaboration among businesses irrespective of geographical boundaries. It enables everyone – from freelancers, small and medium-sized enterprises to larger businesses to participate in temporary or even longer-term networks. Through such collaboration, the partners pool together their resources and expertise, thus becoming capable of offering a common service to the customer that each of them individually would not otherwise have been in a position to do.

An important feature of these dynamic networked organisations is the underlying basis of trust between the individual partner firms that together form the organisation. Such organisations are built upon trust and function effectively only as long as there is trust between the different partner firms. Nevertheless, a number of fundamental issues need to be discussed and resolved between the partners such as how risk and liability are to be apportioned

1 This paper was first published in Vol. 49 of the Scandinavian Studies in Law series on "A Proactive Approach", pp. 305-318, published in May 2006. It is based on two reports – "The VE Interchange Agreement" and "VE Model Contracts"- written by the author within the framework of the ALIVE project funded by the European Commission (IST-2000-25459). Needless to say, this paper does not represent the opinion of the European Commission and the European Commission is not responsible for any use that might be made of the content of this paper.

2 Holland, C.P., *The importance of Trust and Business Relationships in the Formation of Virtual Organisations*, in Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998, Simowa Verlag Bern, p. 55.

between them and who owns intellectual property rights to any works created by their collaboration. For these flexible, networked organisations to function, there must be established and accepted between the partners a set of standards – the "rules of the game" – that will govern the transactions between the partners in such organisation and usually laid down in a contract. This is discussed further in section 0 of this chapter.

Very often, the business partners do not specifically or consciously aim or intend to create a new legal person to carry out the tasks of the collaborative network. However, as is examined below in section 0, irrespective of the intentions or wishes of the partners, some jurisdictions may hold that such a co-operating venture would constitute a partnership. The partners need to be aware of the potential repercussions and consequences of such an eventuality.

The aim of this paper is to suggest proactive measures to obviate future difficulties and disputes among partners in such business collaborations. It should be noted that many of these measures are appropriate not just for temporary collaborative networks as described above, but also for other more long-term collaborations.

Contractual issues

The negotiation stage

Once a business opportunity has been identified, the business promoter determines the various competencies required to develop the product or service to be provided. Businesses that have the required competencies are then identified and evaluated and the business promoter starts preliminary discussions with them. Mutual interest increases, details begin to be discussed and the parties gain a sense of enthusiasm and urgency. However, risks to the negotiating parties exist even at this precontractual stage. Parties may already need to disclose commercially sensitive information, including intellectual property, at the negotiation stage. This information is likely to constitute the life blood of the respective business, especially where such business is a small or medium-sized enterprise. A business may be reluctant to make such a disclosure to a negotiating group which may include competitors or potential competitors. Moreover, the business promoter may also fear that a negotiating party may leave the group and set up his or her competing team to bid for the business opportunity, and may thus be unwilling to disclose extensive details about the business opportunity or the optimal team he/she has in mind, before there are additional legal safeguards in place.

Precontractual liability

It should be borne in mind that an important tenet of civil and common law contract law is that parties should be free to decide whether to enter into contractual relations or to choose not to enter into contractual relations, i.e. to break off negotiations at any time.[3] However, what happens where one of the negotiating parties suddenly and without reason breaks off negotiation or where a party never had an intention to contract at all? What happens where, because of certain blameworthy conduct of a negotiating party at the precontractual stage, the contract is invalid or not perfected?

Some jurisdictions do provide a remedy. A number of civil jurisdictions such as Germany and Italy developed the doctrine of *culpa in contrahendo* which is based on the notion of good faith. As a consequence of the *culpa in contrahendo* doctrine, damages should be recoverable against the party whose blameworthy conduct during negotiations for a contract brought about its invalidity or prevented its perfection in any of the following situations:

i. where there is a sudden and unjustified rupture of negotiations,
ii. where the contract is not concluded because one of the parties had no real intention to contract. [4]

In such cases, the court takes into account whether the other party had incurred expenses in the preparation and in the expectation of concluding the contract.[5]

In English law, according to many writers, there is no general rule requiring the parties to negotiate in good faith.[6] This does not mean that there is

3 Cohen describes the former as "the positive freedom of contract" in that the parties are free to create a binding contract reflecting their will, and the latter as "the negative freedom of contract" which means that the parties are free from obligations so long as a binding contract has not been concluded. *See further* Cohen, N., *Pre-contractual duties: Two freedoms and the contract to negotiate*, in Beatson, J. and Friedmann, D. (ed) Good Faith and Fault in Contract Law, Clarendon Press, Oxford, 1995.

4 Kessler, F. and Fine, E., *'Culpa in contrahendo', Bargaining in Good Faith and Freedom of Contract: A Comparative Study*, Harvard Law Review 77(3):401-449, 1964.

5 *See* Weitzenböck, E.M. *Good Faith and Fair Dealing in Contracts Formed and Performed by Electronic Agents*, in Artificial Intelligence and Law Vol. 12 Nos. 1-2, 2004, Springer, Netherlands, 2005, p.83-110.

6 *See further* O'Connor, J.F., *Good Faith in English Law*, Ashgate Publishing, Limited, 1990, and Whittaker, S. and Zimmermann, R., *Good faith in European contract law: surveying the legal landscape*, in Zimmermann, R. and Whittaker, S. (eds), Good Faith in European Contract Law, Cambridge University Press, Cambridge, 2000.

a free-for-all, with no controls on contracting parties.[7] The traditional rules proscribing duress, undue influence and fraud, still apply. Other than that, in English law, either party is entitled to break off negotiations at any stage before the final conclusion of the contract. Liability for pre-contractual behaviour is only imposed under limited circumstances such as fraudulent representation or negligent misstatement. In the case of a sudden and unjustified rupture of negotiations or where the contract is not concluded because one of the parties had no real intention to contract, common law judges have also ingeniously provided a basis for recovery, without entering into the notion of good faith, by using the different notions of collateral contact and restitution besides the law of torts as aforementioned. An important factor that the court usually gives weight to, is whether the party carried out works and incurred expenses in the preparation and expectation of concluding the contract, and the extent to which this was instigated or brought about by the other party which then suddenly broke off negotiations.[8] According to American jurists, similar to English law, the requirement of good faith in American law does not apply to contract negotiations.[9]

Thus, issues such as precontractual liability as abovementioned, good faith/fair dealing and confidentiality are to be borne in mind, as well as their different

7 As was held in *Interfoto Picture Library Ltd v. Stilletto Visual Programmes Ltd* (1989) 1 QB 433, 439, though "English law has, characteristically, committed itself to no such overriding principle … [it] has developed piecemeal solutions in response to demonstrated problems of unfairness."

8 In *Brewer Street Investments Ltd v. Barclays Woollen Co. Ltd.* ((1954) 1 QB 428), defendants were negotiating the lease of plaintiffs' premises and, in the expectation shared by both parties that a lease would be agreed, defendants had requested that the plaintiffs have certain work done on the premises which was otherwise of no benefit to them. The defendants had, however, expressly undertaken that they would be responsible for the cost of this work. However, before the work was completed, it became clear that the lease would not be concluded. Plaintiffs stopped work and sued for the amounts which they had paid to the contractors in respect of the work carried out. The Court held there was a contract between the parties for the carrying out of the work on the premises, despite the fact that there was no contract of lease concluded. Recovery was granted on the basis of a contractual 'quantum meruit', i.e. a reasonable sum for the work done (which was set at the amount which the plaintiffs had paid their contractors) as the defendants had agreed to pay for the cost of the work. *See further* Weitzenböck, E.M. *op. cit.* n. 280.

9 The Uniform Commercial Code (UCC) provides in section 1-203 that "[e]very contract … imposes an obligation of good faith in its performance or enforcement." This is mirrored in §205 of the Restatement of Contracts Second which states that "[e]very contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement." Good faith is defined in the UCC (§1-201(19)) as "honesty in fact in the conduct or transaction concerned". In the case of a merchant, the UCC (§2-103(1)(b)) provides that good faith means "honesty in fact and the observance of reasonable commercial standards of fair dealing in the trade."

treatment in civil and common law systems. The negotiating parties, including the business promoter, should exercise caution especially where the negotiating parties are established in different jurisdictions, with the chance that behaviour that may be proscribed in one jurisdiction is permitted in another.

Letter of intent

One mechanism that the negotiating parties may decide to opt for at this stage to protect themselves against precontractual risks such as breaches of confidentiality, competition and bad faith, is a letter of intent. A few preliminary comments on letters of intent are opportune at this stage.

The terminology regarding letters of intent varies. Some other designations of a letter of intent are "heads of agreement", "memorandum", "memorandum of understanding", "agreement on principles" and "aide-mémoire".[10] These documents may be very short or they may be around three to four pages long, depending on the details included. Whatever such document is called, a letter of intent is, in general, not intended to bind the parties signing it as regards the proposed final agreement, but is designed to indicate the likelihood of a contract being made in the future. However, it cannot be assumed that parties dealing on the basis of a letter of intent will not be contractually bound as regards the contents or some of the contents of the letter of intent itself. One would therefore need to study the contents and terms of the letter of intent and take the surrounding circumstances into consideration, to see if the parties are contractually bound and to what extent.

In England, it was held in *British Steel Corp v. Cleveland Bridge and Engineering Co Ltd*[11] that there were two possible types of contract that might arise following a letter of intent. The first type was an ordinary executory contract, under which each party assumed reciprocal obligations to the other; the second type was the so-called "if" contract, i.e. a contract under which A asks B to do something and promises him that if he does so he will receive something, usually remuneration, in return. The latter type is really nothing more than a standing offer which, if acted upon before it lapses or is lawfully withdrawn will result in a binding contract.[12]

---

10 Wolf, R.C., *A Guide to International Joint Ventures with Sample Clauses*, 2nd ed., Kluwer Law International, London - The Hague - Boston, 1999, p. 19.

11 [1984] 1 All E.R. 504.

12 *See further* the report on England by Allen, D.K., in *Precontractual Liability: Reports to the XIIIth Congress International Academy of Comparative Law; Montreal, Canada, 18-24 August 1990*, Hondius, E.H. (ed.), Kluwer Law and Taxation Publishers, Deventer – Boston, 1991, pp.139-141.

The most important issues that a letter of intent should address are the following:

1. **Objectives**: There should be a reference as to what the co-operation is about and what the proposed organisation shall do.
2. **Exclusive co-operation**: Another concern of each negotiating party is to ensure that the other firms that he is negotiating with will continue to co-operate and negotiate exclusively with him as regards the future project. The risks here might be that one of the other businesses might decide to join forces with third parties and bid for the project together with them rather than as part of the proposed networked organisation. Furthermore, one of the parties, such as the business promoter, could have already incurred some expenses in having identified the business opportunity and drawn up the work processes and structure – costs which might otherwise be difficult to recover.
3. **Non-competition**: This is linked with the above notion of exclusive co-operation. By disclosing information about the market opportunity, the business promoter may be exposing itself to the risk that some of the other negotiating parties will suddenly break off negotiations and decide to compete in that market.
4. **Confidentiality**: A major concern for the business promoter is that information disclosed to the other negotiating party regarding the business opportunity and the work processes, is kept strictly confidential. Similarly with regards to any other commercially sensitive information and intellectual property that may be disclosed by any of the parties at this stage. It is important that this obligation is also extended to the employees and sub-contractors of such party. This could be done by placing an obligation on this party to bind such other third parties (i.e. employees, sub-contractors, etc.) to whom it may need to disclose such information to, in turn, keep that information confidential. As regards employees, this could be a standard term in the employment contract. In the absence of such a standard clause, the employees should be bound in a confidentiality agreement which echoes the obligations specified between the business promoter and the other business (the employer).
5. **Negotiation in good faith**: Similarly, each business party will want to ensure that the other negotiating parties act in accordance with good faith and fair dealing with a view to eventually reach a definitive agreement. In particular, the promoter will want to ensure that none of the other negotiating parties is merely pretending to negotiate (in order to discover sensitive commercial information) and has no real intention to contract.

6. **Costs**: Mention should also be made as to how the costs and expenses in connection with the preparation and conclusion of the agreement contemplated in the letter of intent are to be split between the parties, e.g. each party could bear its own costs, or costs could be shared between the parties, etc.
7. **Duration**: A date should be set by which the final, definitive agreement is to be reached.
8. **Jurisdiction and choice of law**: Though the parties may be based in different jurisdictions, the ease of communication through ICT facilitates cross-border collaboration. However, if a dispute were to arise, it may be difficult for a court seized of the matter, to determine whether it has jurisdiction to hear the case and, if so, which law is to be applied to resolve the dispute, in the absence of express jurisdiction/arbitration and choice of law clauses.

Although a letter of intent is not usually meant by the parties to bind them to reach a final, definitive agreement on issues that are still subject to negotiations and which may still need to be clarified, the negotiating parties may still desire certain parts of the letter of intent to be binding, irrespective of whether a final, definitive agreement is reached or not. This is because of the important commercial/business implications and repercussions that may ensue where such a final, definitive agreement is not reached – in particular where important confidential information has been disclosed. Hence, for example, the need for binding clauses regarding matters such as disclosure of confidential information and the exclusive nature of the co-operation. Moreover, a number of the provisions of the letter of intent should also survive the expiration or termination of the letter of intent itself, e.g. duty of confidentiality, intellectual property protection.

The operation stage

Where negotiations are fast and concluded swiftly, there is likely to be no need for a written preliminary agreement. Nevertheless, issues such as competition between the parties, intellectual property protection and confidentiality – crucial questions during the precontractual stage – should also be regulated between the parties during the operation of the networked organisation. As abovementioned, for flexible, networked organisations to function, there must be established and accepted between the partners a set of standards – the "rules of the game" – that will govern the transactions between the partners in such organisation and usually laid down in a contract.

Of course, these issues need to encompass the stage of operation of the networked organisation as well as what happens after termination and dissolution of the organisation. For example, with regards to intellectual property, the parties should distinguish between intellectual property which pre-existed the networked organisation but which is made available by the owning contracting party to the organisation (through a mechanism such as licensing, etc.) and intellectual property that is developed, found, produced or made by any party in the course of the collaboration. The parties may also wish to have the right to licence the latter type of intellectual property to a subsidiary or third party. In such a case, they should agree beforehand on the main licensing terms such as, for example, whether there should be payment of a licensee fee.

Similarly, just as exclusivity regarding the scope and object of the collaboration should be ensured between the partners during the negotiation stage, it is also important to be safeguarded during the operation of the networked organisation. This helps to foster the relationship of trust between the partners. However, where the collaborative organisation is made up of partners who together have a significant market share, care should be taken not to be construed as a cartel under competition laws.[13]

Another important issue that needs to be regulated between the parties is dispute settlement. Since trust plays such a crucial role in the proper functioning of dynamic networked organisations, there should be an effective dispute settlement mechanism in place from the creation of the collaborative organisation. For example, as a first stage there could be a mechanism for the amicable settlement of a dispute (such as mediation in front of an expert in the field) failing which, the dispute would be submitted either to arbitration or to the ordinary courts. There is much to be said in favour of arbitration as a dispute settlement mechanism as opposed to proceedings in front of the ordinary courts of the land. Arbitration is likely to be faster, less costly and more conducive to maintaining a good co-operating spirit among the partners (as opposed to a belligerent, adversarial spirit). Moreover, the parties may also select an arbitrator who has experience in their field of business.

The parties should also discuss and agree on the operation and management of the collaborative network, and who is to represent the collaboration with

13 For example, Article 81 of the Treaty establishing the European Community proscribes "all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the common market, and in particular those which: (a) directly or indirectly fix purchase or selling prices or any other trading conditions; (b) limit or control production, markets, technical development, or investment; (c) share markets or sources of supply; …" OJ C325, 24 December 2002.

clients or other third parties. One should remember that while corporate joint ventures operate against the backdrop of rules laid down by statute and the courts, the draftsman of an agreement establishing a collaborative enterprise has to make express provision for the internal running of the organisation.

The parties should also agree on the methods to be used for electronic data exchange and communication. This could be done in a technical annex to the main contract (and therefore also having binding force) and should contain matters such as details of the technology to be used, if and what kind of data should be signed by an electronic signature and what kind of electronic signature should be used, and the procedure to be followed when sending and receiving electronic messages: when is a message to be deemed to have been sent and received, whether there should be acknowledgement of the receipt of a message, etc.

Another critical issue is how risk and liability are to be governed and apportioned among the parties. Different measures may be used to govern liability:[14]

a. contractual instruments: The parties should discuss and consider including in their agreement (i) how third party claims on one partner for actions or omissions of the organisation are to be handled and the rights of recourse that such partner may have on the other partners; (ii) how the grounds of internal allocation of liabilities on the basis of a claim for recourse are to be made such as, for example, in accordance with the allocation of benefits for the distribution of profits, or in proportion to the investment made by each partner, or in accordance with the actions of that partner and thus, the possibility it had to avoid the damage from occurring.
b. the establishment of a voluntary reserve fund by the networked organisation to be used as a guarantee or otherwise as a means of building trust both in the internal relations between the partners and in its relations with third parties. However, one should be aware of possible tax or accounting implications according to the relevant national laws of the individual partners. The parties should also determine how such an asset is to be controlled and by whom.
c. exploiting the legal identities of the individual partners: The unlimited liability that may fall upon each partner for the debts and obligations of the organisation is, of course, limited to the total property of such partner.

14 *See further* Pöyhönen, Juha & Lönnfors, Mirja, *ALIVE Project Deliverable D12: Liability and Insurance* (Rev. 3 dated 07/07/2002) available at http://www.vive-ig.net/projects/alive/docs.html (last visited 14 October 2005).

> Thus, where a partner is a limited liability company, its liability is limited to the total property of that company.

The above discussion highlights the most important issues that should be agreed between the collaborating partners. They should form the basic framework upon which the collaboration will work. However, there should not be too much regulation between the parties so that the creation and functioning of such flexible dynamic networked organisation would not be stifled.[15] Indeed, some business authors have questioned whether dynamic organisations such as virtual enterprises should be based on a contract.[16] The real question here, it is believed, is not whether there should be a contract or not, but whether there should be a written contract (as opposed to a verbal one) since the parties should have already, at least verbally, agreed on certain crucial terms when setting up the organisation or business alliance (such as the objects, pooling and sharing of resources, some form of profit sharing, etc.). The difficulty with verbal agreements is an evidentiary one and arises when there is a dispute between the parties. Thus, it is suggested that there should be a written contract setting out the framework terms for the collaboration.[17] Such a contract should not seek to be too detailed with regards to the actual collaboration – in any case, it is often impossible to know beforehand all the minute details of the tasks. If the contract tries to be too detailed, it might be

15 Some model clauses were developed in the EU-funded ALIVE (Advanced Legal Issues in Virtual Enterprise) project to give negotiating parties intending to set up a collaborative networked organisation a starting point on which to draw up their framework agreement. See the project website at http://www.vive-ig.net/projects/alive/ (last visited 14 October 2005). The EU-funded project Legal-IST (www.legal-ist.org/ - last visited 14 October 2005) looked *inter alia* at some legal issues related to SME clusters and professional virtual communities.

16 For example, Jägers *et al* have held that contracts are too restrictive on the flexibility of a virtual organisation. See Jägers, H., Jansen, W., Steenbakkers, W., *Characteristics of Virtual Organizations*, in Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998, Simowa Verlag Bern, p. 73.

17 This is also the view expressed by Odendahl, Reimer and Marzen who explain that the concept of virtual enterprises is based on trust by definition and therefore it would initially appear that a legal framework does not have to be considered. However, these authors continue that the application of such a culture of trust in practice has proved to be a problem, and the culture of trust is opposed to the temporary character of a virtual enterprise because trust can only arise over a certain period of time. See Odendahl, C. and Scheer, A.-W., *The Concept of Virtual Enterprises and its Relevance for the Maritime Domain*, in Guedes Soares, C., Brodda, J., (eds.), Application of Information Technologies to the Maritime Industries, Edições Salamandra, Lisbon, 1999. A similar view is expressed by Pletsch, A. *Organizational Virtualness in Business and Legal Reality*, in Organizational Virtualness: Proceedings of the VoNet Workshop, April 27-28, 1998, Simowa Verlag Bern, p. 86.

interpreted restrictively on the basis of its specific terms and conditions rather than flexibly in the light of its purpose.

Partnership law issues

As mentioned in the introduction, in most cases the business partners do not specifically or consciously aim or intend to create a new legal person to carry out the tasks of the collaborative network. Indeed some of the partners may believe that their co-operation on the basis of a mere contractual or verbal agreement would definitely exclude the application of partnership and company law (with their concomitant duties and obligations) to their co-operation. However, as is examined below, irrespective of the intentions or wishes of the partners, many jurisdictions hold that such a co-operating venture could constitute a partnership, and a number of such jurisdictions even hold that such a venture is a separate legal person distinct from its members. Following is a brief look at what happens under English, Swedish and Norwegian law when a general partnership is deemed to have been created.

In English law, the question whether a partnership exists is a mixed question of law and fact.[18] The intentions of the parties are not conclusive in determining whether their relations amount in law to a partnership. Thus, if the statutory conditions for the creation of a partnership are fulfilled, the parties will be treated as being in the relation of partners to each other, even though they may assert an entirely contrary intention.[19] Nor can the parties to a consortium agreement or other contract prevent a partnership arising by a declaration that they are not partners. In *Pawsey v. Armstrong*,[20] Kay J. observed that:

"there are certain legal relations which are entered into by agreeing to certain conditions, and when those conditions are agreed to, it is quite idle for people to superadd, or attempt to superadd, a stipulation that the necessary legal consequences of these conditions shall not follow from the arrangement. In this case, supposing it was proved to my satisfaction that there had been a stipulation that the two persons were not to be partners, I could not regard that as altering the legal relation which they have entered into by making this contract."

18 See *Spicer (Keith) Ltd v. Mansell* [1970] 1 All ER 462.

19 See further on this Linklaters & Paines with Nightingale, C., *Joint Ventures*, 1st ed. Longman, London, 1990, pp. 22 *et seq*.

20 (1881) 18 Ch D 698.

This was supported in *Adam v. Newbigging*[21] and, in *Fenston v. Johnstone*,[22] a partnership was found to exist notwithstanding an express declaration that the agreement between the parties should not constitute a partnership.

What are the repercussions where a partnership has been deemed by a court to have been constituted by the partners, even though the latter may have expressly declared the contrary? Under English law,[23] if a collaborative network is deemed to be a partnership, each partner would be treated as an agent of the firm and its other partners for the purposes of the business of the partnership, and every partner who does any act for carrying on in the usual way of business of the kind carried on by the firm of which he is a member binds the firm and his partners, unless the partner so acting has in fact no authority to act for the firm in the particular matter, and the person with whom he is dealing either knows that he has no authority, or does not know or does not believe him to be a partner.[24] Moreover, each partner would be jointly liable with the other partners for all the debts and obligations of the firm.[25]

In Sweden, where a simple partnership ("*det enkla bolaget*") is deemed to have been created, the rights and obligations which arise during the activities of that partnership are the rights and obligations of the individual partners. A contract that is concluded for the partners or under a designation referring to the partners jointly entails contractual rights and obligations only for the partner(s) who has (have) entered into the contract.[26] However, although this is the main rule, certain circumstances may vary it. Thus, if a proxy (which may be given either in writing or orally) was given by another partner, such partner (the mandator) would also be liable. In Swedish law, a proxy may also develop through conduct showing that someone accepts another person as his legal representative through conclusive conduct.[27] If, on the contrary, a trading partnership ("*handelsbolaget*")[28] is deemed to have been set up by

21 (1888) 13 AC 308.

22 (1940) 23 TC 29.

23 The operative law on partnerships in England is the Partnerships Act 1890. The Act does not confer legal personality on the partnership. The partnership is the aggregate of partners who share profits, have individual authority to bind the firm for transactions in the course of business and are ultimately liable to the extent of their personal fortunes for the debts of the partnership.

24 Section 5, UK Partnerships Act.

25 Section 9, UK Partnerships Act.

26 Swedish Partnerships Act, chapter 4, section 5.

27 See Hemström, *Corporations and Partnerships in Sweden*, Fritzes, Stockholm, 1995, pp. 115.-116.

28 The difference between a simple partnership ("*det enkla bolaget*") and a trading partnership ("*handelsbolaget*") is that the latter is intended to engage in business activities in its own right and is a legal person.

the partners, such partnership will be liable for its own debts, since it is a legal person. However, all the partners would also be jointly and severally liable for the debts of the partnership.[29]

It is interesting to note that the Swedish Parliament, in connection with the adoption of the Partnerships Act 1980, discussed in some length one special kind of cooperation, viz. when a number of enterprises enter into a consortium agreement for a special project. Such consortia are sometimes to be characterised as simple partnerships, sometimes – according to earlier rules – as trading partnerships. According to Hemström, in the parliamentary legislative process the following four questions were pointed to as decisive for delimitation purposes in this connection:

> *"are the activities of the different members of the consortium mainly of the same kind as their normal activities, are the activities of the consortium limited to one project and not intended to continue indefinitely, are the different members of the consortium visible in relation to third parties – do they all, for example, sign all contract documents in connection with the project – and do the parties to the consortium agreement use their own personnel and machinery? If all these questions can be answered in the affirmative, a comprehensive view would probably show that the activities connected with the project were not those of a trading partnership but of a simple partnership … But if the answer to one or more of the questions is no, it is sometimes likely and sometimes certain that it is a matter of business carried out in common."*[30]

In Norway, where a general partnership (*ansvarlig selskap* - ANS) is deemed to have been created, each partner is personally liable *in solidum* for all the debts and liabilities of the partnership. However, a creditor must first claim against the partnership. If payment is not made within 14 days from such claim, then the creditor can claim directly from the partners.[31] General partnerships in Norway are legal subjects[32] and can thus have rights, obligations and appear in front of the courts and other authorities. This status is deemed to be acquired

29 Partnership Act, chapter 2, s. 20.

30 See Hemström, *op. cit.* n. 302, p. 114.

31 See §2-4(2) of the Norwegian Partnership Act 1985 (*lov om ansvarlige selskaper og kommandittselskaper*, 21.06.1985).

32 See also R. Knoph, *Knophs oversikt over Norges rett*, 11th ed., Universitetsforlaget Oslo, 1998, p. 33 which provides that organisations and institutions can have rights such as, for example, partnerships, associations, etc.

when the partnership agreement has become binding according to the law[33] and not by registration.[34]

This brief comparative study highlights an important issue. Different national laws may treat the same issue differently and the parties need to be aware of the consequences of this different treatment in order to be able to evaluate and address the risks appropriately. For example, as discussed above, whereas a partner who does any act for the carrying on of business of the kind carried on by the partnership is presumed under English law to bind the firm and the partners, under Swedish law a partner in a simple partnership is presumed to bind only himself. Among the proactive measures that could be taken is insurance. The parties could check whether it is possible to take out an insurance policy to cover potential liabilities of the networked organisation. In the event that this is not possible, each party should try to exploit its own firm's standard insurance policy. Another measure that could be taken is the use of a limitation of liability clause in contracts with third parties to put a cap on the liability towards such third parties.

Concluding remarks

Business collaboration grows and networked organisations prosper as long as there is trust between the collaborating firms. To foster trust, legal knowledge and proactive legal measures should be applied before things go wrong. This paper has discussed the importance of and need for proactive measures during the setting up and operation of networked organisations, such as the use of legal documents of various kinds, in particular letters of intent and contracts. It has also highlighted how overriding, mandatory provisions of national partnership and/or company law(s) could become applicable and the repercussions these provisions would have on the collaborative networked organisation, so that the collaborating parties could take the appropriate steps to minimise and/or contain risks of potential liability. In conclusion, skills, practices and business procedures can be developed to secure a strong legal basis for the business. Litigation is thus avoided or minimized and the parties would have a clear set of "rules of the game" that should be followed.

33 §2-3 Norwegian Partnership Act 1985.

34 See Woxholt, G., *Selskapsloven: Kommentarutgave*, 5th ed., Ad Notam Gyldendal, Oslo, 1998, p. 78. According to Norwegian law, all partnerships – whether general or limited - should be registered. This is not a complex matter to accomplish and, in the case of general partnerships requires certain information to be filed (See *Foretaksregisterloven*, §3-4 and §3-7). Failure to register a partnership is punishable with a fine. The partnership agreement must be in writing (§2-3, first paragraph, Partnerships Act).

FORMUERETTEN I MØTE MED NY TEKNOLOGI

Olav Torvund

Innledning

Noen hevder at den informasjonsteknologiske revolusjonen som skjer rundt oss vil medføre større samfunnsmessige endringer enn boktrykkerkunsten og den industrielle revolusjon. Jeg skal ikke gå inn i den diskusjonen, men nøyer meg med å konstatere at endringene er betydelige. Ingen sektor er uberørt av denne utviklingen, heller ikke retten. I denne artikkelen vil jeg se på noen av de utfordringer vi står overfor innen formueretten.

Teknologiens kjerneegenskaper er at store datamengder kan lagres, gjenfinnes og bearbeides, og ikke minst at data kan overføres over store avstander. Data kan lagres og formidles uavhengig av en fysisk databærer. Vi kan overføre data uten av vi samtidig må transportere papir eller andre fysiske medier.

Data lagres i digital form. Det vil si at alt representeres i form av tall. Tallene er representert i binær form, hvilket vil si at alt er representert i form av ett-tall og nuller. Disse tallene kan selvfølgelig representere tall, men de kan også representere tekst, lyd eller bilder. Når alt er representert i form av tall betyr det også at alle data kan bearbeides ved matematiske metoder, for eksempel for kryptering. Ved at alle data er representert i samme form kan også alle data bearbeides, lagres og overføres ved hjelp av det samme utstyret og i det samme nettverket.

Når data overføres gjennom telenettet skjer det ingen forflytting av data fra et sted til et annet. Det overføres signaler fra avsenderens datamaskin som representerer de data som overføres, og ved hjelp av disse signalene fremstilles en kopi hos mottaker – eller det fremføres lyd eller bilde, omtrent som ved radio- og fjernsynssendinger. Dette gjør det langt enklere å overføre data over avstand, men det betyr også at vi må gi slipp på den forutsetning at det et eller annet sted finnes en "original", om vi skulle ha behov for noe slikt.

Informasjon i vid forstand har fått økt betydning. Dette kan være underholdningsinformasjon som film og musikk, styringsinformasjon i form av datamaskinprogrammer, forretningsinformasjon, personinformasjon, osv. Informasjon er et formuesgode.

Når dette har fått økt betydning og større økonomisk verdi, medfører det også at informasjon oftere vil være gjenstand for rettslig regulering eller rettslige

konflikter. Den retten som knytter seg til informasjon og informasjonshåndtering, så som opphavsrett, har fått en stadig større betydning.

Men alle transaksjoner er også informasjonshåndtering, fram til en eventuell fysisk levering. Rettigheter og plikter er abstrakte størrelser, og er i transaksjoner kun representert i form av informasjon. Når man tar i bruk en annen teknologi endres også informasjonshåndteringen i transaksjonen. Det er disse endringene og de rettslige konsekvenser av disse endringene som skal behandles nærmere i det følgende.

I mange tilfeller vil også selve oppfyllelsen være en informasjonstransaksjon. Det kan være overføring av for eksempel en lydfil eller et dataprogram. Men vel så ofte vil det bare være en melding om at de data som er registrert i et informasjonssystem er endret. Når vi får beskjed fra banken om at vår konto har blitt godskrevet eller belastet et beløp, så ser vi ingen ting til pengene. Vi får bare meldinger om endringer i bankens bokføring.

Avtaler

Er avtale inngått elektronisk bindende?

Jeg vet ikke hvor mange ganger jeg har fått dette spørsmålet. Enhver jurist vet at slike avtaler – i alle fall som hovedregel – vil være bindende. Når man godtar at bindende avtale om salg av et høyfjellshotell kan inngås ved en noe uklar telefonsamtale, da er selvfølgelig en avtale sluttet ved utveksling av e-postmeldinger også bindende.

Men at svaret på et litt feil stilt spørsmål er enkelt, betyr ikke at spørsmålene rundt elektroniske avtaler kan parkeres som løst. Vår oppgave som jurister er ikke bare å svare på de spørsmål som blir stilt, men å finne fram til og stille de relevante spørsmålene.

Vi har ingen generelle formkrav som vilkår for at avtaler er gyldige etter norsk rett. Men det finnes en rekke eksempler på formkrav for bestemte avtaletyper. For ganske mange avtaler er det et vilkår at de skal inngås skriftlig. Et eksempel er en kontoavtale med en finansinstitusjon, se *finansavtl § 16(1)*.

Når man møter slike krav blir spørsmålet om formkravene kan oppfylles ved hjelp av elektronisk kommunikasjon. Det følger av *finansavtal § 8(2)* at krav om skriftlighet etter denne loven som hovedregel kan oppfylles ved bruk av elektronisk medium, på visse nærmere angitte vilkår. I forarbeidene til loven sies bl.a. følgende om spørsmålet:[1]

1 *Ot.prp. nr 41 (1998-99)* avsnitt 7.1

"Departementet vil likevel understreke at man etter omstendighetene kan forstå et krav om skriftlighet utelukkende som et krav om bruk av *skrifttegn*. I så fall vil et skriftlighetskrav kunne oppfylles også ved bruk av elektronisk kommunikasjon."

Etter denne bestemmelsen stilles det krav om at avtalen skal ha vært tilgjengelig på avtaletidspunktet og at man skal ha brukt en betryggende måte for å autentifisere avtalen. Det kan også stilles krav til for eksempel lagring av den avtale som er inngått slik at den senere skal kunne hetes fram.

Vi kan ikke alltid gå ut fra at skriftlighetskrav kan oppfylles ved elektronisk kommunikasjon, slik at spørsmålet må vurderes konkret. I *finansavtl § 61* er det bestemt at *§ 8 annet ledd* ikke gjelder for kausjonsavtaler. Så for slike avtaler må man fortsatt holde seg til penn og papir, eller noe tilsvarende. I forarbeidene begrunnes dette unntaket fra *§ 8* på denne måten:[2]

> *Et krav om skriftlig avtaleinngåelse kan være begrunnet også ut fra andre hensyn enn behovet for bevissikring. Det kan bl a pekes på at en ordinær papirbasert avtaleinngåelse kan gi partene mer tid til å vurdere avtalens innhold før de blir rettslig bundet gjennom undertegning. Avtaleinngåelsen vil som oftest strekke seg over en viss tid, og «alvoret» ved f eks en låneavtale blir understreket når kunden fysisk må innfinne seg i institusjonens lokaler for å undertegne avtalen. Det kan hevdes at man ved elektronisk avtaleinngåelse, der kunden på en enkel måte kan inngå avtalen hjemme eller på sitt eget kontor, kan risikere at de nevnte elementene ved avtaleinngåelsen i større eller mindre grad blir borte.*

I forbindelse med implementeringen av e-handelsdirektivet ble det foretatt en gjennomgang av norsk lovgivning for å legge til rette for bruk av elektronisk kommunikasjon – eller mer reelt: For å fjerne eventuelle bestemmelser som kunne hindre slik kommunikasjon.[3] Resultatet er at en lang rekke lover har bestemmelser med et innhold som ligner *finansavtal § 8(2)*. Men samtidig kan en slik revisjon paradoksalt nok ha medført at man lettere vil komme til at elektronisk kommunikasjon ikke vil oppfylle formkrav der dette ikke er uttrykkelig nevnt. Når man på de fleste områder har spesifikke lovbestemmelser om bruk av elektroniske kommunikasjon vil det være mer nærliggende å trekke en antitetisk slutning der slike bestemmelser eventuelt ikke finnes, enn

2 *Ot.prp. nr 41 (1998-99)* avsnitt 7.3

3 Resultatene av gjennomgangen, med lovendringsforlag på en rekke områder, finnes i *Ot.prp. nr 108 (2000-01)*.

det var i den perioden hvor spørsmålet kun var vurdert i forhold til finansavtaleloven.

Formkrav har imidlertid ikke bare betydning som gyldighetsbetingelser. Bruk av bestemt form kan også være et vilkår for å oppnå bestemte rettsvirkninger, selv om disposisjonen i seg selv er gyldig. Et velkjent eksempel er omsetningsgjeldsbrev. Hva slags form som brukes har ingen betydning for hovedforpliktelsens gyldighet og innhold. Men negotiabilitetsvirkningene forutsetter at man har benyttet en bestemt form.

Da *Verdipapirsentralen* ble etablert kunne man ha valgt å etablere et slikt system for obligasjoner (fordringer) uten å gjøre noen endringer i lovgivningen. Noen obligasjonsutstedende kredittforetak hadde allerede etablert sine egne systemer. Men da ville det ikke lenger ha vært omsetningsgjeldsbrev i form av ihendehaverobligasjoner som hadde blitt omsatt. Dette ville ha vært enkle krav. Fordringene hadde vært gyldige, og også enkle krav kan omsettes. Men man ville ha mistet negotiabiliteten. Det ville ikke ha vært en god løsning om de fordringer som faktisk blir omsatt i et marked skulle falle utenfor den lovgivning som er ment å skulle gjøre fordringene særlig egnet for å kunne omsettes på denne måten. Når det gjelder aksjer var situasjonen mer komplisert, og lovendringer var nødvendige.

Et annet eksempel er manuelle transaksjoner med debetkort. *Sjekkloven § 1* angir hva en sjekk skal inneholde. Sammenligner vi med den papirnotaen vi får man tar avtrykk av kortet med "strykejern", ser vi at det viktigste kravet som ikke er oppfylt er at dokumentet må benevnes som "sjekk". Hvis man hadde valgt å trykke dette magiske ordet på blankettene og gjort noen andre små endringer, ville disse transaksjonene ha fulgt sjekklovens regler. Når sjekklovens regler ikke er oppfylt får vi en transaksjon som er gyldig og bindende, men den faller utenfor denne lovreguleringen. At sjekkloven nok ikke ville være en særlig egnet regulering, er en annen sak. Det illustrerer likevel formens funksjon.

Sekundære formkrav

Vi kan også møte en rekke *sekundære formkrav*. Med dette mener transaksjoner som forutsetter at en annen transaksjon er foretatt i en bestemt form. I Norge er det ikke krav om skriftlighet ved avtaler om fast eiendom. En muntlig avtale, eller en avtale inngått ved utveksling av elektroniske meldinger, vil derfor være gyldig og bindende mellom partene. Men tinglysingen forutsetter skriftlig avtale, for det er bare dokumenter som kan tinglyses. Dermed blir det i praksis ikke mulig å gjennomføre en eiendomstransaksjon uten at man på et stadium i prosessen setter opp et skriftlig dokument.

Kort tid etter SAS i sin tid introduserte elektroniske billetter skulle en forsker ved et av våre forskningsinstitutter en tur til Stockholm. Siden e-handel var hennes forskningstema ville hun selvfølgelig forsøke dette i praksis, og bestilte elektronisk billett. Det meste gikk greit helt til hun skulle hjem. Da gikk hun den sedvanlige turen innom "Tax Free" butikken på Arlanda. I kassen ba de om hennes boardingkort. Hun forsøkte å forklare at hun reiste med elektronisk billett, og at hun derfor ikke hadde noe boardingkort. Men de måtte ha boardingkortet for å kunne selge henne varer, så hun måtte etterlate varene og reise hjem uten avgiftsfri kvote. Nok en gang var det sekundærtransaksjonen, som forutsatte at det var utstedt et dokument i hovedtransaksjonen, som skapte problemet. Men et system som hindrer at nordmenn får kjøpt sin avgiftsfrie kvote er sjanseløst i markedet, så det tok ikke lang tid før man hadde funnet en løsning på dette problemet.

Et sekundært formkrav med utilsiktede bivirkninger er *tvfbl § 7-2*. Etter denne kan et *gjeldsbrev* på visse vilkår være særskilt tvangsgrunnlag. En elektronisk melding eller innførsel i et register kan ikke være et gjeldsbrev. Det er derfor ikke mulig å gjøre en fordring eksigibel med mindre man bruker papir. Det innebærer for eksempel at fordringer registrert i Verdipapirsentralen ikke vil kunne gjøres eksigible.

Denne bestemmelsen har blitt en slags "Flyvende hollender" i forhold til å legge til rette for elektronisk kommunikasjon. Bestemmelsens forgjenger, *§ 3 nr 6* i de gamle tvangsfullbyrdelsesloven ble oversett da det ble utarbeidet lovgivning om Verdipapirsentralen på midten av 1980-tallet. Spørsmålet ble på nytt oversett da vi fikk ny tvangsfullbyrdelseslov i 1992. *Verdipapirsentralloven* ble erstattet av *verdipapirregisterloven* i 2002, men spørsmålet om eksigibilitet ble nok en gang oversett. Ikke i noen av disse tilfellene har man truffet noe bevisst valg om spørsmålet, det har ganske enkelt ikke blitt vurdert. Også ved den foreløpig siste korsvei, revisjon av lovgivning med sikte på å legge til rette for elektronisk kommunikasjon, slapp denne bestemmelsen unna. Tvangsfullbyrdelsesloven ble ansett som en del av prosesslovgivningen, og alle prosesslover ble holdt utenfor gjennomgangen. Prosesslovgivningen er under revisjon, så kanskje vil lovgiver en gang vurdere også dette spørsmålet.

Subjektive krav

Så lenge vi ikke gjør annet enn å endre kommunikasjonen mellom to personer, vil problemet stort sett gjelde formkrav. Om to personer utveksler meldinger pr e-post eller pr brev, betyr lite bare eventuelle formkrav er oppfylt.

Men ofte endres mer enn bare kommunikasjonsformen. Hvis et tilbud, for eksempel en bestilling, mottas og behandles i et automatisert system, når kom

da tilbudet til adressatens kunnskap? Det lar seg gjøre å fastslå når en melding har kommet fram. Men en datamaskin vet ingen ting. Det gir derfor ikke mening å spørre om når tilbudet kom til datamaskinens kunnskap. Vi kan komme rundt problemet ved å ty til fiksjoner. En mulighet er å si at løftet har kommet til "kunnskap" når det er registrert som mottatt i datasystemet, noe som i realiteten er å sette kunnskapstidspunktet lik mottakstidspunktet. Det kan også skyves noe, ved at systemet må ha begynt å behandle transaksjonen. Det vil også lett føre oss tilbake til det tidspunkt transaksjonen ble registrert, ellers vil vi stå overfor det ikke helt enkle spørsmålet om hvor langt prosessen må ha kommet får det inntrer "kunnskap". Vi kan også velge å ta regelen på ordet, og si at løftet ikke har kommet til kunnskap før mottaker eller en person som opptrer på mottakers vegne, har fått kunnskap om dette.[4] Hvis også oppfyllelsen er automatisert, slik den gjerne vil være i for eksempel finansielle transaksjoner, vil mottaker som regel aldri få kunnskap om transaksjonen.

Jeg skal ikke her gå inn i en diskusjon om tilbakekallelsesfristen ved transaksjoner som behandles automatisk. Jeg nøyer meg med å konstatere at det er et uavklart spørsmål, og at det i visse situasjoner kan ha avgjørende betydning for om man vil være bundet av en transaksjon eller ikke.

I avtaleretten kan det også være avgjørende om man har vært i god tro. Men det gir liten mening å spørre om hvorvidt en datamaskin er eller var i god tro. En datamaskin vet ikke, tror ikke og forstår ikke. Den tar alt bokstavelig og gjør det den blir bedt om, uansett hvor dumt eller urimelig dette måtte være.

Broene brister

En rettslig regulering vil i prinsippet alltid ha følgende form: Hvis [nærmere angitte vilkår er oppfylt] så [inntrer visse rettsvirkninger].

Alle som har forsøkt å lage en rettslig regulering har erfart at det kan være vanskelig å avgrense regelens anvendelsesområde. Man skal helst skjære ut et stykke av virkeligheten med kirurgisk presisjon, og knytte rettsvirkningen til dette presist avgrensede fenomenet. Vi skal inkludere alt hvor regelen skal anvendes, og utelukke alle de situasjoner hvor den ikke skal komme til anvendelse. I praksis er dette svært krevende, kanskje umulig. Vi kjenner ikke alle fenomener godt nok i alle dets varianter og avskygninger, og språket er ofte utilstrekkelig for presise avgrensninger.

En vei ut av eller rundt problemet kan være å benytte et indirekte avgrensningskriterium. Vi tar tak i ett typisk kjennetegn ved det fenomen som skal

4 Slik *Bryde Andersen* Grunlæggende aftaleret, s. 196.

reguleres, og knytter reguleringen til dette. Kanskje er det ikke denne egenskapen vi egentlig ønsker å regulere, men den gir en tilknytning til det som egentlig er reguleringens gjenstand. Og den blir enklere å forstå og kan gi en hensiktsmessig avgrensning. Denne egenskapen blir en bro mellom rettsvirkningen og det vi *egentlig* ønsker å regulere.

Noen ganger vil teknologien bidra til å gjøre broen unødvendig. Den blir en omvei og en flaskehals. Det skaper ikke akutte problemer, og disse lar seg stort sett løse over litt tid. En langt større utfordring er når broen fjernes eller brister. Da mister reglene kontakten med den virkelighet de var ment å skulle regulere.

En slik bro – om vi holder oss i det bildet – er *dokumentet*. Tradisjonelt har dokument vært et stykke papir med tegn. Det behøver ikke være papir. Går vi bakover i tid, var dokumentene av pergament. Og rettslig sett hadde det ikke hatt noen betydning om tegnene hadde vært hogd inn i en steinplate. Det hadde vært upraktisk å lagre og transportere (i fysisk forstand) slike dokumenter, men rettslig sett har de samme egenskaper som vi kjenner fra de dokumenter vi har hatt til nå.

Dokumentene er fysisk avgrenset. Vi har et stykke papir. Når vi refererer til dokumenter er det gjerne disse fysiske gjenstandene vi refererer til, selv om det vi ønsker å regulere er de data som dokumentet er bærer av. Rettsteknisk er det enkelt. I stedet for å anstrenge oss for å avgrense hvilke *data* en regulering skal omfatte, regulerer vi dette ved å si *de data som finnes på et identifiserbart stykke papir.* Så kommer noen og napper vekk papiret, og broen brister.

Vi kan ta en tur ut av formueretten. Reglene om innsyn i forvaltningen i *fvl §§ 18–20*, gir rett til innsyn i *dokumenter*. I en rekke forvaltningssaker hentes opplysningene ut fra mange ulike registre og databaser. Dette gjelder ikke minst den forvaltningssak som vi alle stifter bekjentskap med en gang i året: Selvangivelsen. Hvis man har en enkel selvangivelse kan man sende en SMS-melding til ligningskontoret og bekrefte de opplysninger som man har blitt forelagt. Hvis vi ønsker innsyn i ligningsmyndighetenes dokumenter, får vi et problem. Man kan *produsere* et dokument som inneholder de data som beslutningen bygget på. Men dette vil ikke være et saksdokument i vanlig forstand.

Man har forsøkt å definere seg ut av problemet i forvaltningsloven. I *fvl § 2 første ledd, bokstav f* er et dokument definert som følger:

> *"dokument: en logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting, framføring eller overføring."*

Det er kanskje et godt forsøk, men heller ikke så mye mer. For hva er en *logisk avgrenset informasjonsmengde*? Jeg skal ikke gjøre noe forsøk på å

forklare dette. Når man forsøker å bruke dette som et operativt kriterium for eksempel for å avgrense innsynsretten, ser man fort at dette kriteriet er uanvendelig i praksis.

Når broen brister tvinges vi til å ta stilling til de underliggende realiteter. Man kan gjerne si at vi må skjære igjennom transaksjonens overflate og innpakning, og vurdere dens innhold. Om vi fortsatt holder oss til forvaltningsretten, så må vi gå direkte til spørsmålet om hva slags opplysninger vi skal kunne ha innsyn i, uten å måtte gå veien om dokumentene. Dette betyr også at vi ikke kan skjule oss bak dokumentene.

Tinglysingen er et eksempel på at man, i alle fall i første omgang, har kapitulert overfor disse problemene. Utgangspunktet er at man kan tinglyse *dokumenter*. Det stilles videre krav til disse dokumentene. I *tingl § 4a* har man gitt hjemmel for å kunne ta i bruk elektronisk kommunikasjon. Stort sett inneholder bestemmelsen bare hjemler for å gjøre unntak fra tinglysingslovens regler. Foreløpig har man satt i gang et forsøk med elektronisk kommunikasjon ved tinglysing av salgspant i motorvogn. I de forskrifter som er gitt for dette forsøket har man i § 2 sagt at dokumentdefinisjonen i *fvl § 2 første ledd, bokstav f* skal gjelde også på dette området. Men forsøket på å definere et "logisk dokument" fungerer ikke særlig bedre i forhold til tinglysning enn det gjør på forvaltningslovens område.

Problemene illustreres også av reglene om krav til dokumentene. I *tingl § 17* heter det:

> *Skal et skjøte eller pantedokument som ikke er utstedt av offentlig myndighet, kunne anmerkes i grunnboken, må underskriften være bekreftet*

I forskriftene om tinglysing av salgspant i motorvogn har man gått helt bort fra dette, og sier ganske enkelt i § 5:

> *Dokument om salgspant i motorvogn som sendes inn elektronisk behøver ikke være underskrevet.*

Her går man fra den ene ytterlighet til den andre: Fra krav om bekreftet underskrift til at det ikke kreves underskrift i det hele tatt. Det må legges til at man i *forskriftenes § 9, første ledd* har følgende bestemmelse:

> *Oversendelsen av elektroniske dokumenter skal sikres i en teknologisk løsning som til enhver tid ivaretar sikkerheten med hensyn til autentisering, konfidensialitet, integritet og ikke-benekting.*

Man forutsetter at sikkerheten ivaretas. Det stilles ikke opp konkrete krav til hvordan den kan ivaretas, men man har innsett at papirløsningen ikke vil kunne fungere.

Tradisjonelle konsepter og begreper utfordres

Da jeg skrev en kommentar til verdipapirsentralloven av 1985 forsøkte jeg å plassere verdipapirregistrene i forhold til det velkjente begrepsparet *real- og personalregister*. Dette var ikke enkelt. Ser man det fra utstedersiden har det karakter av å være et realregister: Det er register over hvem som for eksempel eier aksjer i selskapet. Ser man det derimot fra investorsiden blir det et register over hva den enkelte eier og heftelser registrert på vedkommende, altså et personalregister.

Etter hvert gikk det opp for meg at denne tradisjonelle inndelingen er begrunnet i den teknologi man tradisjonelt har anvendt. Så lenge man baserer seg på en hengemappeteknologi må man holde seg til en og bare en sorteringsnøkkel. Man må enten sortere arkivet etter navn eller etter gjenstand. En databaseteknologi har ikke slike begrensninger. Man kan ha mange sorteringsnøkler og sortere etter mange indekser. Om vi overfører dette til tinglysingen vil det ikke lenger være noe problem å finne hvem som har rettigheter i en bestemt eiendom, hvem som har tinglyste krav mot en bestemt person, eller hvilket tinglyste rettigheter en person har. Det vil for eksempel være enkelt å finne alle pantsettelser til fordel for en bestemt panthaver.

Hvorvidt vi ønsker å ta mulighetene i bruk er et rettspolitisk spørsmål. Så lenge reglene er basert på den gamle teknologiens muligheter og begrensninger, vil reglene fremstå som omveier og flaskehalser. Men de er ikke direkte hindringer for skifte av teknologi. De hindrer oss bare i å ta i bruk den nye teknologiens muligheter.

Men transaksjonene kan endre karakter på måter som gjør gamle løsninger uanvendelige. *Verdipapirregisterloven § 7-1* har regler om prioritet mellom kolliderende rettigheter. Disse reglene er basert på en illusjon om at man fortsatt har formuesgoder som det kan håndheves rettigheter i forhold til. På en verdipapirkonto kan det for eksempel være registrert 10.000 aksjer i Norsk Hydro. Det vil da fremstå som en beholdning på 10.000 Hydro, på samme måte som man på en pengekonto kan ha 10.000 EUR. Man har ikke 10.000 individualiserte aksjer, angitt med aksjenummer. Man kan ha pant i kontoen, og prioritetsreglene kan si noe om forholdet mellom flere pantheftelser. Men føres aksjer ut av en konto, vil rettigheter ikke kunne følge ikke-individualiserte verdipapirer. Det blir som å skulle spore penger gjennom betalingssystemet for å finne ut hvor de bestemte pengene som sto på en konto har havnet.

Man vil nok kunne følge overføringene, men da bare som overføringer av generisk bestemte verdier. Det kan tenkes at man vil ha et tilbakesøkingskrav eller et erstatningskrav, men det er noe annet enn en rettighet i de verdier som er overført. Man får et obligatorisk krav, mens man før hadde et tinglig krav. Men loven er fortsatt basert på at man har et tinglig krav.

Man vil ofte tvinges til å revurdere gamle løsninger. Under arbeidet med etablering av Verdipapirsentralen hadde jeg på et tidspunkt en ganske intens diskusjon med ledelsen i den danske Værdipapircentralen om forståelsen av en rettsvernsbestemmelse i den danske loven. Regelen var at to rettsstiftelser, for eksempel to erverv, registrert samme dag hadde lik rett. Det er en løsning vi kjenner fra tinglysingen, og den fungerer når man har et individualisert formuesgode. Men når to har kjøpt de samme obligasjonene så kan man i praksis ikke ha en løsning hvor de får obligasjonene i fellesskap. Den ene av kjøperne får dem, den andre ikke. Men når reglene sier at de har lik rett, blir det vanskelig. Jeg spurte om hva man ville gjøre dersom det skulle skje at to kolliderende rettsstiftelser ble registrert samme dag. Svaret var at den ene ville få obligasjonene, den andre ville få erstatning. Jeg insisterte på – og holder fortsatt fast ved – at den som måtte nøye seg med erstatning ikke hadde fått rettsvern.

Da jeg senere reflekterte over denne diskusjonen, gikk det opp for meg at vi i mange tilfeller slett ikke har behov for rettsvern. Den part som måtte nøye seg med et erstatningskrav kom like godt ut av det så lenge det bare var spørsmål om økonomiske verdier og den erstatningsansvarlige ikke har noen problemer med å oppfylle sin erstatningsplikt. Da jeg på midten av 1990-tallet var med på en utredning om elektronisk tinglysing, møtte jeg denne problemstillingen igjen. Som jurister har vi en ryggmargsrefleks som sier at vi i slike situasjoner må ha regler om rettsvern. Men i mange situasjoner bidrar de bare til å komplisere løsningene, uten at vi har behov for dem.

Hvis man må gå fra gård og grunn som følge av en tinglysingsfeil, vil det være en fattig trøst at man får dekket det økonomiske tapet. Men for en panthaver vil en garanti mot økonomisk tap kunne gi like god sikkerhet som pant i eiendommen. For verdipapirer er bildet tilsvarende sammensatt. Når det gjelder obligasjoner vil garantier kunne fungere like godt som rettsvern – det er uansett bare økonomiske verdier som står på spill. Men gjelder det aksjer er det ikke sikkert at en erstatning vil kunne kompensere for at man mister kontrollen i et selskap.

Garantier er på de fleste måter enklere enn rettsvernssystemer. Når de i praksis kan gi like god sikkerhet bør man vurdere å velge slike løsninger – ikke minst siden rettsvern uansett vil være en illusjon i ganske mange tilfeller. På et mer generelt plan kan vi si at vi må frigjøre oss fra gamle løsninger og gammelt tankegods når vi møter ny teknologi.

Nye infrastrukturer

Når jeg her bruker betegnelsen *infrastruktur* sikter jeg til *myke infrastrukturer*. Dette er organisatoriske strukturer, gjerne i form av nettverk. Disse organisasjonene behøver ikke eie fiber og kobber, jernbaneskinner, havner og veier.

Om vi spoler tiden tilbake til før 1984, kunne to personer ha møttes, inngått og gjennomført en avtale om salg av danske obligasjoner. Man kunne ha møttes på Hardangervidda, på Bali eller Everest Base Camp. Selger kunne hatt gjeldsbrevene (obligasjonene) i en dokumentmappe, og kjøper kunne hatt pengene i kontanter. De kunne ha blitt enige om prisen og utvekslet ytelsene. Rettslig sett er løsningen enkel.

En slik transaksjonsform har mange ulemper. Det er enkelt hvis begge parter faktisk er på samme sted. Men ved handel over avstand blir det vanskelig. For å kunne utveksle ytelsene må fysiske papirer fraktes fra et sted til et annet, og kontanter måtte ha vært fraktet den andre veien. I tillegg til at slik transport er tidkrevende og kostbar medfører den høy risiko.

I dag er det ikke noe problem om partene er på ulike steder. Selger kan gjerne sitte i Everest Base Camp mens kjøper er på Hardangervidda. De utveksler de nødvendige meldinger og transaksjonene blir registrert i de systemene som tar hånd om slikt.

Men om de faktisk skulle befinne seg i samme rom, så ville det likevel ikke ha vært mulig å gjøre opp transaksjonen der og da. De ville fortsatt ha måttet gjennomføre transaksjonene i de systemene som tar hånd om slikt.

I praksis vil både selger og kjøper måtte sende sine ordrer til Værdipapircentralen. (VP) Der ville ordrene ha blitt avstemt. Kjøper må samtidig sende en betalingsordre til sin bank. For å kunne opprettholde et prinsipp om ytelse mot ytelse, vil VP-transaksjonen og pengetransaksjonen måtte avstemmes mot hverandre før de kan gjennomføres. Systemet blir langt mer komplisert enn det var da vi kunne levere papirer, selv om det er enklere å foreta handelen.

I de fleste tilfeller hvor man går over fra dokumentbaserte til elektroniske transaksjonssystemer ser vi at vi får nye mellommenn. Hva disse egentlig gjør, vet vi lite om. Det hele fremstilles gjerne som hensiktsmessige løsninger på praktiske problemer, noe det også er. Men deres rolle kan ha betydning for transaksjonene, uten av vi vet hva slags betydning de har.

Bildet er meget sammensatt. Det kan være ren transport. Et enkelt elektronisk postsystem påvirker ikke transaksjonen. Om man får et avtaledokument oversendt som vedlegg til en e-post eller som gammeldags fotpost, har som regel ingen betydning.

Men tjenesteyterne gjør ofte langt mer. En enkel videreutvikling er registrering av trafikk, gjerne med "tidsstempling". Det vil være e-postens versjon av rekommandert post. Tjenesten kan videre inneholde identitetskontroll og andre sikkerhetsløsninger. Systemene vil kunne være ganske sofistikerte. Det behøver ikke bare være et spørsmål om tilgang til systemet, men også om tilgang til ulike tjenester som tilbys gjennom systemet. Man kontrollerer fullmakter, leveringsavtaler m.m. i systemet. Her vekkes juristrefleksene, og man aner at det kan blir spørsmål om ansvar dersom disse tjenestene svikter.

Tjenestene kan utvikles videre slik at man ikke bare registrerer at meldinger har blitt utvekslet, men også innholdet i transaksjonene. Her nærmer man seg en modell som er kjent fra tinglysingen, og som vi ser tas i bruk på stadig flere områder. En annen og mer vanlig variant er at systemene er reservasjons- eller bestillingssystemer, for eksempel flybilletter eller hoteller.

En tredjepart kan også gå inn som direkte part i transaksjonen. Når vi betaler gjennom en bank driver ikke banken noen form for pengetransport. Jeg gir min bank et oppdrag om å overføre et beløp, hvilket vil si at min fordring mot banken (innskudd) reduseres noe, mens mottakers fordring økes tilsvarende. I praksis vil det gjerne være slik at beløpet overføres gjennom flere banker. Hvis jeg instruerer DnB NOR om å overføre et beløp til en mottaker som har konto i Nordea, vil min fordring mot DnB NOR reduseres, samtidig som Nordea får en tilsvarene fordring mot DnB NOR. Mottaker vil bli godskrevet beløpet ved at hans fordring mot Nordea øker, og denne fordringen balanseres av fordringen mot DnB NOR. De to bankene vil så gjøre opp via Norges Bank. Alle leddene er selvstendige transaksjoner, selv om de henger sammen. Jeg har en avtale med DnB NOR, ikke med Nordea. Mottaker har en avtale med Nordea, ikke med DnB NOR.

En clearet opsjon gjennomføres ved at clearingsentral går mellom selger og kjøper, og tar en posisjon i forhold til begge. Hvis A gir en kjøpsopsjon til B vil clearingsentralen være As motpart. A forplikter seg til å selge til clearingsentralen på avtalte vilkår dersom opsjonen gjøres gjeldende. Clearingsentralen gir så en kjøpsopsjon til B, og det er clearingsentralen som er forpliktet overfor B.

Verdipapirregistrene kombinerer gjerne funksjon som handels- og oppgjørssystem med rollen som et "tinglysingsregister". Rettslig sett blir derfor systemene ganske kompliserte.

Vi vet lite om disse nye systemene som dukker opp. Noen få har blitt studert. Men de fleste er "svarte bokser" for oss jurister. Det skal nok skrives en del doktoravhandlinger om ulike systemer av denne type før vi eventuelt kan begynne å se et mønster som gjør det mulig å utvikle dette rettsområdets "alminnelige del".

Når det etableres nye infrastrukturer får vi for det første et spørsmål om organisering. Dersom systemene i praksis blir monopoler eller i alle fall dominerende markedsaktører, kommer konkurranseretten inn. Hvis en nyetablert bank nektes adgang til betalingssystemene vil de i praksis ikke kunne drive bankvirksomhet. Et flyselskap som utestenges fra bestillingssystemene vil også kunne få store problemer. Men disse spørsmålene lar jeg ligge.

Slike systemer vil ofte være lukket selv om tilgangskriteriene kan være transparente og ikke-diskriminerende. I et papirbasert system kan hvem som helst skrive et brev eller fylle ut et dokument og sende det inn. I elektroniske systemer hvor transaksjoner eller transaksjonsdata skal kunne registreres direkte må det være et nettverk av enheter som har tilgang til systemet. Dette kan illustreres med forskrift for prøveprosjekt for elektronisk kommunikasjon ved tinglysing av salgspant i motorvogn § 3, hvor det heter:

> *Bare brukere som er godkjent av Justisdepartementet og Løsøreregisteret kan sende inn elektroniske dokumenter. Godkjennelsen er personlig.*

Brukerne må altså forhåndsgodkjennes før de kan ta tjenesten i bruk. Videre må godkjennelsen være personlig. Her er det ikke åpning for noen ad hoc registrering når behovet måtte melde seg. Nå vil nok akkurat denne tjenesten først og fremst være aktuell for finansinstitusjoner, slik at det neppe er et stort problem i praksis.

For tjenester som skal være tilgjengelig for et stort antall brukere, blir dette vanskeligere. Det ville ha vært en byråkratisk og krevende løsning om for eksempel Verdipapirsentralen skulle ha måttet godkjenne alle som har registrerte verdipapirer. Stiller man krav om at alle utenlandske investorer også skal godkjennes etter slike prosedyrer, vil oppgaven kunne bli uoverkommelig ù om det da ikke blir så komplisert at mange av denne grunn ville unngå å investere i norske aksjer og obligasjoner.

Løsningen er at man benytter et eksisterende organisatorisk nettverk. Verdipapirsentralen har et nettverk av kontoførere, i praksis banker og meglerforetak. Man flytter så identifiseringen og godkjenningen av brukere ut til deltakerne i nettverket. På denne måten kan man nå helt ut til den enkelte forbruker, slik vi kjenner fra nettbankene.

Selv med et slikt nettverk kan det være et uoverkommelig krav at den sentrale enheten skal kjenne identiteten til alle som deltar i systemet. Så lenge vi holder oss til penger er dette ikke så problematisk, for det finnes ikke noe sentralt register over bankkonti og innestående på disse. Men verdipapirregistre illustrerer problemet. I praksis har man et stykke på vei resignert i forhold. Utenlandske investorer er som hovedregel ikke direkte registrert. Man baserer

seg på såkalt forvalterregistrering, hvor man har en konto hos en forvalter, gjerne en bank, og så er forvalteren registrert i Verdipapirsentralen med den samlede portefølje som forvaltes gjennom denne. Myndighetene liker ofte ikke forvalterregistrering, da dette gir muligheter for å skjule sin identitet bak en forvalter. Men man aksepterer det når man innser at det ikke finnes andre praktiske løsninger.

Hensikten her er ikke å se nærmere på noen av enkelttilfellene, men snarere å peke på en utvikling som man ser på mange områder. Her ligger det betydelige oppgaver for rettsvitenskapen.

Internasjonalisering, deterritorialisering og reterritorialisering.

Internasjonaliseringen er så tydelig at det knapt er grunn til å gjøre mer enn å minne om den i en oversiktsartikkel som dette. Nettbaserte tjenester og digitale ytelser vil lett krysse landegrensene. Spørsmål om jurisdiksjon og lovvalg får en helt annen aktualitet enn hva de hadde for en del år siden. Men også disse dukker opp i nye varianter.

Går vi tilbake til eksemplet med danske obligasjoner, så var det før 1984 mulig å gjennomføre en slik transaksjon for eksempel i en hytte på Hardangervidda. Det ville være liten tvil om at kjøpsavtalen ville være underlagt norsk rett, selv om det hadde vært danske obligasjoner som ble omsatt. I dag behøver ikke partene å møtes. Den ene kan fortsatt være på Hardangervidda, mens den andre for eksempel er på Bali. Man får det man kan kalle en *deterritorialisering*. Men uansatt hvor partene måtte befinne seg og uansett hva de selv måtte avtale, så vil transaksjonen gjennomføres via VP utenfor København, og det som skjer der vil være underlagt dansk rett og dansk jurisdiksjon. Mens endepunktene i transaksjonen løsrives fra territoriet, vil vi få en sentral institusjon med en klar territoriell tilknytning. Vi får med andre ord også en *reterritorialisering*.

Så lenge man ikke kjenner organiseringen av de systemer vi benytter oss av vil den rettslige situasjonen være lite overblikkbar. Ved pengeoverføringer vil oppgjøret for alle beløp av betydning i praksis skje via sentralbanken i valutalandet. Betales det i NOK skjer oppgjøret i Norges Bank, oppgjør i EURO skjer via Den europeiske sentralbanken i Frankfurt, og oppgjør i USD skjer via Federal Reserve i New York.

Problemstillingen illustreres i de engelske dommene Libyan Arab Foreign Bank v. Bankers Trust Co[5] og Libyan Arab Bank v. Manufacturer Hanover Trust.[6] Begge disse dommene kom opp etter at president Reagan den 8. januar

5 1 Lloyd's 259 [1988], [1989] 3 All ER 252.
6 [1989] 1 Lloyd's Rep 608

1986 utstedte en «Executive order» som bl.a. gikk ut på å fryse libyske innskudd i amerikanske banker. Den libyske banken hadde USD konti ved de to andre bankenes London-filialer, kombinert med en folio-konto i New York. Nær alle overføringer ut og inn fra de respektive London-konti gikk via New York. (Bakgrunnen for et slikt arrangement var at euro-dollar markedet ga høyere rente enn hva man kunne få på USD i USA.) Etter Reagans executive order, var det ulovlig etter New York rett å tillate den libyske banken å ta ut eller overføre sitt innskudd, mens det etter engelsk rett ville være et kontraktsbrudd ikke å gjøre det. Begge sakene ble avgjort etter engelsk rett, og de amerikanske bankene tapte. (I den første dommen kom retten til at det var én avtale som omfattet konti både i London og New York, og at den dels var underlagt engelsk rett, og dels New York rett. Situasjonen blir unektelig komplisert når begge lands rett kommer til anvendelse i samme sak, og det man er forpliktet til etter det ene lands rett er ulovlig og straffbart etter det andre landets rett.)

I den amerikanske dommen *Delbrueck & Co v. Maufacturers Hanover Trust Company*[7] får man en mer ordinær lovvalgssituasjon, som viser hvordan fremmed rett lett kan få betydning for overføringer mellom norske kontohavere. Dommen gjaldt overføring av USD fra en tysk bank til en annen. Da overføringen ble foretatt mellom de tyske bankers konti i to amerikanske banker, og avregningen skjedde i New York, ble New York rett lagt til grunn.

Mange har fått erfare dette i praksis uten at det har blitt rettssak om spørsmålet, hvis de har forsøkt å overføre USD til Cuba. På grunn av USAs boikott av Cuba stanses alle slike overføringer i USA, og beløpene blir stående på sperret konto i Federal Reserve.

Metode

Man møter noen ganger spørsmålet om man anvender en særskilt metode når man arbeider med rettsspørsmål i skjæringsflaten mellom jus og teknologi. Spørsmålet er vanskelig å besvare fordi den rettsvitenskapelige forskningsmetode er så lite utviklet. Når jurister nokså upresist sier at de anvender "alminnelig juridisk metode", så tenker man gjerne rettskildelære. Dette er en rettsanvendelsesmetode, hvor målet er å begrunne et standpunkt innenfor rammen av gjeldende rett. Rettsvitenskapen har et videre siktemål enn dette.

Når man møter ny teknologi er første utfordring å finne ut hva som faktisk skjer. Vi må åpne de "svarte boksene" og undersøke hva som skjer inne i dem. Man har ikke en noenlunde klart formulert juridisk problemstilling, og

7 609 F.2d 1047 (1979). Lovvalgsspørsmålet drøftes bare i førsteinstansens avgjørelse, som finnes i 464 F. Supp. 989 (1979).

har dermed ikke kommet til det stadium hvor en metode for rettsanvendelse kommer til nytte. "Alminnelig juridisk metode" sier lite eller ingen ting om hvordan man finner ut av faktum.

Oppgaven er ofte krevende, som regel mer krevende enn de som ikke har forsøkt det er villige til å tro. Vår oppgave er å finne ut de rettslige relevante sider ved transaksjonen, og det kan man ikke gjøre uten juridisk innsikt. Det finnes derfor som regel ikke noen egnede beskrivelser. Man har reklamebrosjyrer med mye bilder og lite innhold, og man har detaljerte tekniske beskrivelser. Men det finnes lite på nivået i mellom. Vi trenger en funksjonell beskrivelse. Som regel er det ingen vei utenom å grave seg ned i detaljene ved hjelp av tekniske spesifikasjoner, for så å bygge opp en funksjonell beskrivelse ut fra dette.

Ganske ofte vil man havne et annet sted enn der man trodde da man startet. Det som forelå om betalingsformidling før jeg gikk løs på emnet hadde stort sett et transportrettslig utgangspunkt. Dette var også mitt utgangspunkt. Men etter hvert som jeg fikk bedre innsikt i hva som faktisk skjer, innså jeg at dette ikke var et holdbart grunnlag for rettslig analyse. Betalingssystemene er i sin kjerne bokføringssystemer – informasjonssystemer – hvor man holder rede på fordringsbalansene mellom aktørene. Det skjer ingen transport av "penger". Alt som formidles er instrukser om endringer som skal foretas i bokføringen og bekreftelser på at dette er gjort. Dermed falt transportrettslige problemstillinger som "transportansvar" bort. Fordringene forsvinner ikke selv om det blir feil i bokføringen. Dermed måtte drøftelsen bygges på et annet grunnlag enn det jeg trodde da jeg startet. Dette er en erfaring som mange har gjort. De "svarte boksene" viser seg å inneholde noe annet enn det vi trodde da vi bare betraktet dem fra utsiden.

Når man har klart å redegjøre for faktum møter man gjerne ganske velkjente rettslige problemstillinger. Men veien dit er ofte lang. Derfra og ut vil man kunne anvende "alminnelig juridisk metode", dog med den modifikasjon at rettskildematerialet ofte er så sparsomt at man ikke har noe særlig grunnlag for å uttale seg om "gjeldende rett". Forskningsresultatene ligger gjerne i begrepsutvikling og problemforståelse, og ikke i å tilføye flere desimaler til svarene.

Forskningsmessige utfordringer

Så langt har vi bare sette begynnelsen. Jeg tenker noen ganger på situasjonen som om vi har ryddet vei slik at vi har kommet oss ut av skogen og står foran et åpent landskap. Vi begynner å komme oss løs fra de mest bastante bindingene til det gamle. Men utfordringen ligger ikke i frigjøringen fra det gamle. Den ligger i forståelsen og analysen av det nye som vi så møter.

Vi må finne ut hva alle de nye aktørene i markedet egentlig gjør med transaksjonene, og beskrive deres roller i et rettslig perspektiv. Dette er første etappe, men vi må starte der. Først når vi begynner å forstå mer inngående hva som faktisk skjer vil vi bli i stand til å gjennomføre mer tradisjonelle rettslige analyser.