Law and Information Technology. Swedish Views

An anthology produced by the IT Law Observatory of the Swedish ICT Commission

Editor Peter Seipel

Information and Communication Technology Commission Report
Stockholm 2002

STATENS OFFENTLIGA UTREDNINGAR

Swedish Government Official Reports
SOU 2002:112

Table of Contents

Table of Contents....3

Part I: General Background....5

Editor's Foreword....7

Christer Marking The Swedish ICT Commission....9

Peter Seipel, Kjell Skoglund The IT Law Observatory....14

PART II: In Search of a Perspective....19

Peter Seipel Law and ICT. A Whole and its Parts....21

Håkan Hydén Remunerative Gifts, Societal Development and Legal Futures....33

Joachim Benno Why the Use of ICT Engenders Legal Problems – in Search of a Common Denominator....44

Per Furberg Lawmaking and IT: Reflections on the Need for New Concepts and Categories of Thought....55

Viveca Bergstedt Sten The IT-practitioner's world....67

Part III: ICT in Government and Administration....75

Hans Sundström, Gustaf Johnssén Shaping the Future Public Administration – The Legal Perspective....77

Peter Seipel Access Laws in a Flux....88

Claes Gränström Archives of the Future....99

Part IV: ICT in Commerce and Work....107

Christina Ramberg Contracting on the Internet – Trends and Challenges for Law....109

Agne Lindberg, Henrik Bengtsson Database-Aided IPR Due Diligence....117

Mikael Pawlo Efficiency, Innovation, and Transparency – The Future of Intellectual Property Rights....128

Lena Olsen Children and Internet Trade....139

Gustaf Johnssén Bits or Balloons? The Need to Rethink Tax Concepts and Principles on the Internet 147

Anders R. Olsson Freedom of Speech and the New Media 154

Håkan Hydén Self-employed – The Problem of Societal Development and Adequate Legal Concepts 161

Anders Victorin Electronic Plumbing – Building the Telecom Infrastructure 167

Part V: Security and Vulnerability 175

Sören Öman Protection of Personal Data – But How? 177

Per Furberg Dealing with computer crime. A Critical Review of Legislative Reactions to Computer Crime 185

Part VI: Legal Machinery Matters 193

Cecilia Magnusson Sjöberg The Melting Pot Paradox of Structured Documents 195

Peter Wahlgren The Quest for Law. Legal Sources via IT 207

Ulf Maunsbach Alternative Dispute Resolution – The Features and the Future 218

Björn Larsson Courts of the Future 225

Annex 1 The IT Law Observatory 239

Annex 2 References to documentary materials of the IT Law Observatory 243

Part I:
General Background

Editor's Foreword

A recurring theme in the contributions to this anthology has to do with the nature of the relationships between law and ICT (information and communication technology). In a nutshell: are the relationships between law and ICT important and particular enough to merit special attention?

Three reasons argue for an affirmative answer. The first has to do with *complexity*. The second with *magnitude*. The third with *uncertainty*.

The *complexity* of ICT involves not only technical intricacies in a narrow sense. ICT has moved out from closed research environments and become a ubiquitous and flexible instrument for all kinds of information handling in society. Thus, it is necessary to take into account matters having to do with the design and operation of information systems, existing and possible applications of ICT, including their effects and interdependencies, and conceptual issues having to do with the changing nature of information processing. From this point of view, the study of law and ICT should be perceived not as a trivial affair but as a rather demanding challenge. It requires a broad outlook and, quite often, expert knowledge of the increasingly intertwined world of law and technology.

Magnitude, obviously, refers to the economic and practical significance of ICT in society. Briefly, we are dealing with a "mega-technology" capable of both creating and destroying markets and, generally speaking, ways of living. This is the background of the often quite loud calls for actions to do away with outmoded legal solutions – viewed as "obstacles" – as well as for actions to legally restrain and control the electronic environment

Uncertainty (and its corollary curiosity), finally, provides good reasons for delving into the many issues that emerge as ICT gradually alters significant parts of society's infrastructure. We need to understand what is going on, preferably before conflicts and problems have surfaced. The legal system is affected – but in what ways and how deeply?

The contributions to this anthology all seek answers to such questions. They do so in different ways and in different areas but they all reflect the work that since 1996 has been going on in the IT Law Observatory of the Swedish ICT Commission. The spirit

of this work has always been: *let's take a closer look, it may be worth it*. This can also be termed the motto of the anthology.

There are twenty-two contributors. They come from the Observatory itself as well as from the network of experts that the IT Law Observatory has built up and consulted. The number could easily have been increased, but for limitations of space.

The anthology is divided into six main parts. Part I, "General background", outlines the work of the Swedish ICT Commission and its IT Law Observatory. Part II, "In Search of a Perspective", discusses the area of law and ICT as a whole from different points of view, setting the framework for the area-specific contributions that follow. Part III, "ICT in Government and Administration", comments on certain basic issues of electronic public administration such as the citizens' access to official documents. Part IV, "ICT in Commerce and Work", is broadly conceived, ranging from contracting and taxation on the Internet to matters of freedom of speech and self-employment in the new electronic environment. Part V, "Security and Vulnerability", deals with two topics, *viz* how to shape adequate protection of personal data, and legislative responses to computer crime. It ought to be mentioned that the Swedish ICT Commission has done much broader work in the security area. This work has been reported on elsewhere.[1] Part VI, "Legal Machinery Matters", serves as a reminder that the interaction of law and ICT comprises more than matters of substantive law. Briefly, there are numerous methodological issues linked to the use of ICT in the judiciary etc. A few of them are dealt with here.

Finally, on behalf of the IT Law Observatory, I wish to express my sincere thanks to all the contributors for their willingness to participate and also to Roger Tanner, who has kept an eye on the language but is not to blame for any remaining blemishes.

Peter Seipel
Chairman of the IT Law Observatory

1 Information can be accessed at www.itkommissionen.se.

Christer Marking*
The Swedish ICT Commission

1 Background

International comparisons have ranked Sweden as one of the most "mature" countries in terms of information technology – penetration of PCs to homes, the use of Internet, mobile telephones, broadband etc. A number of factors might help to explain this. The early adoption of ICT in public administration, banking and industry made people familiar with computers at work and in their dealings with the authorities. Swedes also seem to have a positive attitude to new technology and are early adopters. In the middle of the 1990s, more than 40% of Swedish households had a PC. As all of them had telephones, Internet penetration soon became very high. Information technology was also used broadly in working life in general so most people met it at work.

For a small country, Sweden has quite an interesting history in the field of computers and information technology, related to both hardware and software. In fact, in the 1950s and 1960s, Sweden was at the international forefront of both industry and R&D. Today, apart from Ericsson, there are no real indigenous computer manufacturers in Sweden, although there are fairly broad activities in the field of specific ICT applications development.

2 Early public and political concern

The use of computer technology in more and more areas of life gave rise to public concern. The new opportunities to perform cross-computations of different registers or databases already

---

* *Christer Marking* is the director of the ICT Commission since February 1999. He is also the chairman of the Swedish Centre for Internet Technology, a research institute, and was earlier the director of R&D policy at the Ministry of Industry. He has been involved in research on production systems and work organisation at the Royal Institute of Technology, The Swedish Work Life Centre and The Swedish Metal Workers Union and has been the director of the Swedish Commission for Skills and Competence in Working Life.

created in the public and private sector, prompted the concern for privacy which ultimately led to the world's first regulation on the national level of computers and privacy.

There was also growing concern about work conditions related to the application of automatic data processing. This related both to the area of public administration and to the use of computer technology to automate manual work in industry. In the late 1970s particularly, that concern surfaced and led to a number of government-initiated commissions looking into various aspects such as regulation by law, matters of security, and effects on working life and productivity. Meanwhile, the economic recession at the time prompted the oft-recurrent discussion about technology-induced unemployment. There was a subsequent need for policy formation related to computers and society and a number of different policy commissions were formed, with representatives from politics, public administration, trade unions and business organisations. They were all links in a chain of which the ICT Commission is the latest link so far.

3 The formation of the ICT Commission

The Internet concept ushered in a new era. The myth has it that Sweden's prime minister at that time, Mr Carl Bildt, sent an e-mail to President Clinton in the USA in early 1994. That was an act of great symbolic import, inaugurating in Sweden the era of ICT as communication technology, as opposed to ICT as merely computer technology. We were no longer talking about stand-alone computers. No, we were talking communication, of which computers were only a part. Prime Minister Bildt set up an ICT Commission which included a number of ministers from his government but also many high-ranking businessmen and professors from the universities. The aim was to explore the opportunities of the new technology and to deal with the downsides, if there were any. In a way the remit could be termed that of alerting society to the prospect of a new future. The Swedish ICT Commission thus formed crowned its endeavours by publishing the book "Wings to Human Ability". Some say that this book inspired the young generation to move to ICT as the land of opportunities – these were the people who created the huge number of start-up companies in the Internet area.

4 The present ICT Commission

The present ICT Commission, formed in 1998, is the fourth since 1994. Its mandate expires in June 2003. In general terms one can say that the scope of the ICT Commission has shifted from the creation of general awareness of the opportunities of ICT to in-depth understanding of specific issues related to the use of ICT in society. The view taken by the Swedish ICT Commission of technological change is in a way rather mainstream, namely that the usefulness and acceptability of a technical innovation depends on its social and cultural context. In the Commission's view, it is fairly obvious that the present mismatch between aspirations and reality in productivity gains from ICT is primarily due to the technology being insufficiently adapted to social and organisational needs.

So far, the development of the Internet has been dramatic and has posed a number of new questions. Generally speaking, the proliferation of ICT at work and in people's homes has exceeded all expectation. That implies major adjustments over time to the way in which people and organisations co-operate and co-ordinate their efforts. The obstacles to improvements and development are not exclusively technical. The counterforces are just as often legal, economical or organisational and are often a part of cultural habits and preferences.

The Commission has thus set out to explore a number of societal aspects of ICT implementation. In a number of areas considered to be of prime interest, the ICT Commission has formed its own so-called Observatories, each comprising prominent actors and savants in its particular area. There are six main areas of such ICT related studies, *viz* "Law", "Infrastructure", "Information Security", "Democracy and Citizenship", "Learning, Knowledge, Competence" and "ICT and Growth".

The legal aspects are numerous. They concern the pressure exerted by the fast spread of ICT use on existing norms and regulations. They also concern various more or less foreseeable demands for institutional changes that emerge from increasingly widespread use of ICT – not least the transition from simple, local use of computers to nationwide use of complex systems and platforms where ICT serves as the basis and the necessary prerequisite.

Since its work began, one important area for the Commission has been the development of the communication infrastructure. In 1999 the Commission published its vision of a "future-

proof IT-infrastructure".[1] That vision was based on a comprehensive analysis of the technical and economical preconditions for building an infrastructure that could accommodate steadily rising demands for transmission.

Security and safety are also among the Commission's prime concerns. They may be regarded as aspects of the infrastructure and they touch upon issues such as privacy, redundancy in the fibre optic network system, and securing your own PC so that you are not a potential menace to the net.

Presently, the area of ICT in relation to learning, knowledge, and competence is dynamic. The Commission emphasises ICT as a means for broad access to learning opportunities both at work and in other situations, at school and in everyday life. To reach the desired goals, new kinds of learning environments must be developed. The Commission seeks to support and accelerate this work.

Gradually, more and more of the Commission's work is being devoted to information as a fundamental resource in society. The development of tomorrow's digital services presupposes the widespread availability of all kinds of information on the net. This means that considerable efforts are needed to achieve standardization of both syntactic and semantic resources. The importance of a transparent information infrastructure cannot be exaggerated and concerns all areas of interest of the Commission, not least ICT and democracy and ICT and growth. To label its strivings, the Commission has launched the notion of "Broad Services". Such services are based on three basic elements: (a) Services that are truly useful to a large number of citizens. (b) Services of a high value due to combined use of information from many sources. (c) Widespread availability of broadband communication facilities.

5 The future of ICT policy?

Starting with Government Bill 1981/82:123 on "a co-ordinated data policy", a number of computer- or ICT-related bills and policy documents have been passed by the Swedish Parliament. Although very differently worded, they are rather similar in spirit and principle. The focus is rarely on technology itself, apart from

[1] "In 5 years, at least 5 Mbps to everyone, at no more than the cost of a monthly bus pass and with the possibility for everyone to choose between at least 5 operators at his or her access point". See: A future-proof IT infrastructure, SOU 1999:134.

some fairly comprehensive R&D programmes. Today, numerous government agencies are responsible for different aspects of the public use of ICT. Co-operation with organs in the private sector is often vital. The efficiency of an overall ICT-policy is therefore highly dependent on the day-to-day work of many organs. From the point of view of the Commission, concerted actions and preparedness for swift changes are of the essence. The Commission can help by spotting problems at an early stage, by engaging itself in future-oriented debates on the ICT society, and by exploring opportunities, obstacles and levers for future productivity and welfare gains. The assessment of policy in action is an important task, although policy formation is still the dominant mission. In its present work, the Commission has pointed to the need for a new "phase" in ICT policy formation with a focus on information as a general resource for the development of new, electronic or "digital" services of great value and benefit for society, industry, and individuals.

Will ICT policy be as prominent in the future as it is today? Or will the development and use of ICT be a "mainstream" activity in all areas while not forming a policy area in it self? Much remains to be explored in the deployment of ICT in society. The effects of ICT use are not fully understood. Technology changes our society and ICT is now becoming a more powerful agent of change than ever before. That in turn underscores the need for a comprehensive social effort to assess, to understand, and to raise social awareness, which in fact is the present ICT Commission's prime task. The experience of the present period of change underlines the need for policy formation in the ICT area; the potential for dramatic changes is still too great to make mainstreaming an option.

Peter Seipel, Kjell Skoglund*
The IT Law Observatory

1 The background of the IT Law Observatory

In March 1994 the Swedish Government convened a commission to foster widespread use of information technology in Sweden as a means to raise the quality of life in the nation, and to enhance its ability to compete internationally. The commission, chaired by the then Prime Minister Carl Bildt, issued its report in August 1994. Two of the key areas treated in the report were "The Legal System" and "Public Administration". Among other things, the report set the goal that the law must not unnecessarily prevent or complicate the use of information technology. On the other hand, basic demands for rule of law, information security, and personal data protection must be met. Information technology should be used to make it easy for the citizens to learn about and gain access to legal source materials.

The social democratic Government elected in September 1994 turned the commission into a more regular Government committee, with a secretariat and with tasks set out in a formal committee directive.[1] The interest taken in matters of law has continued to be strong. Among other things, the Commission, in accordance with Government Bill 1995/96:38, decided to set up an IT Law Observatory in November 1996.

2 The tasks of the IT Law Observatory

The IT Law Observatory may be described as a sort of think tank intended to supplement the ordinary machinery for lawmaking

---

* *Peter Seipel* is a member of the IT Law Observatory. See presentation in Annex 1. *Kjell Skoglund* is senior project manager at the secretariat of the ICT Commission. See presentation of the IT Law Observatory in Annex 1.

1 Committee Terms of reference Dir. 1995:1. This commission came to be known as the Second ICT Commission (chaired by Minister Jan Nygren). It has been followed by the Third ICT Commission 1996-1998 (Dir. 1996:46) chaired by Minister Ines Uusmann,, and the present Fourth ICT Commission 1998-2003 (Dir. 1998:38) chaired by Minister Björn Rosengren (until October 2002. At present, the question of Mr. Rosengren's successor has not yet been decided).

and, more generally, for legally oriented analyses of matters of law and IT. In other words, the aim is to support work in the Ministry of Justice and other ministries as well as work of central organs in the court administration system, in law enforcement, and so forth. Proposals from the Observatory are channelled through the Swedish ICT Commission and the Commission decides what actions are to be suggested to the Government. The Observatory has strived to establish itself as a national platform for discussions and studies in the field of law and IT. It has arranged numerous seminars, workshops etc. and engaged experts to analyse and comment on various matters. The results have been presented in a report series which by now comprises more than 40 publications.[2]

3 The Observatory's work in practice

The IT Law Observatory has three layers of participants. The core consists of sixteen members from the public and private sectors who meet regularly to discuss selected issues, listen to oral reports by experts, prepare reports to the ICT Commission, plan the work of the Observatory, and so forth.[3] The second layer consists of persons with whom the Observatory has close working contacts over a short or long period. They may be employees of Government organs, scholars at universities, experts engaged in legislative committee work, etc. Such persons have often been commissioned by the Observatory to write reports on specific topics of interest. The third layer consists of professionals all over the nation who take an interest in the Observatory, study its reports, and participate in its open seminars and conferences. In particular, the third layer comprises a national network of legal scholars taking an interest in the field of law and IT.

The area of interest covers both matters of substantive ICT law (such as the protection of personal data) and applications of ICT in the field of law. For example, the Observatory has arranged a number of conferences on electronic legal information in Sweden and suggested actions and strategies in this field. Generally speaking, there has never been any lack of projects or ideas. Quite on the contrary, the recurring difficulty has been to set priorities and coordinate the work of the Observatory with other organs.

---

2 A listing of reports published by the IT Law Observatory will be found in Annex 2.

3 The members of the IT Law Observatory are presented in Annex 1.

From the outset, it was clear that the Observatory should avoid duplicating work done by other parties – legislative committees, for instance. The Observatory decided early on to try to look beyond the present-day legal aspects of ICT and to engage in a "legal futurology" in a bid to dispel the criticism frequently voiced concerning legal backwardness. Summing up, the Observatory has sought to operate through a speculative, prospective consideration of new legal structures as an adjunct to the discussion of current law (*lex lata*) and argumentation for proposed changes etc. (*lex ferenda*). One can speak of *lex ponderanda* – a speculative, critical analysis of the law. This means that the Observatory has tried to stay ahead, to be proactive. However, this is easier said than done, considering the rapid changeability of ICT and its applications in society where the future and its uncertainties is never very far away. A typical example of the work pattern attempted can be found in the field of real estate law and data communications, where the Observatory, aided by experts in the field, has helped in structuring the issues and preparing the ground for an ordinary legislative committee (see further the contribution by Anders Victorin below on "electronic plumbing"). Similarly, in the fields of access to official documents, protection of personal data, intellectual property rights etc., the Observatory has supplemented the work of legislative organs by preparing reports and arranging discussions on diverse topics.

On the whole the Observatory has been successful. Negative opinions that existed here and there when its work began have faded away. Moreover, the IT Law Observatory soon became a model for the work of the ICT commission, and five other, similar observatories have later been set up for other areas.[4] The value of the Observatory work model has been proven in a number of ways: It has showed itself flexible and easily adaptable to changing needs and upcoming issues. It has succeeded in bringing together theoretical and practical expertise on the national level and building a useful knowledge base that has been tapped

[4] The five other areas are: Infrastructure, Information security, Democracy and citizenship, Learning and knowledge, Growth. These other observatories have now concluded their work and only the IT Law Observatory will continue until the expected demise of the ICT Commission in May 2003.

by many interested parties. Finally, it has demonstrated the need for orchestrated efforts to handle the numerous legal issues of the information society. This need will persist even after the IT Law Observatory has completed its work in May 2003.

PART II:
In Search of a Perspective

Peter Seipel*
Law and ICT. A Whole and its Parts

"Man must serve his electric technology with the same servo-mechanistic fidelity with which he served his coracle, his canoe, his typography, and all other extensions of his physical organs. But there is this difference, that previous technologies were partial and fragmentary, and the electric is total and inclusive. An external consensus or conscience is now as necessary as private consciousness. With the new media, however, it is also possible to store and to translate everything; and, as for speed, that is no problem. No further acceleration is possible this side of the light barrier."

Marshall McLuhan, "Understanding Media: The Extensions of Man", 1964

1 From ballistics to remote sensing

Few people remember the BARK and the BESK computers, once the flagships of Sweden's budding information industry. BARK was ready for operation in 1950, BESK in 1953. For a short while BESK held the world record in computing speed. Both machines were calculators in the strict sense, i.e. they were designed, built, and used for mathematical work such as ballistic calculations. Their development was supervised by a Board of Mathematical Machines, created in 1948 and existing until 1963. At that time computers were no longer simply "mathematical machines", they had become Automatic Data Processing machines. They had also begun to raise legal questions, not very many at first, and not very interrelated, but still questions worth attention. There was, for example, the question of patent protection of computing devices, and there were questions of contracts, and questions of insurance. Step by step the legal questions have

* *Peter Seipel* is a member of the IT Law Observatory. See presentation in Annex 1.

become more numerous, more complex, and more interrelated. Part of the explanation has to do with the nature of information and communication technology (ICT).

ICT is made up of certain basic elements. The elements have all been present since the birth of the technology, but their relative significance and their visibility are still changing. The elements are automation, information, communication, integration, and sensation.

Automation was the natural first element to attract attention. The computer speeded up computation by doing away with slow manual action. Even the primitive BARK could perform mathematical operations at a speed of 5 to 10 per second. From the legal point of view, automation of this kind did not pass unnoticed. For one thing, computer programs needed to be inserted into the framework of intellectual property law. And automated decision-making in public administration soon caused concern from the point of view of both legality and jurisprudential theory.

At the outset, the *information element* did not mean very much. Both input and output data were mere trickles compared with what we have become used to. Step by step the situation changed and the new technology began to be perceived as an instrument for storing and using large volumes of data. This meant, among other things, that computer systems found uses in many new contexts where automation could be combined with comprehensive filing systems and databases. In consequence, new legal interests arose having to do, for example, with computerised processing of personal data and the building of systems for the storage and retrieval of legal texts.

Communication via local and global networks has been a reality for decades. But not until the Internet revolution of the 1990s did communication begin to be perceived as an essential element on a par with, and perhaps even surpassing, the automation and information elements in terms of importance. This development is reflected by the increasingly frequent use of the term ICT instead of the older IT. It should be underlined that communication has to do not only with communication between machines but also with communication between people. Thus, ICT has become a medium both for private communication (e-mail, chat) and for mass communication (spam, streaming audio). This development is mirrored by the legal discussion, which has moved from relatively straightforward issues of traditional telecommunications regulation involving “conduit” to issues of “content” having to do with such themes as free speech, crime in cyberspace, and different strategies for the governance of global data networks.

Integration has to do with different kinds of convergence phenomena, best known among them being perhaps the convergence or fusion of telecommunications, mass communication media and data processing. These fields have traditionally been regarded as separate areas of legal regulation, and their coming together has required (and still requires) changes of regulatory strategies and instruments. Generally speaking, digital technology has implosive effects, for the simple reason that ICT is universal in nature and can be used to process and communicate information of any kind as long as it can be reduced to ones and zeroes.

Finally, *sensation*, is perhaps the most difficult of the five elements to grasp. In his "Understanding Media" (1964), Marshall McLuhan attempted to describe, among other things, the characteristics of different media in terms of "hot" and "cold", depending upon such factors as the intensity of the communication and the degree of involvement of the participants. If nothing else, McLuhan helped to make people aware that media as such are not neutral, that they affect our behaviour, our expectations, our experience, and so forth. Modern cognitive science studies the relationships between mind, body, and various tools for information processing (notational systems, books, maps, calendars, speedometers, microscopes, etc.). It emphasises interaction and interdependencies. Briefly, human beings think and sense not only with their brain and body but also with their tools. One looks in vain for a clear dividing line between the "inside" and the "outside" of man's mind. As for ICT, we are only beginning to understand the consequences. And a legal understanding hardly exists. One may look for its first signs in themes such as 'protection of minors', 'universal information services', and 'digital divide'.

To summarise: Information and communication technology is a complex and multifaceted array of elements finding its uses in the most diverse contexts. From the point of view of law this is an essential assertion. Sloppy thinking sometimes seeks to reduce ICT to a simple tool, similar in kind to a saw or a typewriter. The reasoning goes: We don't need a law of typewriters, neither is there any need for a legal theory of saws and sawing. Ergo, ICT is not worth fussing about. But is that really all there is to it?

2 Dealing with a tool

How often does a saw interact with the law? In what contexts? In what ways can a typewriter have an impact on administrative decision-making? Silly questions like these quickly indicate that tools are of many kinds and that their relationship to law varies. An attempt at generalising will make it clear that tools may be simple (such as a ring binder) or complex (such as an organisational and technical set-up for verification of electronic signatures), that they may be "hard" (a tape recorder) or "soft" (a classification scheme), special (a pencil sharpener) or general (paper), and so on. Obviously, a simile such as "there is no need for a law of typewriters" ought to be used with care.

ICT must be placed into the category of extremely powerful tools – complex, general, and with far-reaching consequences for society. Perhaps the word "tool" is not even a very good way of labelling it, perhaps it is even misleading. Other words to characterise ICT come to mind – and have indeed been used by different observers. "Industry", "market", "ecology", "culture", and "language" may be mentioned. Regardless of their exactness, such notions are useful since they point towards broader perspectives and create an interest in exploring legal aspects of ICT instead of belittling their importance.

Ever since it began, the discussion of ICT and law has distinguished between two main relationships between the two phenomena. One relationship at an early stage became evident mainly through the development of computerised legal information retrieval systems. Briefly, this relationship concerns *the use of ICT for legal purposes*. The other relationship has to do with substantive law, *viz* matters of legal regulation associated with ICT and its uses in various contexts. The questions that will occupy us in the following concern both types of relationships, including the possible links between them. First some comments on ICT law in general.

Although 'fields of law' are not of the kind to be found in the Linnæan flora there are, of course, criteria which can be used to classify and divide. Many of these criteria are associated with classical, conceptual or institutional legal ordering – private law, tort law, contract law, insurance law, and so forth. Other criteria are associated with different areas of activity, with practical interests, and the like. Some examples are building law, banking law, and maritime law. The two types of criteria, conceptual and practical, often blend into one another, so that it may be difficult

to tell to what extent a particular field of law is delimited and characterised by theoretical or practical concerns.

The prevailing view of ICT law seems to emphasise its practical nature. The radical version of this view does not even recognise ICT law as a field of law proper: It isn't sufficiently coherent, at most it is a loosely interconnected collection of legal problems having to do with computers and data networks. These problems are best treated separately within established fields such as contract law, copyright law, penal law, and so forth. We may call this approach the traditionalist's view. It reflects a healthy scepticism towards far-reaching (sometimes almost boastful) claims that ICT has given rise to a new legal order or that ICT in general and cyberspace in particular are phenomena beyond the reach of the law, that the Internet is a lawless country, and so on. This is the revolutionary's view.

The divergent reactions of legal professionals (theorists as well as practitioners) can be seen as reflecting the complexity of ICT and the many perspectives that one may apply in order to understand its legal hurdles. One way of describing these hurdles is to focus on what may be called 'the paradoxes of ICT law'.

- ICT law encompasses almost all branches of law, but in order to be meaningful it must nevertheless be narrowed down and delimited.
- ICT law ought to be independent of technology (technologically neutral). At the same time it must be capable of regulating and steering technology and its various uses.
- The development of ICT law often requires broad as well as deep understanding of machinery and methods, but the legal solutions must be simple to understand and apply.
- ICT law requires foresight but encounters many difficulties when it comes to predicting future developments, situations, applications, issues etc.
- ICT law involves demands for "new law" but must at the same time be based on inherited legal views and existing legal concepts and regulations.
- ICT law has to solve urgent local and national problems (in tax law, for example) but it has to do so in an international, quite often global framework.
- Legal solutions to ICT-related problems must often be developed speedily but the solutions should be well thought-out and dependable.

These ‘paradoxes’ are, of course, to be seen, not as logical impasses but as practical and theoretical difficulties. They may also be seen as arguments against the radical version of the traditionalist’s view (the ‘business as usual’ view). Above all, the traditionalist’s view is based on two shaky presumptions: (a) that ICT is a relatively simple phenomenon that does not pose demands for legal rethinking, and (b) that a fragmented or piecemeal approach is sufficient, i.e. that the legal problems of ICT can be solved when they come into view and without any need for efforts to apply holistic thinking.

Moving away from the traditionalist’s standpoint can mean a variety of things. To begin with, ICT law may be structured and delimited in different ways. As we have already discussed, these differences have to do, among other things, with the diverse criteria that can be used to structure and classify. For one thing, the criteria may be theoretical or practical, and they may be more or less closely related to the kind of interest taken in the technology. Thus, there are efforts to treat ICT law as ‘information law’, i.e. as a general law of information handling. Such a view involves obvious difficulties of delimitation and invokes needs for a theoretical basis founded in both jurisprudence and information science. Typically, information law advocates tend to look for structuring criteria in the different stages of information handling (collection, storage, ordering, etc.) and take an interest in information processing whatever the kind of tools that are being used. For natural reasons, it is mostly academics who engage in this kind of thinking. On the practical side, the flow of treatises on ‘Computer law’, ‘Internet law’, ‘Cyberspace law’, ‘Software law’, and so on continues to swell. This literature at least bears witness to the steady interest taken in ICT law as a field of legal practice where special expertise is appreciated and where issues are often treated across areas of law such as contract law, intellectual property law, insurance law, tax law, penal law etc. A sort of interdisciplinary treatment, one may say. Of course, the ambition with regard to integrated analysis varies. Many treatises are little more than compilations of comments on assorted ICT-related legal issues that could equally well have been treated separately.

One question remains: what of the legal use of ICT? Is it completely separated from the notion of ICT law? At first sight, the answer may seem obvious, namely that ‘use’ and ‘regulation’ are two different things that have nothing in common. A closer look, however, makes the answer less obvious. For both pursuits there is a need for an understanding of the complex phenomenon of ICT, not only an understanding in general, but a legal understanding, i.e. knowledge of technology in the legal perspective. A

bond between the two subjects, yes, but the question is, how strong? Is it only the superficial fact that ICT is of interest both to those who are engaged in legal uses and to those who work with its regulation? No, there is more to consider. Let us return to the interest taken in a possible theoretical platform or basis for a notion of 'information law'. Generally speaking, a deeper understanding of ICT law appears to require a deeper understanding of ICT phenomena and how ICT interacts with the law. In this way, attention focuses not only on legal uses of ICT in a simple sense (automatic calculation of social security benefits or contracting through e-mail, for example) but on legal aspects of uses of ICT in society in general. Consider, for example, use of ICT by financial institutions or use of ICT in commerce. They are not first and foremost "legal uses" but certainly important enough from the point of view of legal regulation. One way of summarising this use/regulation connection is to say that ICT creates new environments or a new infrastructure for legally orientated activities and that, in consequence, more and more uses of ICT in society become a legal concern and must be closely studied. Some aspects of this task will now be considered.

3 A complex interaction

Many committees and study groups have done their best to chart the *legal effects* of ICT. Others have studied *legal obstacles* to the development of ICT uses in society. Both starting points are viable, but the "effects and obstacles" approaches both risk being too narrow. The reason is that 'law' and 'ICT' should be seen as mutually preconditioning phenomena. In other words, the two phenomena interact in more or less dynamic and complex patterns. The study of this interaction should not limit itself to certain simple effects and obstacles at a given point of time.

Consider as an example the emergence of electronic documents. The initial legal effect consists in uncertainty regarding their treatment. Briefly, should they be equalled with traditional paper documents or not? The search for an answer soon makes it apparent that the question has different answers in different legal contexts. If all is well, the most pressing problems are solved through actions of the lawmakers, development of case law, elucidatory comments by legal scholars, and so forth. But technology never rests. Among other things, changes in the electronic environment can bring about factual situations that may or may not have been foreseen. Consequently, legal solutions that were

well-suited at a certain stage may become uncertain or even disputed and in need of review. On the other hand, it may be considered necessary to impose constraints and requirements that shape or re-shape the electronic environment in a legally acceptable way. For example, if there is found to exist a legal need for "original" electronic documents, then the technical tools for producing such documents must be developed and used in the relevant situations.

The example is sketchy and simple. Nevertheless, it suffices to illustrate that what is initially looked upon as a simple conceptual issue ("can documents be electronic?") will soon turn into more or less complex questions of an interplay between law and ICT over time.

Above the level of single concepts, similar conclusions may also be drawn. Consider, again, the notion of *integration* (convergence). It refers to the fact that digital information processing and communication brings with it the disappearance of borders of different kinds. Some examples of such disappearing or increasingly fuzzy borders concern technical equipment (e.g. the mobile phone becoming a computer terminal), markets (e.g. the software firm becoming a vendor of communications services), and the public and private sectors (e.g. private companies performing information services for public authorities). All these and other forms of integration have resulted in needs for reappraisals of legal regulation that has relied upon stable borders and the possibility of upholding different regimes for different sectors or phenomena. Debates and analyses have been going on for decades and illustrate well the difficulties of coming to grips with the changing interplay of law and ICT.

A third example has to do with legal use of ICT, *viz* automation and data networks in the administration of justice in a broad sense, i.e. use of ICT in lawmaking, in the judiciary, in public administration, and so on. By now it is generally accepted that much more than simple efficiency improvements and basic retooling (word processing replacing typewriters) is involved. In fact, as present endeavours in Sweden and elsewhere illustrate, the very foundations of the legal order need to be scrutinised. Suffice it to mention two examples: (i) the structure and functioning of the criminal justice system (questions associated with data flows between the different actors, rules on evidence and use of digital media in the courtroom, changes in the overall organisation of the courts, etc.) and (ii) the respective roles and responsibilities of the state and of private parties with regard to the storage and dissemination of legal sources (what information should be regarded as a common good available without cost to the citi-

zens, and to what extent should the state refrain from providing information services that may come close to a new form of law-making?).

As already remarked, the issues are neither new, nor can they be formulated and solved once and for all. They aroused theoretical interest already when ICT was at a more primitive stage and its ramifications more uncertain. One of my own contributions to this early discussion was a theory of "legal system management" (in "Computing Law. Perspectives on a New Legal Discipline", Liber 1977). To summarise a complex argument, legal system management as it was presented in the monograph concerned both the management of legal information systems proper, such as the ones designed and operated for the courts, and management of legal aspects of information systems of other kinds such as systems aiming at strengthening participatory democracy and systems for rights administration and the like. The basic thoughts have already been presented above, *viz* that the complex and dynamic interaction of law and ICT (at that time referred to as EDP, Electronic Data Processing) requires serious attention and even some new legal thinking. In practice, the theory has found an expression in, among other things, the notion of a "satisfactory openness structure", i.e. basic requirements that Swedish public authorities design and operate their information systems with due regard for the right of access to official documents (see Chapter 15 of the Secrecy Act (1980:100)).

Today there is a relatively widespread awareness that law and ICT interact in various ways: that the one may steer the other, that they may complement one another, and that they may counteract one another. Viewed in this way, law and ICT form part of a whole, and abstract reasoning in the 1970s about, for example, the need for a legal "structural theory" of data processing has become practical concerns in relation to computer programs that put legal norms into operation, rights management systems, privacy enhancing technologies, filtering of harmful content on the web, and so on. Even in the USA, where "computer law" has tended to be a predominantly practical concern, the interest taken in theoretical and structural aspects appears to be growing. A recent example is Lawrence Lessig's lucid analysis of the interplay of legal regulation in the traditional sense and the design of computer programs and other elements of information processing systems.[1]

---

[1] A useful illustration of the early discussion may be found in Herbert Fiedler, *Forschungsaufgaben der juristischen Informatik*. In: EDV und Recht. Möglichkeiten und Probleme. Hrsg. A. Kaufman. Berlin: J

Against this background two assertions may be made. Firstly, ICT law is not devoid of a theoretical basis. On the contrary, the complex interaction of law and ICT opens up a field of interesting and challenging questions and possibilities, many of which have yet to be exploited. Secondly, even if one accepts the traditionalist's view that ICT law is to be looked upon as a collection of legal issues belonging to different established fields of law (contract law, administrative law, penal law etc.), the collection need not be indiscriminate but can and ought to be shaped according to particular points of view.

4 Points of view

The world one sees depends on one's view of the world. This truth is old and well-known to us all, although we are apt to forget it. Thus, the question of whether there *is* such a thing as ICT law oversimplifies things and must be reformulated. One way of doing so is to pick a number of viewpoints and use them to reflect on some Swedish experiences.

As for the viewpoint of *legal practice,* for some legal practitioners ICT law appears to constitute a distinct field of expertise whereas others are inclined to let it melt into the classical pattern of general contract law, tax law, labour law, penal law, and so forth (cf. the contribution by Viveca Bergstedt Sten). Clearly, views depend on the kind of professional and commercial interests taken in the subject matter. For a lawyer specialising, for example, in issues of software contracts (different types of contracts, existing standard contracts, proprietary rights, insurance coverage, practical concerns etc.) it will be natural to emphasise the bonds that tie the issues together. For a lawyer specialising in tax law or in general company law, the ICT issues naturally form part of a legal framework where their distinctiveness is a minor concern. However, the law firms that offer advice on matters of ICT law should not be regarded as vendors of snake oil. To the extent that they base their claims to expertise on area-specific knowledge and experience, they are just as serious as the ones offering specialist advice on matters of maritime law, building law, media law, or whatever.

Turning to the viewpoint of *lawmaking*, one finds that the Swedish Ministry of Justice has a number of sections for different areas of law (private law, administrative law, penal law etc.).

Schweitzer 1973. EDV und Recht, Band 6. As for Lessig, see *Code and Other Laws of Cyberspace*. New York: Basic Books 1999.

Matters of ICT are distributed among these sections, so that intellectual property rights are handled by one section, protection of personal data by another, and so forth. As a consequence there have been difficulties with regard to co-ordination and practically no development of a sort of "meta knowledge" about the regulatory issues of ICT (cf. the contributions by Per Furberg). Some people may regard this as a weakness, whereas others will point to the advantages of the existing organisation and emphasise the value of developing and applying in-depth knowledge of traditional fields of law instead of organising work crosswise.

In academic *teaching and training*, the law faculty of Stockholm University offers an example of how issues of law and ICT may be treated in an integrated fashion at different levels of activities. During their first year of study, the law students are introduced to ICT as a field of legal interest from the point of view of both usage and regulation. The course totals six study weeks and is labelled "legal informatics" (rättsinformatik). Its main difficulty is to be found in the student-beginner's superficial knowledge of law and legal thinking. Nevertheless, it is possible to address at least some fundamental issues of ICT and law, the problems of security and vulnerability, for example. The obligatory basic legal informatics course is followed by elective one-semester courses dealing with particular aspects of ICT law such as e-commerce and information risk management. Many students also choose to write their final "graduation paper" on matters of ICT and law. As for post-graduate courses the faculty offers an international programme in "Law and Information Technology". The one-year program reflects the basic strategy by spending time both on more conventional study of ICT law and on methodological issues associated with such issues as legal system management (cf. above), structuring of legal information (XML and related tools), and automation of legal decision making. Above the master programme level, there is a doctoral programme. At present, theses are underway on access rights regulation, freedom of expression and new media, rights in databases, and information security issues. To summarise, for a law faculty that decides to include law and ICT in its syllabus it is not difficult to design suitable offerings and find a place for them in its curriculum. It may be mentioned that courses in "legal informatics" are also in demand in other branches of Stockholm University, not least the Department for data and system science. In particular, courses on ICT law basics attract a considerable number of students.

Last but not least there is *legal science*. By now, the study of law and ICT has gained recognition as an area of specialisa-

tion. But just as in legal practice, views differ regarding its significance and its future. There are also varying views on how it ought to be conducted, i.e. views regarding its delimitation, its centre and periphery, its relations to traditional branches of legal science, and so forth. The situation for the field at the different law faculties in Sweden varies accordingly. Basically, three approaches may be distinguished. One may be described as disinterest, i.e. the field is not perceived of as worthy of any particular, methodological attention. Another approach recognises that there may be merits in paying attention to the field as a whole or, at least, that it is fruitful to organise co-ordinated efforts to study its various aspects, even if such efforts had better be placed into the framework of the traditional disciplinary matrix. The "Lex Cyberia" programme at the law faculty of the University of Lund may be seen as an example of this kind of approach. The third approach is to be found at the law faculty of Stockholm University, where the teaching programme described above is matched by ambitious scholarly work aimed at developing "legal informatics" as a sub-field of legal science. The project got going in the mid-1960s. In 1968 the Faculty Board formally agreed to set up a special working party for law and EDP, later to be renamed "the Law and Informatics Research Institute" (IRI). Thus, work has been going on for about thirty-five years and the IRI is by now a well integrated part of the legal science endeavours of the Stockholm University law faculty.

To summarise. 'Law and ICT' is variously perceived, depending upon perspectives, professional interests etc. This diversity is hardly surprising and is to be welcomed, at least so long as the different views challenge, enrich, and develop one another. The important thing to keep in mind is the complex and powerful nature of ICT. It is an amalgamation of old and new information utensils (alphabet, paper, calculator, map, telegraph, camera, radio, motion picture etc.) in a joint, basic "electric" format (to return to McLuhan's terminology). Many experts believe we have so far seen only a fraction of the changes that this amalgamation is capable of bringing about on both the societal and the individual level. Some of the changes will be deep, others shallow. It is my conviction that this also holds true with regard to the legal order and that the task of observing, analysing, and understanding the interaction of law and ICT constitutes both a challenge and a responsibility for legal professionals, be they academics or practitioners. To put it simply, many "technical" issues are in fact "legal" and an increasing number of traditional "legal" issues come shrouded in "technical" concerns. Law and ICT are more of a wholeness than many of us realise.

Håkan Hydén*
Remunerative Gifts, Societal Development and Legal Futures

1 Thinking about potlatch

As a law student, I came across a legal term, remunerative gift, which made an impression on me. What caught my interest was the hybrid character of the concept, the same kind of confusion as in the concept, self-employed, which I comment on below under. Remunerative gift is something midway between *obligatio* and *donatio*, between a binding contract and a free gift.[1] Over time it also has been treated in these different directions. Remunerative gift is defined as something given to remunerate past services.

There, for my part, the matter rested, until recently when I read a book written by Alf Rehn, titled *Electronic Potlatch* (KTH, Stockholm, 2001). In it, Rehn identifies similarities between new technologies and primitive economic behaviours in terms of a gift economy. He draws parallels between the gift economy among the native Americans of British Columbia and the inhabitants of the virtual land of Warezonia, which can only be reached through the screen of a computer. The Native Americans lived in a gift economy. One central element in realising the gift economy was to give a potlatch, a feast. It was a social gathering of great import. What is interesting is its economic importance, but it is also central to social structure, politics, religion, morality and law within the community. It has been used as an example of a "total social phenomenon".[2] Potlatching was, thus, a reflection of the native society as a whole. From a legal point of view it is interesting to note that the economy was regulated by social norms. Describing the gift, Marcel Mauss sets out the origin of economy. The potlatch can be regarded as a game where individuals were given status and identity, within an activity having implicit economic functions.

---

* *Håkan Hydén* is member of the IT Law Observatory. See presentation in Annex 1.

1 See Reinhard Zimmerman, *The Law of Obligations. Roman Foundations of the Civilian Tradition*. Cape Town: Juta & Co. 1990

2 Marcel Mauss, *The Gift: The Form and Reason for Exchange in Archaic Societies*. New York: W.W. Norton, 1924/1990.

Briefly, Warezonia, consists of groupings of people that compete in giving away commercial software and the people who participate in this as either intermediaries or "fans/consumers". At the centre there is the hard core of the scene, consisting solely of those who give software to others, with the aim of being the most efficient and overall best provider of warez, i.e. programs, software. Any social structure has of necessity one implicit norm, the norm of continuing participation. In the social scene of Warezonia the rule regarding participation is stated by Rehn to be one of sharing and movement (pp. 139-140). To be a warez dude, you have to be a party to the circulation of programs/warez. The circulation of warez, in other words, is the social structure, and the actors merely assume various positions in this structure. The norm of sharing is perhaps the most telling. What is implied in membership in Warezonia is that you are part of the networked sharing on the whole. Not to do so is to disassociate yourself from the community. The other implicit norm, movement, refers to the continuous striving for total coverage, i.e. that all new releases are to be had at all relevant sites as quickly as possible.

Warezonia also has additional, explicit norms of what constitutes the good and the just. These norms are speed and functionality. Furthermore, we can speak of norms regarding primacy or origin. Following these norms, you are a successful participant in the community activities. Last but not least, we have the norm of giving. A warez release can only be given. The absence of money, or more precisely the absence of price, is a condition for Warezonia's gift economy. A release can have no price, although it can have a value. The work done within the circulation of warez is thus seen as a gift to the scene, as a contribution towards a greater good. To be good is, quite simply, to be a productive member of the community.

Alf Rehn claims in his book that the structure evident in the Potlatch is structurally synonymous to the structured interactions of competitive giving on the warez scene. The way in which the societies of the First Nations were structured wholly around the practice of the potlatch, with social life within the tribes being dependent on it, is mirrored on the warez scene. In both cases, Rehn points out, it is the process of giving and proving one's mettle that gives meaning to the social, and the material instances of exchange can be viewed as mere instruments for a "higher" purpose (p. 276). Based on observations regarding the way in which the rituals of the potlatch changed with the introduction of Western trading posts and similar instances of the market economy into the territories of British Columbia, Mauss has referred to it as "the monster child" of the market and the gift. Warezonia,

says Rehn, could in this vein be called the return gift, the monstrous introduction of gift-exchange into capitalist hegemony (p. 294).

Several other authors have raised the same point as Rehn about the feature of a gift economy within the new economy.[3] Raymond calls the development model belonging to the spirit of the new economy the Bazaar, as contrasted with the Cathedral, which characterises the commercial world of the old economy. Referring to Linus Thorvalds, the promoter of the open source based operative system, Linux OS, Raymond speaks of Linus' law: "With a sufficient number of eyes all bugs will be noticed." He regards egoboosting as the fundamental driving force behind an open source mentality, which gives it the features of a gift economy. The utility function hackers produce is not a question of classical economy, but is the intangible of their own ego satisfaction and reputation among other hackers. There are, according to Raymond, many voluntary cultures which operate in this way.

The young Finnish philosopher Pekka Himanen has described the same phenomenon in his book, *The Hacker Ethic and the Spirit of the Information Age* (London: Secker & Warburg, 2001), where he enumerates seven values of the hacker ethic that have had a significant role in the formation of the new society. A hacker who lives according to the hacker ethic gains the community's highest respect, he reaches the final level and gets the seventh and final value, which is creativity. This is in Himanen's description "the imaginative use of one's own abilities, the surprising continuous surpassing of oneself, and the giving to the world of a genuinely valuable new contribution" (p. 141). What characterises a hacker ethic is the co-operative structure of coders, where ideas and codes are shared, and work is done primarily out of enthusiasm and the joy of participating in a social sphere. But this is not a gift economy according to Alf Rehn of the same kind as in the Warezonian case, for two reasons: the problem of meaning and that of novelty.

Rehn claims that hackers, like the Protestant worker, find work in itself to be meaningful. They are climbing the ladder of accumulation. For the Warezonians, however, the scene makes sense in the same way as the Native Americans found meaning in the potlatch. The other point, on which Rehn criticises Hima-

---

[3] See, for instance, Eric Raymond in his famous essay *The Cathedral and the Bazaar: Musings on Linux and Open Source By An Accidental Revolutionary*, London: O'Reilly, 2001. In his analysis of the open-source movement Raymond has made explicit the way in which the "hacker" culture behaves as a gift economy.

nen´s book concerns novelty. Himanen, like many others addressing the network society, emphasises the paradigm shift that the new technology has created. It makes it seem that we, as humans, are entering something wholly new, Rehn describes it, and he continues: “This is the direct opposite of my contention. The technology might be new, but there is precious little that is new about society.... what is truly spectacular about the social world is not its newness but the way in which it has remained unchanged” (p. 303).

The interesting thing is that both Rehn and Himanen may be right. As so often, it is a question of how one specifies the underlying world view. Both Rehn and Himanen regard information technology as something new. They both also accept that this technology creates new things and material wealth. But while Himanen finds a new society representing a challenging alternative spirit of informationalism, Rehn is sceptical and looks at our daily lives, finding that not much has actually changed. We still have friends over for dinner, we still give alms, and we feel for those who have less than we do. Culture might bring radical variations and things can recur in numerous settings, but these alterations take place within the same theme of human behaviour, if I understand Rehn correctly.

The behaviour of the Warezonians shows remarkable similarities to that of the Native Americans. In both cases, the communities draw upon the surplus of the market economy in order to create economies that squander. In both cases, outsiders consider this criminal. Potlatching was terrifying enough for the Canadian legislature of the time for legislation to be passed against it. The same tendencies can be seen in relation to the practice of warez. The Native Americans adapted to the new economy at that time in a fashion that is hard for us to understand. They created a hybrid form, just as the Warezonians have created a marketplace for honour and gifts. The legal hybridity, remunerative gift, corresponds to the normative asymmetry in a society as a whole where the social structure belongs to one mind-set and the dominant economic rationality belongs to another. This was obviously the case for the Native Americans and what has probably characterised transitional periods from a gift economy to a market-based economy in other parts of the world, including our own. The question is what conclusions can be drawn from these experiences. Are we facing something new or not? The answer is both yes and no. Let me explain.

2 The long waves

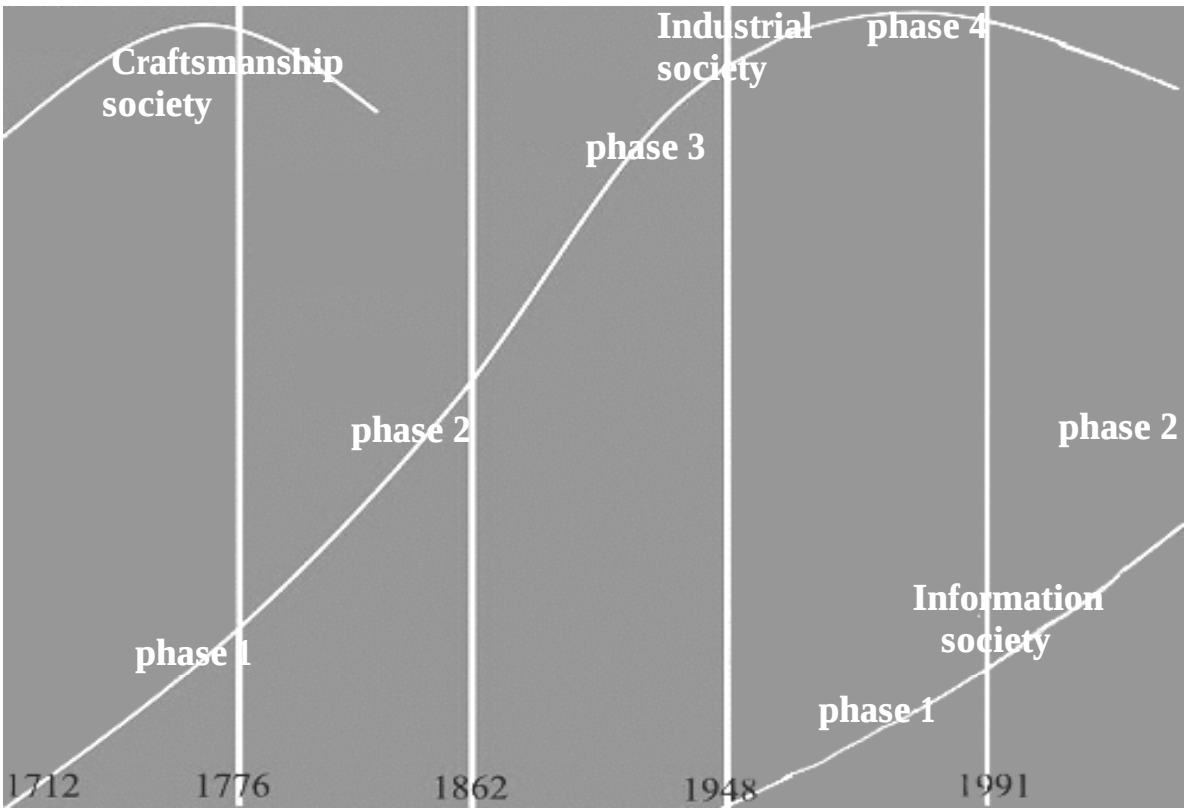
Information technology is a core technology, i.e. a technology, which needs itself to develop further and which is broad and deep enough to trigger the creativity and imagination of people for a sufficient length of time. Hand-tools were needed in order to make more and better tools. Precision mechanics helped to develop new precision mechanics, such as clocks. Steam engines were a prerequisite for the construction of more and more effective (steam) engines. Computers are used in order to create new generations of computers. This kind of technological development has, without a doubt, implications for society. Each of these technological periods marks a certain era in the development of an epoch. Thus the industrial society is the last era in the Market epoch, which can be traced approximately 1,000 years back.

The Market epoch was initiated by the businessman era in the beginning of the last millennium, followed by the era of the trading houses and the handicraft era. When mankind in the beginning for the first time learned how to produce and distribute artificial energy, starting with the steam-engine in the beginning of the 18th century, later complemented by electricity, a new core technology with societal implications was born, the industrial society. Many existing machines could then be used much more effectively, with much higher productivity. An era goes through four phases of about 75 years, following a certain pattern. In a biological perspective one can speak of birth, adolescence, maturity and death. In a societal perspective, changes take place in a certain order following the phases that have now been mentioned. A new society is born with the new (core)technology which marks the first phase. The next step in the formation of a new society is the social phase as an expression for the need of social adjustments and alterations due to the implications of the new technology. When the core technology is established and developing and the society adapted to the new conditions, it is time for large-scale economic exploitation of the new technology. This is the heyday of the era, a time of linear development, when the mentality shifts from synthesising to specialisation and reductionism. For the industrial society we are talking about the time between the beginning of the 1860s and late 1940s. After a period of economic production of material wealth it is time for the political system to take the lead. At this time in history the accumulated surplus value calls for mechanisms for distribution. This becomes an important part of the political system in combination with corporate structures of different kinds. Later on the

over-ripeness of the system necessitates political interventions in order to avoid crises of legitimacy.

In this way something new can be said to take place. Technological development creates new and technically more advanced possibilities of providing for human needs. But this is just one side of the coin. I return to the other side shortly. The best graphic illustration of the societal development is the horizontal S-curve or a wave. The S-curve is constituted by the combination of the law of increasing returns and the law of diminishing returns. Together they form the horizontal S, as in the following figure:

Benefit



Time

The different phases indicated in the figure correspond to the ones commented upon above. The shift from one society to another is a question of developing a new core technology. It is noticeable that a new core technology starts as a reaction to the old one already before this one has reached its peak. Inventors, artists and other forerunners recognise the law of diminishing returns long before the economy shows itself to be on the downgrade as a whole. This also means that the first phase in the growing society is parallel to the fourth phase in the old society. It is phase 4 which dominates the mental processes. The new technology is

first applied in the old production structures and thereby speeds up the process of decay. Similarly, new social phenomena are interpreted and received within the mental structures of the old society. This tendency is explained by the prevailing institutions and the vested interests related to them.

The initial part of the process has a negative return, as indicated by the S. The economists call this phenomenon, the productivity paradox. In the mid 1980s, when everybody was talking about and started working with computers, this had no impact on the economic statistics. From a micro-economic perspective, the question that accompanies the paradoxical state of the initial phase when a new society is born, concerns incentives and motivation. What are the social-psychological driving forces among actors underlying an economy that is not remunerative for those involved?

As we can see from the discussion above, there are different, optional understandings. One is the mentality of a gift economy. In relation to the information society and the so-called new economy, Alf Rehn's story about the Warezonians is an illustration of that. The affluence following on the large-scale industrial economy has created a basis for a gift economy within a small but expanding sector of society. When the technical barriers to duplication are removed and when a program can be copied a thousand times at basically no cost, a particular form of abundance is at hand. The day someone succeeds in putting a price on the digital goods by being able to give them the right package, the gift economy will turn into an exchange economy. A second possible explanation is the hacker ethics connected to the open-source movement. For those coding enthusiasts, devoting time and competence to a development project is to a great extent accepted as a gift to the larger community, and prestige in this community is a direct effect of either egoism or altruism. This behaviour is also rational from a societal point of view. The ethos of being open has shown itself more dynamic than and implicitly superior to 'normal' program development, due very much to the social aspects of such an approach and the creativity which a freer system assumedly bestows upon a project. A third possible explanation of driving forces, explaining why the economic process is developed despite lack of economic remuneration for actors involved, is related to the dedication and devotion of those individuals to the joy of innovation and creativity. All three interpretations might be true at the same time, but for different actors and different parts of society.

3 A future for IT law?

Somewhere along the way the morality of the gift gets lost, but we can trace back barter and market exchange to their original forms, the total social phenomenon of the primitive gift. The legal construction of the remunerative gift marks the step from a gift economy to an exchange economy. In the transitional period, law has to be used to enforce and uphold the old structures while the new ones grow organically through a continuing social process, where certain patterns of behaviour become entrenched and turn into the "real" reasons for engaging in a particular activity. In this way gifts turn into exchange relations via the remunerative gift conception. This story has certain implications for an understanding of the role of law and legal development.

Law does not come into play until a societal phenomenon is threatened, i.e. cannot reproduce itself by itself. As long as something is growing spontaneously, it organises itself according to principles of self-regulation. It is probably when the gift-economy is threatened and in dispersion that the gift becomes a remunerative gift and the law comes into play. Established segments of society are using law in order to uphold norms and institutions. Law is nothing but spontaneous norms that at a certain point in time have been given a special status and protection of the legal machinery.[4] After the initial – gift-oriented, egoistic, altruistic, dedicated – phase of the new society based on the new core technology, the law of increasing returns predominates.

If we apply this reasoning to society as a whole and the role of law in relation to its development, the following conclusions become valid. As long as the law of increasing returns is operating, activities in society regulate themselves. We can hear talk of self-regulation. When the law of diminishing returns takes over, the role of law increases. The transformation from self-regulation into a fully-fledged legal system goes step by step. The first stage is that of rules of the game, where law only provides certain basic norms for the co-ordination of activities. The activity as such is then still unaffected. The legal system sets up limits for socially acceptable behaviour within penal law and provides instruments for co-operation in terms of law of contract and of property, etc within civil law. The next step corresponds to the initial part of the fourth phase in the figure above. When the political system comes into the arena, then law becomes a political instrument. This takes, firstly, the form of public law, primarily in order to

[4] These aspects are elaborated in Håkan Hydén, *Normvetenskap* (Norm-science), Lund studies in Sociology of Law nr 11, 2002, chapter 4.

entitle public authorities with competence to act on behalf of the politicians when providing the public services which are asked for at this time in history. Later on, in the dying phase of the old (industrial) society, the state has to intervene in order to hold society together. Law, then, changes character and becomes an intervening tool where public authorities are engaged in controlling more and more private activities. In this last phase the legal system tends to be overloaded and to have lost its soul manifested in what is called frame-laws.

Changing perspective from the upper curve of industrial society down to the lower curve of information society means, according to what has been said and what can be learned from similar transitional periods earlier in history, going from state regulation to self-regulation. This is due to certain common patterns of the transition.

These situations are characterised by a shift of focus from large scale to small scale. It is a question of looking for new ways of fulfilling old human needs using the new technology. Another transition is from planned to random processes in society. We are leaving a time of planned production and random consumption in favour of a time of random production and planned consumption.[5] Wealth in future will depend on sufficient diversity of visions and strategies being mobilised, i.e. more risk-taking and trial-and-error operations. In this transition, society changes social and economic codes, norms and taboos are altered and some legal rules become obsolete. The formal structure of a code appears at the moment when production declines and/or the appearance of meaning fades. In the perspective of the industrial society, we are faced with a situation where corporate loyalty will probably cease to exist and the old (social) contract between company and employee will disappear. We will later on imagine a new social contract. These are examples of factors which contribute to the understanding of the normative changes in society of our time.

When it comes to law, these changes follow a certain pattern, going from pure self-regulation to self-regulation with legal support, to legal regulation and state intervention. The interesting thing, though, is that during its flow in time the legal system is confronted with the same kind of issues when entering the different societal eras. There is, in that sense, nothing new under the sun. The famous sociologist of law, later the early 20th century Austrian prime minister Karl Renner, has shown, in his book

---

5 Anders Ewerman, *Marknaden 1000 år* (The Market 1,000 Years). Falun 1996.

Private property and its social functions, that the concept of property has been the same over the last two thousand years, but the substratum has undergone radical changes. The legal content has been unchanged, despite the changing socio-economic implications. Thus, during the time of Roman slavery, private property meant a relation between a subject and a subject, while also accepting a relation between a subject and an object, which became the typical character of the concept. Later on, during the period of large-scale industrialism and the wage-earning system of capitalism, private property once again became a relation between a subject and another subject. Finally, in our time of state interventionism, private property was accepted as limited by state regulations of different kinds. These changes in practical implications were possible due mainly to the fact that the property concept over time has been connected to various other legal concepts, the law of contract, of security rights, public law, etc. in different combinations.

What are the consequences for the forecasting of law of the information age? I think there is reason to talk of a particular IT law. But following the reasoning above, one should not expect a lot of new legal constructions and concepts. Established legal principles will do, but they might be combined and put into new contexts, which will affect their socio-economic substratum. There will also be a renewal of old concepts that might have been obsolete. For example, there is reason to expect that the old regulation about the trustee (syssloman) will take on a new lease of life. Furthermore, legal regulations that have grown into special expert fields, like labour law, can be supposed to fade out and merge with the main regulatory categories within civil law, when going from the upper, industrial society, to the lower curve of the information society. Only a few new legal concepts, like self-employed, might be needed. Most of the institutionalisation of the new information society will initially take place outside the classical legal arenas and find its way via self-regulation. The most important part of this transitional period is related to the need for de-regulation in order to set the new normative structures free. This is shown by the fact that legal development follows the curves indicated in the figure above. The present situation, the relation between the industrial and the information society, is no exception.

Law in the digital world is confronted with the same kind of eternal questions as mankind has always had to find an answer

to.[6] This is the other side of the coin. While the tail is changing, the head faces the same kind of problems over time. The Swedish word for railway engine, *lokomotiv*, is a case in point. It comes from the Latin word *locus*, meaning place, and *motivus*, meaning movement. The word *lokomotiv*, then, contains both something static, a certain place, and something dynamic, movement. It is spatial and temporal at one and the same time. Since development in the world is found to be in different eras, a spatial move is also a temporal one. The same goes for the course of law, which is spatial and temporal simultaneously. It changes its content while moving from one societal phase to another. But it is the same legal principles that are being applied to new material conditions, in our time, to new virtual realities. In that sense we are from a legal point of view looking at something new but through old spectacles.

[6] For more about these aspects, see Håkan Hydén, *Normvetenskap* (Norm-science), Lund studies in Sociology of Law nr 11, 2002, chapter 6.

Joachim Benno[*]
Why the Use of ICT Engenders Legal Problems – in Search of a Common Denominator

"...The purpose of a deeper perspective is above all to provide opportunities for more initiated discussions and more soundly based proposed solutions. In many fields, therefore, this can be just as much a question of looking up and perceiving the connection between different activities and different types of legal solution. This is something which can require far greater analytical inputs, because the material will be more extensive, but it is at the same time a method which can lead to far more uniform and appropriate solutions."

Peter Wahlgren [1]

1 In search of a common denominator

The emergence of the "information society" confronts legislators, judicial practice, businesses and individuals with regulatory challenges of apparently unprecedented extent and complexity. At the centre of it all we have the Information and Communication Technology (ICT), not only as the motive force of development and of the possibilities which the information society affords, but also as a factor generating legal problems which have to be dealt with. Most traditional areas of the law are affected, often by common and at the same time overarching problems disturbing not only specific legal issues, but also basic structures of the legal system as such.

Although legal aspects of the use of ICT have been addressed and dealt with by academics in the Nordic countries since the late 1960s, it is only since the 1990s that ICT-related legal problems have gained more general attention through all

---

[*] *Joachim Benno* is a member of the IT Law Observatory. See presentation in Annex 1.

[1] Peter Wahlgren, *Rättsfrågor kring tjänster i nät*. In:: Nordisk Årsbok i Rättsinformatik 1996. Martin Brinnen, ed., Stockholm, Norstedts Juridik, 1996, pp. 49-58, 53-54. (Freely translated)

levels of society. The basic reason is that the technology and its use are achieving a higher grade of penetration and are thus bringing the problems out from the rooms of academics to the practical spheres of everyday life. The basic driving force is, of course, the continuing development of the Internet and the World Wide Web as open and standardised platforms enabling small companies, the public sector and households eventually to make broad use of ICT as a tool for communication and the carrying out of different types of transactions.

> In the present account, the term "transaction" is used in the broad sense, so as also to include unilateral acts and activities, such as criminal acts and situations where somebody uses a freely accessible database in order to transmit or collect information, without necessarily entering into a contractual relationship with the provider of the database.

However, even though there is a vast amount of literature, reports, public investigations, etc. concerning ICT-related legal problems, these are generally devoted to specific legal problems or areas of the law. Overarching studies exist, of course, but strikingly little attention seems to have been devoted to understanding the basic question in this context, namely *why* the *use* of ICT, in itself, engenders legal problems.[2]

In effect, in such cases as described, the problems in question are often sought to be solved without a deeper understanding of what it is that actually generates the very problems to be solved.

The purpose of this article is to draw attention to, and shed some light on, the question of why the use of ICT engenders legal problems. The article demonstrates the possibility of pointing to common factors – denominators – making it more difficult for individuals, businesses, legislators and judicial practice to understand and deal with the transaction and its environment.

This is not just an academic question. The possibility of pointing to one or more common denominators to the ICT-related legal problems arising, not only provides opportunities for better understanding the nature of the problems, but also creates oppor-

---

[2] A good exemption, well worth studying, is Herbert Burkert, *Which Law for the European Information Society?* (text of a presentation given at the EC Information Day for senior executives of IEPRC, ICRT and EPC Brussels, 31st January 1996), http://www.gmd.de /People/ Herbert.Burkert /Brussels.html (as of 16th March 1998 at 10:47 am). See also Peter Seipel, *Computing Law. Perspectives on a New Legal Discipline*. Stockholm: Liber 1977.

tunities of problem solving in a wider perspective, in which the solution in one area can also furnish guidance for solutions in others.

This in itself provides for better results in legislative and judicial activities and, furthermore, for businesses and individuals to protect and vindicate their rights in different situations. Businesses which devote resources to gaining a deeper understanding of the regulatory framework governing their business activities, will find themselves in a better position not only to handle regulatory issues in a cost-preventing and value-adding manner, but often also in gaining competitive advantages by feeding this knowledge into business strategy, product development and the handling of public/regulatory affairs.

2 The cause and effects

2.1 The transforming character of ICT

Most of the legal problems arising in the context of ICT do not concern new, unregulated, legal phenomena. On the contrary, in most cases they concern "traditional" transactions, where the *use* of ICT to *perform* the transaction renders current law incapable of serving its intended purpose. To understand why the use of ICT has this effect, one must firstly understand the changes ICT brings about as a tool for performing different types of transactions.

Basically, ICT provides new ways of performing transactions and at the same time is transforming the environment in which transactions take place. Compared with more "traditional" ways of performing transactions, the use of ICT has the effect of dissolving the contours of a transaction and blurring the difference between different types of transaction. In addition, transaction time inputs are diminishing and geographical distance is ceasing to matter. Ordering goods and services, carrying out banking transactions, making travel and other ticket reservations, collecting and passing on information – all these things, and much else besides, can be done through one and the same medium, from one and the same position, without the parties involved needing to move from A to B or meet face to face.

Another way of describing this is by saying that ICT is transforming the characteristics of the transaction, and entities such as

time, *frame* and *space*, as determinants of the perception and performance of different types of transaction.[3]

2.2 Effects on insight, understanding and perception – consequences for individuals, businesses, legislators, and judicial practice

The above-mentioned changes make ICT-assisted transactions more difficult to trace, identify and distinguish, in relation to more "traditional" ways of performing transactions of different kinds – the transaction, its features and consequences, becomes more difficult to "grasp". The consequences for individuals and businesses are manifested through less knowledge of the transaction as such and of its various elements. These effects are accentuated by the problems of knowledge and understanding already entailed by the technology underlying the transaction.

In more concrete terms, the use of ICT can make it more difficult to *distinguish between different types of transaction* whose performance, previously, demanded measures that were more distinct and distinguishable. That which, in reality, would seem a manifest impropriety to the individual, becomes harder to distinguish in an electronic environment. The connection between act and consequence becomes less clear and the borderline of the impermissible therefore becomes easier to transgress, both deliberately and inadvertently. For example, appropriating other people's banking assets through the Internet by cracking their PIN codes can be expected to provide a lower moral threshold to cross, than the physical act of breaking into and robbing a bank.

Furthermore, it is probably impossible for the uninitiated web surfer to perceive the borderline between proper and improper use of copyright material available through the Internet. Perhaps he or she does not even realise that an act entails the copying of copyright material, comparable to the manifest act of copying a book from end to end and producing a certain number of copies for further distribution, with the help of a copying machine.

ICT has also made it more difficult to tell *what is required in order for an act to be completed*, and thus legally binding. This can apply both to commercial transactions, for example when entering into a contractual relationship, and to the relationship between pub-

[3] Cf. Herbert Burkert, *ibid.*. Burkert describes these aspects in the way that ICT invites – by its basic characteristics – uses that seek to overcome the limitations of time, complexity, quantity, space and physical representation, and that it does so in a manner that makes the process appear to the user as intangible, invisible and variable.

lic authorities and private individuals, for example concerning the date when a document is deemed to have been received. Even though legal rules, case law and custom may point out or indicate certain elements as determinant in these respects, it may be unclear to the parties concerned *when* these elements occur in an electronic environment and, moreover, *how* evidence of their occurrence can be secured and presented.

Another consequence is that it becomes more difficult to *identify* the other party and to decide in *what capacity* and with *what authority* he or she is acting – for example, whether the opposite number is the person he or she professes to be, is acting in a consumer capacity, has due authorisation (e.g. power of attorney), is over a certain age, and so on.

Furthermore, in connection with "traditionally" performed transactions, the individual can normally be expected to be in reasonably good *control of the information* which he or she provides, whether directly or indirectly, and reasonably able to decide *who* receives that information and in what way. The opposite applies to electronic transactions, the individual often being entirely unaware of the "electronic track" which he or she leaves behind him and, consequently, of the person or persons to whom these tracks become accessible.

To this are added the above-mentioned changes of *time, frame* and *space* as determinants of the performance and perception of the transaction. Everything happens faster, the margins for reflection and consideration are diminishing. Geographical distances are losing their practical relevance, and it is becoming less and less easy to ascertain the location from which a party trades or carries on his business, or the geographical source of information. With a growing risk of rights being lost, this leaves the user with less insight and understanding of the transaction, its elements and its consequences.

The problems which the use of ICT creates for legislators and judicial practice are to a great extent matched by the problems described above in relation to individuals and businesses, but of course in terms of the perspectives and tasks of these institutions; the transaction and its parties are growing more difficult to trace, identify, define, classify and characterise, which poses problems both in the development of new legal rules and in the modification and implementation of existing law.

Allowance also has to be made for the fact that, since the design of the regulatory structure and its implementation are to a great extent based on the possibilities of the individual understanding the transaction, its elements and its consequences, the

legislator and judicial practice must also relate to the problems which the use of ICT presents to the user.

In addition, the legislator and judicial practice must also relate to the insensitivity of technology to political boundaries, the very boundaries which impose restrictions on their competence and possibilities of action.

2.3 Effects on regulation – the framing and purpose of a legal rule

To fully understand why legal problems arise from the use of ICT, the consequences for individuals, businesses, legislators and judicial practice must be seen in the light of the design and purpose of the regulation in question.

Here, on closer analysis, one finds that the purposes to be served, the interest or interests to be protected or reconciled, are very often represented by criteria or concepts that are hard hit by the transforming character of ICT, i.e. criteria and concepts based on the possibilities of the parties or the user to understand and foresee the transaction, its scope and consequences, as well as its positioning in time and space, and so on. Consequently, the criteria laid down for a legal rule to take effect, often loose their relevance for the accomplishment of that rule's purpose and the balance sought between the different interests involved.

In the light of the above discussion, we find that the use of ICT impacts above all on legal criteria and concepts based on knowledge and perception of:

- **Who** (which person or persons) are involved in the transaction or commit a criminal act, and in what capacity that person or persons act.
- **What** constitutes the object of the transaction/protection and how this is to be classified, defined and delimited, e.g. in relation to various types of exclusive rights and to data collections of importance for personal privacy.
- **Where** the transaction/criminal act takes place, where the effect occurs, where the party/culprit acts from, where the information originates and is supplied from, where a party can be deemed to be established, and so on.
- **When** an activity has legal consequences: when a legal commitment occurs, when a document is to be deemed to have been received, and so on.
- **How** the transaction and its various stages are performed, how evidence is presented and evaluated in these respects.

3 Examples

The "blurring" effect on different types of transactions is a fundamental element in most of the ICT related legal problems that arise. The actual problems may be related to specific fields of law or to the particular contexts in which they appear. In IT Law Observatory Report 6/98 examples are given which illustrate how legal criteria and concepts, workable in the context of "traditional" transactions, either fail to serve their purpose or demand a new understanding of the same transactions, when performed with ICT.[4] The examples concern freedom of expression and information, copyright, penal law, protection of privacy, the distinction between "product" and "service" in sales law and taxation law perspectives, contract law, imaginary/virtual organisations and applicable law and jurisdiction.

From a regulatory perspective, maybe the most interesting development over the last couple of years comes from the convergence between the IT, telecommunications and media sectors. The convergence phenomenon serves as a good example of the fact that the use of ICT brings about common and at the same time overarching problems disturbing not only specific legal issues, but also basic structures in the legal system as such.

3.1 The convergence between the IT, telecommunications and media sectors

Convergence as a phenomenon can be described in various ways, depending on the perspective that is being discussed, and with varying degrees of complexity. The conditions which, in the context of technical progress, are leading to the convergence of infrastructures, services and apparatus, are fundamental. To this are added the market movements whereby actors in different sectors are involving themselves with one or more neighbouring sectors.
The legal consequences of convergence are revealed by the increasing difficulty of distinguishing between the IT, telecommunications and media sectors, which used to be relatively clearly segregated. One and the same service can, for example, come under different, possibly several, regulatory instruments, depending on

[4] Joachim Benno, *The "anonymisation" of the transaction and its impact on legal problems*, IT Law Observatory Report 6/98, ICT Stockholm: ICT Commission 1998, pp. 12-25.

the medium or channel of communication used for conveying it to the recipient or on the manner in which the recipient obtains the service. In addition, technical progress is also bringing new types of services and phenomena and new possibilities of conducting telecommunications and media activities, whose subjection to the existing regulatory systems may not be very practical or convenient.

This has to be viewed against the background of the regulatory instruments of these sectors being framed on different premises, with different underlying political motives and aims, and with different authorities in charge: The – more or less – unregulated IT sector, which, on the basis of business and consumer policy incentives, is governed by market legislation; the telecommunications sector, which is being liberalised in order to achieve effective competition for the achievement of particular aims of telecommunications policy; the media sector, which is governed by democratic and cultural policy aims, and in which the State has taken upon itself a special public service responsibility in radio and television broadcasting.

The effects which have now been described not only change the ability of existing regulatory instruments to serve their purpose, they also impact on the basic preconditions and assumptions of existing law.

For the market actors this, amongst other things, leads to difficulties in identifying the regulatory framework and the legal obligations to which they are subject when carrying on their business. This problem is accentuated by the fact that these businesses find themselves in an environment which, instead of being, as previously, characterised by a relatively simple value-chain, is becoming a market which is hard to define and is characterised by a highly complex value-system. The future success of these businesses depend on their ability to adapt to these changes, be innovative and rethink in terms of customer loyalty, product development, market positioning, internationalising and pricing.

From this perspective, the businesses acting within the converging sectors are highly dependent on a clear and foreseeable regulatory framework, which at the same time assures them of the necessary freedom of action to adapt to the changes that convergence brings about.

The proper handling of these regulatory effects is therefore crucial, not only to the businesses affected, but also to national economies depending on these involved markets to be successful and innovative. A regulatory framework that is inappropriate and ineffective will hamper and negatively effect investment and

strategy assessments, which in turn will hamper the development of new services and effective infrastructure solutions.

There has been extensive work within the EU, both at national and transnational level, for adjusting the legal framework to the progress of convergence. Since 1997 the Commission has issued a Green Paper, a working document and a communication on convergence. The experience gained from this process and the 1999 review of the telecommunications regulations, forms the basis of the new regulatory framework for electronic communications that was introduced in 2001/2002. In the so-called regulatory package to govern the electronic communications sector, a more horizontal regulatory approach is adapted, i.e. the same rules are to apply to communication infrastructures regardless of the kind of infrastructure used and the type of service mediated.

4 Concluding reflections

4.1 The transforming character of ICT – a common denominator

The discussion in the preceding sections deals with the question of why the use of ICT engenders legal problems. The discussion shows that a basic explanation is to be found in the way the use of ICT affects the time, frame and space in which the transaction takes place and thus, in turn, affects the insight, understanding and perception of different kinds of transaction.

In order to counteract and cope with the effects of the use of ICT, attention has to be focused on the use of legal criteria and concepts based upon the identification of the questions of who (party, culprit, subject for protection), what (object of, respectively, transaction and protection), where (direction, effect, establishment, origin), when (legal obligation) and how (the various stages of implementation, pleading and evaluation of evidence).

This must, furthermore, be seen in the light of the framing, wording and structure of a legal rule, its purpose and the balance sought between different interests and also with an awareness of the international perspective, with a variety of legal systems involved.

The understanding of these effects as a common denominator for the legal problems deriving from the use of ICT, not only provides for a better understanding of the nature of the problems, but also creates opportunities of problem-solving in a wider perspective, in which the solution in one area can also furnish guidance for solutions in others.

4.2 Legislative techniques to handle the problem

Various legal techniques for tackling the problems posed by the transforming character of ICT are discussed in IT Law Observatory Report 6/98.[5] It is suggested that in certain respects greater flexibility is needed in legislation, which among other things could mean less distinctness and predictability. Not infrequently, however, such legislation is criticised as providing scope for arbitrary decision-making, reducing predictability and creating uncertainty about the legal position.

Basically I endorse this reflection. Generally worded statements of objectives and general clauses must not be a "cop out" in situations where the legislator is working against the clock and with inadequate supportive documentation. This does not augur well for the quality of the result. The same goes for excessive reliance on the analogical method of interpretation as sufficient means of solving ICT related problems within the scope of current legislation.

On the other hand, this does not rule out the need for greater flexibility in legislation. To counteract the legal problems entailed with the use of ICT, it is often necessary to provide legislative solutions that allow special circumstances in the concrete case to be taken into consideration and which at the same time afford scope for the development of more exact principles in the process of interaction between legislator, judicial practice and market. In this way the codified law can become more dynamic and can grow within given frames which at the same time ensure stability; the continuity of legislation will be promoted, at the same time as the problem of rapidly obsolescent norms out of tune with technical progress can be counteracted.

It is immensely important, however, that more flexible legislation should provide clear and steady frames within which the freer assessment is to take place and which are based on the interests that the current legal rule is meant to balance or safeguard. For greater predictability and as a form of guidance, these frames can very well be supplemented by non-exhaustive examples and presumptions, i.e. guidelines.

Another approach is the, above-mentioned, "horizontal" approach, based on the principle of technological neutrality, used in the EU new regulatory package governing electronic communications. The horizontal approach in this context implies that the

---

5 Joachim Benno, *op. cit.* at pp. 25-28, 29-31.

same rules are to apply to communication infrastructures regardless of the kind of infrastructure being used and the type of service being mediated. This solution should be seen in the light of the convergence phenomenon and the regulatory implications that this development brings about, blurring the distinction between the IT, telecommunications and media sectors. Basically, this seems to be a promising and necessary approach to dealing with many of the problems arising in this context.

However, it is important within this legal framework, as well as in other situations, that the legislator should not blindly rely on the principle of technological neutrality – implying that regulation should focus on the transaction, irrespective of the technology being used to perform the transaction – to solve problems relating to the use of ICT. The principle of technological neutrality is not, and should not be treated as, a goal in itself. In doing so there is an imminent risk of losing sight of the actual aim of the regulation in question and unintentionally altering the balance originally sought between different interests.

4.3 The wider perspective

When facing the problems which ICT entails in the legal system, it is important that one should also consider the more fundamental, overarching perspective: A transformation is taking place of the whole of the society, in which the legal system is one of the pillars on which the social order rests. In democratic states, the foremost task of the legal system is to manifest and maintain the democratic ideals, and legislation is framed in conformity with those ideals.

One of the greatest risks here is that the complexity and rapidity characterising the development of the information society will result in prevailing ethical and moral values being undermined and changed without any standpoints being consciously adopted (cf. the above discussion concerning the use of the principle of technological neutrality).

This is not to say that there can be no reason for a revaluation of prevailing views, but this must be done on the basis of a deliberate standpoint concerning the consequences that this may have for both democracy and the individual. Among other things this has to take place within the democratic process and with an open, initiated debate in which everyone has an opportunity of taking part.

Per Furberg*

Lawmaking and IT: Reflections on the Need for New Concepts and Categories of Thought

1 Introduction

Laws and regulations are normally built on legal concepts established long ago and influencing everyday life almost like laws of nature. These legal concepts may seem hard to apply in cyberspace where, normally, the main focus of attention is on the information as such – irrespective of how it is stored and communicated. This paper will discuss whether completely new concepts and categories of thought are needed or whether it will after all prove appropriate in the IT-environment to take advantage of the legal principles meant for the traditional world.

2 Electronic places and digital bearers in the legal system

The development of Information Technology (IT), Internet and World Wide Webb has radically changed our way of communicating, running business and doing research. This new "environment" has normally been described in symbolic language derived from the traditional physical world. Take, for example, the electronic equivalents of documents, archives, mailboxes, stores and marketplaces, where the use of metaphors such as electronic documents, electronic archives, websites and web shops reflects the need for understandable, user-friendly terms and descriptions.

However, in the IT-environment, the legislator has limited the *dimensions* given by the physical world, which enables well-defined legal structures and delimitations. The main focus has been on processing of *information* and the title to information as such, c.f. data protection and intellectual property law. Laws and regulations founding their effects on the existence or location of a certain *physical object* or *physical place* have often been ignored, e.g. clauses with bearing on electronic equivalents to locked rooms, closed places of storage, signed documents etc. Thus, it is unclear e.g.

---

* *Per Furberg* is a member of the IT Law Observatory. See presentation in Annex 1.

- when an electronic document sent to a public authority or to a private entity is deemed to be received according to procedural law or contract law,
- whether electronic places and electronic handing over (traditio) will enjoy the same legal protection and legal effects as its traditional physical prototypes.

The following survey outlines these issues with a starting point from "digital bearers", such as electronic money (E-money), and from "electronic places" created to receive electronic documents, such as electronic mailboxes.

3 Immaterial "tokens" and absence of time and place?

The lack of legal guidance in the field of electronic document and payment management, for example, may derive from the customary limitation to computer *data* as *immaterial* information. Electronic equivalents to physical places and objects, and the difference between rules and regulations applicable to immaterial information on the one hand and a person's protected custody of digital data and documentary evidence on the other hand are hardly mentioned. The importance of this distinction is indicated even in our constitution. According to Chapter 1, Section 9 of the 1949 Freedom of the Press Act and Chapter 1, Section 12 of the 1991 Fundamental Law on Freedom of Expression anyone may be responsible and liable for damages with respect to his mode of obtaining the material if the *method* is unlawful, notwithstanding the constitutional right to obtain information for the purpose of publishing. Consequently, it is not an infringement of the constitution to ban methods based, for example, on unlawful pressure or intimidation, unlawful intrusion, breach of postal or telecommunication secrecy, intrusion into safe depositories etc.

This dividing line is, however, unclear in the IT-environment. It has been debated whether the penal provision regarding breach of data secrecy – consisting of unlawful access to a recording for automatic data processing – should be understood as a regulation regarding information as such or a criminalisation of certain methods to obtain information. This question may be of practical importance if, for example, a press reporter unlawfully hacks into a computer with a view to publishing data stored on it. Will the constitution exonerate him?

Further, it is often stated that time and place have lost their meaning on the Internet. It is true that data in transit, e.g. repre-

senting an offer or an acceptance, will reach their destination much faster in the IT-environment and may be communicated globally, but the same need to divide risks and responsibilities between sender and addressee will exist, if the item of mail is delayed, mutilated or does not arrive. Thus, it is necessary to create clear borderlines for electronic places, e-mailboxes and the like and to elaborate distinct views on how to judge when these borderlines are reached and crossed. The same need exists to clarify when digital bit strings, designed to carry legal rights, will be apprehended as documents, coins or bills, the possession and transfer of which will be decisive of the parties' legal rights.

4 Dematerialisation on different levels

The dematerialisation of documents, archives, mailboxes, marketplaces etc. described above has become especially apparent in the area of payments, where the changes brought about by IT could be seen as the last step in an evolution;

- from physical goods as objects for barter to tokens representing value and used as means of payment,
- from certificates of deposit to instruments of debt and finally to a monetary value in itself,
- from the *bearer* of monetary value to an *account-based* system, and
- from traditional physical objects to digital data.

The first two kinds of changes have appeared without any connection to the computerisation and involved:

- a transition from tangible goods (e.g. gold) which is considered to have a certain value, to means of payment represented by tokens which are generally considered to be bearers of a certain value, first backed up by, for example, the corresponding value in gold, but later accepted as a completely dematerialised means of payment;
- a legal transition from certificate of deposit to a written debt note and finally to coins and bank notes, which are considered to have a certain value although no debt exists tied to the coin or bill.

When computers are taken into consideration, not only will the new technology's partly intangible character appear – i.e. the

transition from traditional physical objects to digital data – but also the shifting from physical carriers of means of payments to account based transactions. As electronic registrations have been considered incapable of carrying rights, due to the risk of double spending it has been self-evident that IT-based payment services have to be account-based.

However, when new systems for E-money, equivalent to the handling of cash, are introduced, the digital monetary units are *"transferred"* more or less anonymously from payer to payee, from virtual "wallets" to virtual "cashboxes". The location and tradition of data representing the digital monetary units are of vital importance in these systems as payments effected with digital monetary units work like transactions with coins and bills. The routines are characterised by an ambition to achieve

- immediate settlement,
- limitation of the payment risks, and
- secure *instruments* that can be "transferred" electronically.

The payee should not have to check

- who the payer is (the identity),
- if the payer has the right of disposal with respect to the electronic monetary units (authority), or
- if the payment is covered (balance on an account).

Regulations regarding account-based transactions do not fit such digital instruments and payment services. The account-based services demand that the person who authorises the transaction must be identified and must have the right of disposal and that the payment must be covered. Further, this information must be securely stored to enable a party to contest an incorrect statement that the transaction was not duly authorised. As far as payments with coins and banknotes and other bearer-instruments are concerned, the possession of the instrument is intended to give enough protection.

5 Accounts versus digital bearers

The transition to account-based transactions has been consistent with the lack of technical and administrative routines to hinder double spending and to recreate the functions based on posses-

sion and tradition. The treatment of data is built on copying. The development of cryptographic and administrative routines making it possible to recreate *bearer instruments* protected against duplication in the IT-environment will in this connection serve as a breakthrough. IT and the market are developing monetary units in electronic form to be used as bearers of certain rights that are "transferred" between payer and payee. The question therefore arises whether the existing legal framework of private law, procedural law, debt enforcement law, criminal law etc. is suitable and able to handle electronic monetary units. Clearly, the existing deep-rooted thinking based on accounts will have to face a major challenge. In some areas new legislation has been given to render central registers – accounts – the same legal effects as possession and transferral (traditio) of traditional instruments and these provisions are not built on the legal effects of "possession" and "transferral".

The following alternatives may serve as a starting point for considering the legal issues;

- to bear in mind digital data's partly dematerialised character and state that an account-based point of view has to be applicable, in the absence of any unique physical object such as a banknote, or
- to focus on the functions which the digital monetary units will fulfil in an E-money system, functions replicating those of traditional cash.

If the first alternative is accepted, the result will be a kind of modernised thinking based on bankbooks. It is true that such "accounts" in electronic form should be kept decentralised to a disc-drive or chip-card etc. which the holder of the "account" would have in his possession or otherwise under his control, but this approach would anyway imply that the payee will have to identify the payer, check his authority, document the transaction etc.

Should the starting point instead be taken in the functions the electronic monetary units are meant to fulfil within the E-money system, the idea of E-money will be brought in harmony with and subordinated to rules and regulations that fit into this technical and legal product's way of functioning. Digital bearers which are protected against double spending and thereby given functions fully equivalent with cash make it possible to recreate the functions fulfilled by coins and banknotes. As a consequence of this approach, it will be feasible to recreate in the IT-environment nearly any bearer instrument, e.g. digital stock certificates and negotiable electronic shipping documents, without the long detour of central accounts.

6 A starting point from objects or functionality?

The legal issues may be analysed from a variety of starting points. A study, based on IT and data's *character* together with descriptions of the digital *instruments*, may aim at considering whether the electronic monetary unit

- is a physical object or something immaterial, and
- is possible to hand over (traditio) in the same way as a traditional physical object.

A similar angle of approach, taking the legal system and judicial classifications into different *kinds of property* as our starting point, is to ask whether an electronic monetary unit shall be considered to be

- chattels,
- a claim, perhaps tied to an instrument, e.g. a bank note or a promissory note, which is carrying the monetary value, or a cheque or another generally accepted instrument evidencing a non-negotiable claim, or
- another legal title.

If E-money should be seen as one of these physical objects or categories of property, it could maybe be stated that the answer is more or less obvious: the laws and regulations for the traditional environment thereby pointed out should be applicable. Such a linguistic analysis of terms and legislation will, however, entail certain risks. Digital data and consequently also the electronic monetary units have a partly physical character (data exists), a partly immaterial character (data may flow in ways giving immaterial dimensions). It may further be questioned whether any instrument exists (in the meaning intended by the law), whether it has any spatial localisation, and whether traditional dividing in kinds of property is relevant in cyberspace.

Any interpretation from the mentioned starting points – concealed in an analysis of terms and definitions – will probably reflect the interpreter's own intent, not the legislator's, regarding these legislative questions. The laws and regulations have usually not been adopted during the time computers have existed. Details in the formulation of laws and regulations and the legal technical solutions can therefore hardly give any answers, and, hardly any case law exists. An analysis beginning with the character of IT,

the kind of property, the kind of instrument etc. may consequently produce misleading results.

The functions the electronic instrument is intended to fulfil within the system will probably make a more fruitful starting point. The determining factor will then be whether the electronic monetary unit, the digital promissory note etc. can offer the same functionality within a system as for example traditional coins and banknotes (traditio) or if the payment functions created in electronic forms should be seen as dispositions regarding account-based property. There is nothing new with such a "functional" starting point. Traditional physical objects have been suited to function within certain commercial patterns of transactions and, when these patterns have changed the legislature has adapted the objects' functions to these new patterns. How the electronic monetary unit is constructed and represented and if it is tied to a card or is stored on a hard disk, if it is considered to be a physical object etc. will consequently have to come second. These differences are of limited interest from a legal point of view as the instruments, independently of how they are constructed, fulfil the same functions.

However, this doesn't mean that the character of the monetary units and the kind of property they represent should be completely ignored. Wordings and existing law have a considerable power over our thoughts. Therefore an analysis is hardly possible without, on the one hand, metaphors such as "handing over", "possess" and "receive" the digital "coins" kept in an electronic "wallet", and, on the other hand, a comparison with rules and regulations regarding different kinds of property and instruments.

7 Payments and civil law issues

7.1 Cash-based payments procedures

The question when a payment with E-money is accomplished may be a suitable introduction to the legal issues that will arise. Most people are of the opinion that a payment with E-money is completed when the procedure to put the card into the terminal and push the button to accept – or make the same arrangements with network money – has led to the registration of the electronic monetary unit in the payee's technical equipment. The idea is that the monetary unit is "transferred" from the payer's technical aid to the payee's. This action will probably also be apprehended as a legal act equivalent to the transfer of coins and banknotes.

The question is how such an approach may be explained in legal terms.

Normally payer and payee have not made any agreement beforehand regarding how and on what conditions a payment with E-money should be made. E-money systems are meant to enable quick and simple payments, e.g. when goods are bought in a store. Consequently, it is important to be able to co-ordinate current legislation with the basic functions, even though the parties are free to agree mutually on these conditions. Another important issue is when the payment with an electronic monetary unit shall be considered to be binding with respect to third parties. Such issues are not possible to solve within contracts between payer and payee, as their agreements do not bind a third party.

7.2 E-money represents a claim

With respect to what has been said regarding the character of data, it is not realistic to state that E-money *is* chattels – i.e. traditional physical objects – and that legislation regarding ownership and transfer of chattels should be applicable, as a consequence of their character. There are substantial differences between traditional physical objects and digital data. The same will apply regarding judgements based on the opinion that the electronic monetary units should *be* banknotes.

The directive (2000/46/EC) of the European Parliament and the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of E-money institutions, clarifies these issues partly thanks to the definition in the directive of E-money as "monetary value as represented by *a claim* on the issuer". However, it is not enough to establish that the receiver of E-money obtains a claim. Completely different laws and regulations are applicable on non-negotiable claims and claims tied to negotiable instruments, and different kinds of bearer instruments tied to partly different laws and regulations exist.

7.3 An analysis of issues related to third parties

Third party issues are particularly interesting for the matter of a functioning legal framework for E-money, as such issues of law are not possible to solve within contracts between payer and payee. An analysis based on functions may focus on the jurispru-

dence regarding bearer bonds, non-negotiable claims and chattels. In this connection e.g. the following legal questions are of interest. What is the effect of holding the electronic monetary units ("possession")? Does the possession function as an authorisation or is it necessary for the payee to otherwise check the payer's authorisation to dispose of the funds and to document his findings?

If the Swedish laws regarding bearer bonds or chattels should be applicable, the possession of the E-money will authorise. A right of disposition is presumed. An application of the Swedish provisions regarding non-negotiable claims will on the contrary not authorise the possessor. Thus, the payee should have to verify, at his own risk, that the payer has the funds at his disposal.

The result is that a payee, who in good faith has acquired an electronic monetary unit and got it in his "possession", is seen as the rightful owner, if the laws regarding bearer bonds or chattels are applicable, even if the payer has found a card containing the monetary units and used them unlawfully. On the other hand it should be possible for the owner who lost the card to reclaim the funds, despite the payee's acquisition in good faith, if the provisions regarding non-negotiable claims were to apply. The same result will become visible if other legal issues related to third parties are analysed from these starting points.

Consequently, the legal functions given by transfer (traditio) of traditional bearer bonds fit perfectly when traditional coins and bills are replaced by E-money systems. The technical and administrative IT-routines, modelled for coins and bills, have recreated the functions given by possession of traditional instruments and these routines are simple and functional from a legal viewpoint.

7.4 A Swedish law on emission of E-money

This approach already seems to have been accepted in Sweden. The Government will shortly be taking a definite position to a Bill to implement the EC-directive on E-money. The bill states in its travaux préparatoires that the legal principles applicable to other traditional bearer instruments, such as bearer bonds, bills and coins or chattels should be applicable to E-money. On the other hand, the provisions regarding non-negotiable claims may not be applied to E-money, as the stored monetary value is

handed over when a payment with E-money is accomplished (prop. 2001/02:85 p. 60).

Consequently, the legislature has accepted a digital bit string as carrier of a certain legal right and has not found any objections to applying the legal concept of traditio in the electronic environment, provided that the system within which the digital instruments are used creates the analogous functionality as when handing over bills or bearer bonds.

8 Electronic places and incoming documents

A similar survey of incoming electronic documents and the approach to laws and regulations, founding their effects on the existence or location of a certain physical object and place, may reveal the need for electronic equivalents to traditional instruments and places of storage.

Under Section 10 of the Swedish Public Administration Act (1986:223), a traditional document – according to the main rule – is deemed to have been received by an agency the day on which the document has been delivered to the agency. This means that the paper document must have arrived on the agency's premises.

The natural thing may be to apply the same principle to messages transmitted electronically and consider an e-mail, for example, to have been received by the agency when the data which represents the document has reached the agency's mail-receiving function. This may be applicable whether this receiving function is physically located in the agency's information system or has been relegated to a mediating company which furnishes a service in which the "mailbox" is physically located on the mediating company's premises. However, different approaches to the interpretation of this clause, and the corresponding provisions in the Swedish Code of Judicial Procedure, have been established.

Some experts advocate the *principle of accessibility* with reference to the provisions on incoming documents according to the Freedom of the Press Act (Chapter 2, Section 6). An extensive application of a principle of accessibility in the procedural field could, however, entail the disadvantage that electronic documents put on a publicly available website – which is accessible to administrative officials but never visited by them – could be deemed to have been received by the agency. A restricted principle of access may on the other hand complicate the application of the principle of the sender's risk, if the item of mail is delayed or will not arrive. Further, the point of delivery would lose

its connection to the function established as the authority's electronic mailbox, where delivery receipts are generated and posted according to established information system architectures.

Other legal advisers claim that the procedural provisions on incoming documents should be interpreted in accordance with a *principle of print-out; viz* the document is deemed to have been received by the agency the day on which the message is printed on paper by the authority. The arguments for this interpretation have been limited to the statement that it has to be questioned whether it is possible to incorporate the usage of electronic documents in a time-honoured demand to communicate in writing; i.e. no document exists before the print-out. Such a principle leads to a situation where only the authority is able to bring about the circumstances that will result in delivery and, consequently, will have the time of delivery at its disposal. A similar approach with the same effects is recommended in the commentary to the Swedish Code of Judicial Procedure – a *principle of taking into custody* – meaning that an electronic document is not deemed to have been received until a competent representative of the authority has taken care of it.

These interpretations are difficult to reconcile with the legal rights of the individual. A party must be able to secure his rights when certain time limits are to be upheld. Consequently, when electronic filing and electronic mailboxes are put into practice the authority creates an electronic equivalent to a post-office box assigned as the electronic place of delivery, either housed on the authority's premises or outsourced or otherwise located somewhere else, but functionally equivalent to a mail-receiving function within the authority's office. This does not mean that an electronic message must have arrived at the administrative official's mailbox for incoming electronic mail *within his PC*. The determining factor should be when it has arrived at the server for incoming e-mail; cf. that a traditional postal letter must not have arrived at the administrative official's desk. Such a *principle of electronic custody* is consistent with the actual usage and probably applied in the authorities' daily work (c.f. prop. 1996/97:100 part 1, p. 461 *et seq*.).

9 Closing lines

To claim that an electronic message is not a "document" according to the Code of Judicial Procedure until data has been printed out is an example of old-fashioned jurisprudence, according to

which judgements could be derived from interpretations of certain general notions; so-called “Begriffsjurisprudenz” in a bad sense. Such an opinion will be in glaring contrast to the acceptance, in the Government bill on E-money, of a digital bit string as carrier of a certain legal right, controlled by the “possessor” and possible to “hand over” (traditio).

The approach chosen in the Government bill makes it – simplistically described – possible to treat electronic “documents” as documents, electronic “cash” as cash, account-based systems as account-based disposals, within current law. On the other hand, an approach based mainly on the historical meaning of the wordings – disregarding the practical usage – will call for extensive amendments of laws and regulations.

Hopefully, the virtual IT based structures and instruments, shaped by the information system builders, will be accepted by the legislator and in case law. These concepts and categories of thought need to be reassembled into co-ordinated approaches for the IT-environment, whatever steps forward the conception of justice, will take. The question is how to create this basis without being hampered by “stifling” legislation or case law, based on details and technical solutions, incompatible with the speedy development driven by the Internet and World Wide Web.

Viveca Bergstedt Sten*
The IT-practitioner's World

1 Introduction

Consider this. Is there really anything to imply that there is a new legal field worth the name of IT-law? Isn't this simply a trademark invented by lawyers to describe all the services performed in response to demands from the information society – albeit in a new format? Or is there merit to the idea that the 21st century has brought with it a legal discipline distinct enough from other legal areas to deserve independent recognition and specialised practitioners?

In a world where the finer points of law have been the subject of analysis and debate for decades, the concept of IT-law would be considered a mere baby – all but newborn – compared to the senior citizens of general civil law. To illustrate the foregoing, let us take a closer look at the matters requiring the attention of someone practising "IT-law", and in doing so, perhaps arrive at a conclusion – is there or is there not anything out there deserving the epithet of IT-law?

2 The scope of "IT-law"

In Sweden, the "IT field" in its broadest sense is characterised by a notable dearth of court cases and literature compared to most other legal fields. In many instances, there are so few rulings that guidance has to be sought from other countries where similar matters – albeit based on national law – have been adjudicated.

There is a distinct international flavour surrounding IT-practitioners which is also very much influenced by our dominant neighbour in the West. The American software industry, whose anxiety, or perhaps paranoia (as the case may be), regarding unauthorised use of software, has helped form the basis for the legal framework surrounding many of these products, has impacted heavily. Although comparing the Swedish legal tradition and its American counterpart is like comparing apples to pears, the American influence in Sweden is tangible and growing. Like a

---

* *Viveca Bergstedt Sten* is a member of the IT Law Observatory. See presentation in Annex 1.

weed quietly finding its way into a bed of roses, the American legal tradition of complex, detailed contracts spelling out exact boundaries for use and crying out for impossible damages, is unobtrusively being adopted in Sweden. Through the medium of American licence agreements fed to Swedish customers through subsidiaries, franchise agreements, license rights, and over-ambitious lawyers equipped with the latest small print imported from the west, the Swedish IT industry seems content enough to do business deals moulded in legal clay vastly different from Sweden's own.

Let us examine some issues that would allegedly fall within the scope of IT-law.

All questions relating to the Personal Data Act (1998:204) and other matters pertaining to the capturing of personal data – including the construction and mining of databases and any ensuing use and transfer of their contents – would typically spring to mind. Regulation of information handling may be thought of as state-of-the-art IT-law in its purest form, but this could merely stem from the fact that the legal environment must mirror the effects of technical development to protect personal privacy as time goes by. Rather than allowing legislation on information processing to be considered as IT-law merely because the processing is performed by obvious IT devices such as computers and servers, this could easily be viewed as yet another area where the individual is enabled to enjoy his privacy by appropriate legislative measures in the same tradition as the expansion of the 1949 Freedom of the Press Act to cover new media, for example.

The Swedes, who harbour a deep respect for matters organised and streamlined, have developed a number of standardised IT agreements, addressing such matters as *system deliveries, IT consulting services, support and maintenance and outsourcing of IT services*[1]. In some cases these agreements have been drafted by the supplier side only. In some cases they have been negotiated or at least reviewed by both sides prior to public release. Although these standard agreements are widely used by both sellers and buyers, including their lawyers, and are often referred to as IT-agreements, they hardly constitute proof of the concept of IT-law. On the contrary, interpretation and understanding of these agreements normally calls for a lawyer with a good grasp of general contractual principles, i.e. somebody who understands the principles of entering into, being bound by, and terminating a contract. The fact that the object of these contracts – IT equip-

[1] Avtal 96, Utveckling –92, ABDAKA -96, Drifttjänster-99 etc.

ment and services – has come to label the same, does not in itself provide any evidence of a new legal repertoire.

Typically, an IT-practitioner would also come into close contact with matters such as *software development, customised systems and system integration agreements* as well as *on-line services, electronic commerce (including internet marketing), telecommunication services and computerised crime*, all of which are distinguished by their focus on services rather than goods, and more often than not by their obvious lack of physical form. There are also contracts for services performed by IT-consultants and the question of ultimate ownership to the intellectual property rights created compared to work products developed by employees. However, these matters are, at the risk of repeating myself, much more typical of contractual law, marketing law, labour law, and criminal law etc., etc. than anything else.

Then we have the issues of intellectual property rights that will appear in almost every instance. There are the complex matters of *proprietary rights* to all tangible and intangible work products that are being produced every day of the week in this age. Many, many hours are also spent in commercial negotiations when lawyers try to find a common ground to agree on matters such as *recognition of ownership, agreement on joint use, regulation of future development, global marketing rights, potential licensing, franchising rights, publication rights* etc., etc., etc.

The dot.com industry further expanded the legal horizon by bringing into focus the great importance attached to *domain names*. Without going into too much detail, it is clear that the domain name issue, and of course its underlying relationship to the regulations surrounding *trade marks*, is a key legal issue to anybody working in this setting. However, the area of intellectual property rights has hardly seen the light of day in the context of the information society, although, admittedly, the recent technical developments which will allow any ten-year-old to download the long-awaited Harry Potter movie from the Web five days after its world premiere, have certainly highlighted the need for appropriate and speedy legal action.

In conclusion, there seems to be little hard evidence that there is indeed any such thing as IT-law. It would seem more appropriate to use the term as a general heading for a number of legal areas that become involved. Legal areas which have been brought together by the fact that the object that triggered the need for legal expertise is composed of intangible electronic data flowing at lightning speed and calling for different legal analysis and opinions at different intervals. Thus, it would seem that the cen-

tre of legal attention is an IT-object, but the legislation involved is not.

3 The IT-practitioner

If it is difficult to find enough of reason for designating "IT-law" as a legal field in its own right, is there some common ground that will serve as a denominator for "IT- practitioners", those legal fellows who work with the legal aspects of IT-related matters on a daily basis?

Perhaps IT-practitioners may be characterised by the interest they take in a new and unexplored field that presents its own challenges in terms of technical complexity, terminology, and legal impact. Although this would seem to also require some technical understanding and insight into electronic devices and their operating principles far beyond the interest of a typical lawyer, the IT-practitioners are probably better identified by their apparent appetite for working at the legal frontier and affinity for an innovative industry in a very dynamic environment. But maybe there is also a genuine desire to leave a legal footprint somewhere in cyberspace?

How do IT-practitioners practise? To begin with, she (or he, please interpret the further use of "she" as the simplification it is) probably needs to fine-tune her communication skills more than most lawyers, since an integral part of her work involves acting as a go-between and interpreter between the technical staff and the legal requirements. Although the comparison may be less than flattering, the IT-lawyer could be likened to a legal transformer or even a processing filter, i.e. somebody who eases the communication between the legal world and the information world.

Does this distinguish her from other lawyers with other legal specialities? This might very well be the case, as the information technology society seems to require more of its appointed legal counsel than most. Not content to remain bystanders, the citizens of the electronic world expect their lawyers to take an active part in their business, involve themselves in the task at hand and develop an understanding of their products. Many times, a client will not only ask for legal advice relating to a contract, but will also expect the IT-lawyer to provide an insight into his needs; guidance is required in more respects than traditional drafting and negotiations: the lawyer must also assist in defining what the client wants, how he should go about obtaining it, and

what the contract is actually about. This is an environment where buyers are frequently unsophisticated in terms of insight and professional assessment of their own corporate needs. This is probably explained by the fact that although IT-products are purchased by most if not all companies today, the buyers are usually active in different industries altogether. Buying IT-products and services does not constitute the bread-and-butter of most buyers; the products are necessary, but not necessarily understood or even desired. Hence the feeling of operating on unfamiliar territory. Hence the increased need to rely on experienced lawyers.

What other interesting distinctive features might we find in the IT-practitioner? That the IT-lawyer must be curious as a cat, interested in technical solutions, more service-minded than most, and certainly be able to switch effortlessly between legal lingo and technical mumbo-jumbo. It probably helps if she has a hands-on personality and does not mind having to do a great deal of client handholding as well. To sum it up – here is somebody who has to be very adept at "out of the box thinking" and able to function in the most real of real-time environments.

4 Experiences of "Internet law"

If we hesitate to award the concept of IT-law a status of its own, is there something called "cyber law" available to IT-practitioners?

The explosion of the dot.com industry in the late nineties served to illustrate a crucial point to lawyers working with the expanding Internet industry. There was no such thing as "cyber law" reaching across the national borders of the member countries of the EU. Here was an area that did not emerge as a homogeneous legal field, even though its late "coming of age" could have been a model example of how to create European legal harmonisation.

When the many Internet ventures rushed to establish themselves across Europe a few years ago, legal advice was much in demand in respect of the planned launches on the European market. What every company, (especially those involved in "business-to-consumer" operations) interested in establishing itself across Europe discovered, was that substantial amounts had to be spent on obtaining legal advice to ensure that a site was in compliance with the legal framework of each country. From a practical viewpoint, this meant that for each country launched, local legal advice had to be obtained primarily with regard to three ar-

eas: reviewing and commenting on the legality of the business model itself, reviewing all offers made to the public by the company, and scrutinising the text on the site. In particular, this meant that local expertise had to be sought in respect of at least contractual law, marketing law, personal privacy/processing of customer data, and consumer legislation (if applicable).

For each country, appropriate legal counsel had to be contacted and briefed about the company and its business model, before proceeding to review the matters at hand, which further increased the costs. The fact that consumer legislation could differ substantially from country to country also added to the complexity, as it was difficult to determine to what extent local legislation would be considered if an individual agreement between the company and a consumer were to become subject to interpretation or dispute. To illustrate, in many countries an agreement will not only be construed on the merits of its actual text and content, but will also be analysed with a view to the relevant legislation that may impact on the interpretation.

The national implementation of EC directives further complicated matters, as there were substantial variations in the ensuing national laws. In the matter of the Distance Contracts Directive (97/7/EC), different countries chose to embellish the open return period and added more time than the directive laid down. Consequently, it was not possible for a company to implement a single, uniform open return policy, as the conditions had to conform to the preferences of the individual countries. Another example relates to the Data Protection Directive (95/46/EC), whose implementation was severely delayed in many countries. As it was also implemented in different ways in various countries, this meant that each country had to be analysed individually. Furthermore, local legislation would add layers of regulations, which had to be considered. Take Denmark for example, where the law on payment instruments has provisions of a far-reaching character in relation to the processing of personal data in connection with payments made through the use of credit cards. This meant that, even if a company followed the appropriate EU directives closely, it still had to make sure that the law on payment instruments were observed when certain data was processed or it would run the risk of finding itself in conflict with Danish legislation.

Consequently, those companies wishing to take advantage of the simplicity built into e-commerce through the use of a single medium – the Internet – found (somewhat to their surprise) that there was no hope of relying on an equivalent legal model to simplify matters. On the contrary, in not one single instance was

it possible to take a business model, have it translated and adapted to relevant EC directives and then put it to commercial use without further ado. As a side remark, it is worth noting than in comparison with the relative ease of launching a cross border e-commerce business in the United States, the present situation in Europe and the legal divergences offer a considerable disadvantage to any European e-commerce venture aiming at establishing itself in Europe.

As reality dawned on the lawyers advising Internet companies, the conclusion became evident. There was little point in discussing any concept of cyber law, as it hardly existed, let alone could be used to facilitate business for commercial ventures using the technique of the Internet. As for the legal matters that needed to be analysed in connection with these enterprises, they turned out to be cloaked in the habits of marketing laws, competition laws, consumer legislation, and many other legal fields, which on a daily basis would be referred to as traditional commercial and consumer legislation.

Summing up, there seems to be little in the way of either IT-law or cyber law to provide tailored IT-legislation or even legal harmonisation to constitute a new legal field set to join the ranks of other established areas such as tort law, commercial law or building law, just to mention a few. However, this should not deflect from the fact that there remain many legal matters relative to IT and electronic services and products that require the attention of IT-practitioners, but also scholars reaching into cyberspace. In the world of the Internet anything is possible, but clear legal structures evade those who choose to practise law within it.

Part III:
ICT in Government and Administration

Hans Sundström, Gustaf Johnssén[*] Shaping the Future Public Administration – The Legal Perspective

1 Introduction

In this paper we will discuss some of the legal problems connected to the reforms under way in the Swedish administration. We will also touch upon some more general problems relating to law and IT, but we will keep the administrative perspective throughout.

Our aim is to give our view of some of the short and long-term legal effects of the use of IT in the administration. The discussion is not intended to be complete in any way, merely to highlight some aspects that we find particularly interesting.

We will describe the administrative development from three perspectives that are all related to the use of IT: technological, democratic, and organisational change. We will then examine some legal aspects of these change processes.

2 Government in transition

The fundamental goals of the Swedish administrative policy are *Democracy*, *Efficiency*, and the *Rule of Law*. These goals are set out in the action programme *Public Administration in the Service of Democracy*, laid down by the government in the year 2000. [1] All administrative initiatives shall serve the fundamental goals of administrative policy. These goals are not entirely separable. They are constantly interacting in political and administrative practice. Sometimes they all pull in the same direction. At other times, they collide.

Several development initiatives are currently under way in the Swedish administration, many of them related to IT. We will

---

[*] *Hans Sundström* is a member of the IT Law Observatory. See presentation in Annex 1. *Gustaf Johnssén* is an adviser at the Swedish Agency for Public Management (Statskontoret), working primarily with ICT and administrative reform. He has also served at the ICT Commission and at the Ministry of Justice.

[1] http://justitie.regeringen.se/inenglish/pdf/publicadministration.pdf.

start by giving an overview of some of them, before we examine their legal implications.

3 Technology, communication, and organisation

Computers, telecommunications and other forms of information and communication technologies have been widely used in the Swedish administration for several decades. The administration has been an early adopter of new technologies.

Traditionally, IT has been seen merely as a tool for performing traditional processes in traditional organisations, only more effectively. It has been argued that this may not be an entirely adequate description. Be that as it may, the ultimate aim of the current reforms is a fundamental reshaping of government.

The major initiative in administrative development is called the 24/7-agency.[2] This programme has been initiated by the government and is being carried out by the Agency for Public Management. According to the 24/7-program any governmental service that can be provided by electronic means, shall be provided electronically. The individual citizen shall be able to contact all governmental agencies by electronic means in order to obtain governmental services, make applications, and initiate governmental actions, independently of time and place. It does not, as the somewhat ill conceived term 24/7-agency may seem to imply, mean that government officials are expected to be available around the clock. Traditional means of communication will be maintained along with the electronic communication channels. This means that there will be two parallel systems of communication with the government: by electronic means and by traditional means. The latter includes mail, personal calls, telephone etc.

The concept of 24/7-agencies includes both communication between agencies and communication between government and citizens. A new communications infrastructure must be developed for communication with citizens as well as for the exchange of information within the government, between agencies and so on. This new technical infrastructure will, for example, comprise means of communication between agencies, methods for security and identification, and solutions for long-term documentation.

---

2 *The 24/7 Agency: Criteria for 24/7 Agencies in the Networked Public Administration* (Statskontoret 2000:41), available at www.statskontoret.se.

The development of the 24/7-administration involves all aspects of administrative policy, such as technological, legal, and organisational aspects.

As mentioned above, although IT is often perceived merely as a tool, it does in fact change the organisations into which it is introduced. In many cases this change is unexpected, unintended, and possibly unwanted. Within administration this could be the case, for example, when systems that were originally designed for commercial organisations are introduced in government. In Sweden, this may earlier have been the case in government. The disadvantage of the past is now the goal of the future. One of the goals of the 24/7-program is to change the organisation of government by using IT. Governmental agencies of the past were "drainpipe"-agencies having little or no contact with each other. Governmental agencies of the future are expected to collaborate with other agencies. The goal is that the citizen, in each situation, should only have one point of contact with government. Backstage, the different agencies are expected to co-operate and exchange information. The citizen will then be presented with the result from the single contact point, even when several agencies have in fact been involved in the process in some capacity. This one-stop shop will necessitate co-operation between agencies at the same level of government, as well as between agencies at different levels of government.

The inevitable impact of technical infrastructure on the organisation of the government is mainly a long-term change, but some aspects are clearly visible also on the early stages in the development.

4 New forms of democratic interaction

Many people have great hopes of information and communication technologies fundamentally changing and improving democracy. Some see it as a chance to realise the ideal of direct democracy, including every citizen in every decision. Others have more modest hopes, ranging from better-informed citizens casting votes in traditional elections to continuing dialogue between citizens and politicians at the local level. In Sweden, some experiments have been carried out at different levels of government. Some legal aspects of such experiments will be briefly related below.

Without doubt, the forms of democracy and citizen's participation will change. Consequently, the forms of government

will change, and so will the forms of administration. It is too early to say how these changes will look. What we can say is that they are going to take place, and that they will have an enormous impact on the legal system.

5 Administrative law in transition

Many rules in the realm of administrative law regulate aspects of information and information processing. Some rules relate to the information in itself, i.e. the content. Rules on secrecy or personal data protection are a case in point. Other rules relate to the communication, i.e. the form, such as rules requiring that a message be signed in order for it to have legal validity or status.

In many cases, these rules were laid down without regard to IT or EDP (Electronic Data Processing). In some cases, therefore, they seem to prohibit, or at least not provide for, use of IT. The law is often perceived as an obstacle to the desired technological development. Whatever one's opinion on that score, there is no doubt that the development does pose a problem to the legal system and, not least, to the legal profession.

In some cases, the legal infrastructure governing the administration has been dynamically adapted to the use of IT, one good example being openness and access to public documents.[3] In this area of administrative law, regulation has been adapted through case law as well as legislation. The adaptation may not always have been very swift, but legal development has on the whole kept pace with technological development. In other areas, development has been somewhat slower, perhaps because the strain on the legal system has not yet been severe enough to force the system to adapt. One such area concerns forms prescribed by law, which will be further discussed below.

Perhaps the most evident and down-to-earth legal problems are those related to new forms of organisation and co-operation. Administrative law is modelled on the organisation of the administration and it refers to boundaries between agencies, between levels of government, and between the public and the private sectors. This can cause problems when new processes are introduced that involve several agencies, perhaps at different levels of government. One example of an area where such problems occur is secrecy. According to the Official Secrets Act (1980:100), information that is secret at one agency would normally not be secret when transferred to another agency. This and similar pro-

[3] See Peter Seipel's paper *Access Laws in a Flux* in this anthology.

visions may be obstacles to the technologically and politically desired uses of IT. We will not explore the legal problems related to organisational changes here, but will eventually return to it after having explored two other issues: forms prescribed by law and new legal documents.

6 Forms prescribed by law

Many laws and regulations contain provisions on the mandatory use of paper communication. This can be the case when a signature is a condition for the validity of an agreement, an application, or some other document. In Swedish law, these provisions are scarce in private law, but very common in administrative law. The most common provisions are those requiring an application or other communication to be *in writing* or to bear the *signature* of the originator. There has been some debate as to whether provisions of this kind can be satisfied when using electronic communication. Some claim that a message or communication is in writing as long as it consists of text. If so, an electronic communication would meet the requirements that a communication must be in writing. Others claim that an electronic message can never be considered to be in writing, since writing must be traditional style ink on paper.

In order to promote the use of IT and enable agencies to transform into 24/7-agencies, the Ministry of Justice has initiated a survey of all provisions of form in Swedish law. The aim of this survey is to do away with all unnecessary provisions, and to change provisions in order to allow electronic alternatives to signatures and other provisions for form. Some questions and problems that have emerged in this project will be used here to illustrate some more general problems and questions regarding administrative law and IT as well as law and IT in general.

We will focus on signatures, as being among the forms most commonly prescribed by law, especially if taken to include signature-like forms, such as stamps or seals. The signature is also of particular interest from the point of view of the clash between technology and law.

The legal uncertainty is a particular problem in administrative law. In the areas covered by private law, it is in most cases possible to agree on the forms of communication. If the parties to a business relation of some kind are not certain that a provision in law permits electronic communication, they always have the option of contractual agreement to use it. They can also agree on

what security measures to take, and how to allocate the risks. This has made it possible for the Swedish banks to communicate over the Internet with a large portion of their customers. Similar solutions for mass-transactions would be desirable in the administration. This demands another kind of legal infrastructure than in the private sector. The administration should be ruled by law and it is not possible or suitable for the administration to rely on contracts when communicating with the citizens (cf. below). This means that the administration must rely on legislation. In this case, the law seems to be an obstacle to development.

Seen from the technological point of view, the task of changing provisions of form to allow electronic communication is a trivial one. It is a security problem. The written signature is a security measure, and the task is to find out in each case what the security functions of the signature are. Then one has to determine how these functions can be performed by electronic means. This can be somewhat difficult, since the written signature does not have distinct functions such as the functions of the electronic signature. In fact, written signatures generally do not provide the same level of security as electronic signatures. From the technological point of view, this is not a big problem, since it is possible to obtain at least the same level of security by electronic means as with traditional signatures. The problem is mostly a pedagogical one: to persuade lawyers of the blessings of electronic communication and electronic signatures.

Although this could be hard enough, it is still a far too superficial analysis of the task, which on closer inspection turns out to be much more delicate. The functions of the signature, be it analogue or digital, are far more complex than they may seem at first. The task therefore goes far beyond a mere comparison of technological security functions. These problems are not limited to the area of administrative law, but are relevant to all areas of law. Administrative law is an area where it is particularly fruitful to examine these questions.

One of the most interesting aspects of the signature is its iconic function. This function transcends the technical functions of the signature. The signature is a well-known and powerful legal icon. Everybody knows that it means something special to put your signature to a document. It means that you accept and commit yourself to the contents of the document. It means that you are bound not only legally, but also morally, by the document. It means that you have reached the point of no return. It also communicates solemnity. It means that this is not just any ordinary message, but a document. This function is even stronger, of course, if the document is signed *on one's honour*, as

in the case of tax returns. The iconic function cannot be analysed in technological terms. It is dependent on psychological, cultural, and historical factors.

This function is probably present to some extent whenever a signature is used, but in some cases, it is explicitly intended. This is the case, for example, with contracts regarding real estate. The traditional importance of land ownership combined with the social significance of habitation argues that it should not be too easy to alienate real estate. The provision for forms in this case also has a consumer protection aspect.

These esoteric functions are central to the perception of government. In the case of applications and similar cases, the form prescribed by law is an aspect of the exercise of governmental power. When the citizen signs a document and submits it to the government, he performs an act of submission. The subject turns his fate over to the discretion of the sovereign. The form is a way for government to communicate power when approached by the citizen.

Government makes similar use of symbols and icons to communicate power when communicating outwardly. The Prime Minister's signature under a law, the national coat of arms, an official seal – all these are signs of power. In fact, perhaps the most suggestive icon is the stamp. The stamp is the government's equivalent of the citizen's signature. Only the stamp is impersonal. While the signature is a symbol of commitment, the stamp could be regarded as the symbol of the impersonal power of government.

These esoteric functions of the signature, the stamp and their equivalents are not that easily transferred to the digital environment. It is not possible to translate them into a new technical form, since they are unrelated to the technological security functions of the electronic signature. Perhaps these functions cannot be fully analysed or even understood, but they will definitely not remain the same when using electronic communication instead of paper. Even so, it will be necessary to adapt administrative law to allow electronic communication. We still have to realise that reforming provisions for form is more complicated than a simple security problem.

In a short perspective, the reform of forms prescribed by law is an enabling project. Its purpose is to remove obstacles to technological and organisational development. Nevertheless, it would be unwise to believe that the reform will not have more far-reaching consequences. In the end, it may prove to change fundamental aspects of the administration and of administrative law.

7 New legal documents

By tradition, the administration is governed by laws, ordinances, and regulations, i.e. different kinds of legislation. The parliament passes laws, the government passes ordinances and individual agencies pass regulations. The ordinances must be founded on laws, and the regulations must be founded on ordinances or laws. All these different kinds of rules are in a positivist view aspects of the law. They are binding for the individual citizen, as well as for the governmental agency. Their legal status is well known and recognised.

The government issues other texts of a legislative character. The status of these texts is sometimes less than obvious. Many agencies issue guidelines of different kinds. These guidelines are not legally binding on citizens, neither on the agency itself. Some of them, e.g. those of the National Tax Board, have such an enormous impact that their status approaches that of law.

Apart from these unilateral documents, the government and its agencies can also enter into contracts and other bilateral agreements. Thus contracts, though not governed by administrative law, are a part of the legal infrastructure of the administration.

The use of IT seems to promote the use of non-traditional legal or quasi-legal documents and texts. Some of these texts have a form that is quite different from traditional legal texts, for example spreadsheets used to calculate a subsidy. Other documents are electronic translations of traditional semi-legal documents, for example electronic forms. Still others are non-legal or semi-legal documents and texts that are well known, such as guidelines and policy documents. We will focus here on the use of the latter kind of documents.

The increasing use of electronic documents could perhaps be called government self-regulation. In the private sector, self-regulation is often invoked as the proper way to regulate the IT environment. This may be so, although the arguments may not always be very convincing. For government, self-regulation would normally not be an option since, obviously, regulation by government would not be self-regulation. This could, however, be a suitable term for some new forms of documents with ambiguous legal status, issued by agencies.

In the network environment, agencies tend to regulate their activities through documents that are neither regulations nor guidelines in the legal sense. Examples of such documents are policy documents related to the use of electronic signatures, for

example so-called certification policy statements, CPS. In these statements such issues as liability and dispute resolution are regulated. Another example is so-called service declarations, where agencies commit themselves to a certain level of service, and pledge themselves to certain penalties, should the service levels not be reached. These service declarations have been introduced in Swedish agencies as a new kind of democratic interaction between agencies and users, i.e. citizens. We will briefly discuss some legal problems related to such policy documents.

The signature-related policy documents would normally, when used in the private sector, be part of a contract between the parties. This would hardly cause any legal problems. A government agency, on the other hand, cannot normally enter into a contract with a citizen. The relationship between government and citizens is, and should be, regulated by law. This is the fundamental demand of the rule of law. It does not necessarily have to be a problem in the individual case that an agency relies on a policy document. It may even give the citizen more rights than law entitles him to. On the other hand, it may deprive the citizen of his rights. We have, for example, seen a document providing that disputes between the citizen and the agency be resolved by an arbitrator. This would not be allowed under Swedish administrative law.

The content of such documents is often dependent on international standards. These standards are laid down by international organisations, and their foundation is private law, not Swedish administrative law. This way, foreign private law sneaks into areas that normally are, and should be, governed by national administrative law.

The major short-term risk with this kind of documents is the uncertainty as to their legal status. The citizen could rely on a document that might prove to be not legally valid. It could also happen that an agency limited its own freedom of action in a way that is not in accordance with administrative law, denying the citizen some right he would be entitled to by law.

In the end, the inclusion of this kind of policy document in the legal infrastructure of the administration may be unavoidable. This will transform the legal infrastructure and the relationship between citizens and government. It is essential that these changes should not be allowed to take place willy-nilly and, not least, that these documents should be introduced with the participation of administrative lawyers.

8 Old rules, new roles

We have outlined two areas of administrative development that are of particular interest from the legal point of view: legal provisions for forms, and new legal documents in the administration.

One of the main conclusions of the discussion on forms could be that what seemed on the face of things to be a simple question turned out to have quite far-reaching and perhaps unexpected implications. What appeared to be a security problem turned out to be potentially capable of changing the perception of government. Some of the traditional signs of power will lose their meaning, and in consequence the role of government in relation to the citizens is likely to change. It will be less of a sovereign and more of a partner or a supplier of certain services. Services that are not granted ex gratia on the subject's humble petition, but are supplied on demand to a citizen-consumer.

The new kinds of legal documents tend to blur the line between administrative and private law. This is in fact a change along the same lines as the changes just mentioned. The government will be perceived more as just another organisation, and it is only reasonable that it should be subject to the same legal framework as any other organisation.

This leads us back to the organisational changes mentioned briefly above. The use of IT will ultimately change not only the perception of government as well as the forms of regulation. It will change the fundamental role of government. The new roles of government are impossible to foresee. It would be dangerous to give up basic principles of administrative law, such as the rule of law, to enable technological development in the short term. It would be equally ill advised to cling to outdated legal principles, only to one day find that reality has left the law behind.

The new forms of interaction between government and citizens will contribute to the changing role of government. With the use of IT, the citizens can be consulted on a regular basis not only in parliamentary elections every four years, but also on all questions that concern them (and for that matter on questions that do not concern them). They will then also expect to be consulted. The roles of citizens, politicians and public servants will change fundamentally in ways that we do not know and cannot fully control. It is important that administrative law keep abreast of these changes.

In the end, we have argued; the character of administrative law will change. But what, then, could be the role of law, if it is futile to resist the technological changes?

The law and the lawyers are often perceived as obstacles to development. This opinion is not without merit. As we see it, however, there is no fundamental conflict between law and development. It is merely a question of attitude, both among technologists and among lawyers. It is important that those who most aggressively argue for changes recognise the value of the continuity in law and the value of the rule of law. At the same time, those defending the principles of administrative law must see that some development may be not only desirable but unavoidable. The role of law, then, must not be to obstruct, but instead to be a powerful tool for change. The law can give certainty and guarantee that technological development will be in the service of the citizens.

In order to defend the rule of law, it will be necessary to redefine the role of law.

Peter Seipel*
Access Laws in a Flux

"… and I say, hey stop, where is that database, is it on the net, it isn't on the big net is it? Yes, it is on the net, he says, but I hate the net, because the net is water, in fact only Sibelius and death are more water than the net, because on the net everything flows, on the net the flow is free, freer than all other places taken together, it changes all the time, it is like an information flock of birds, it constantly changes direction, but not elegantly and at the same time, like a flock of birds, the image was miserable, forget it, but the direction changes, and you cannot step down into the same net twice, because it only exists for the moment and the next moment it will be something else, and I hate everything that is something else the next moment and I don't want to have anything to do with it…"
Erlend Loe[1]

1 Naming and taming

The narrator in Erlend Loe's novel "Facts about Finland" hates water because he hates change. The reader is not surprised to find that he also hates the Internet, and data networks generally. Like water the data nets stand for change and change involves threats that take on the shapes of uncertainty, blurry categories, lost dividing lines, broken connections with the past, and so forth. Not only an individual but also a society, its legal system included, may have reasons to fear change.

Several years ago in Sweden, a legislative committee arranged a public hearing on the adaptation of access laws to modern information technology. The discussion soon made it clear that the traditional object of the constitutionally guaranteed access right had lost its previous stability. In fact, as some of the

---

* *Peter Seipel* is a member of the IT Law Observatory. See presentation in Annex 1.

1 Erlend Loe, *Fakta om Finland* (Facts about Finland), Oslo: Cappelen 2001, p. 137. My translation from Norwegian does poor justice to Loe's extraordinary prose.

participating experts pointed out, information seekers had a right to request documents regardless of whether they existed as written or printed, ready-made objects in the archive of a public authority. A distinguished justice of the Supreme Administrative Court, also a renowned specialist on access rights law, found this to be a monstrosity. How on earth, he asked, can a public authority be required to hand out things that don't exist? How on earth can the law be construed and applied in such a way that a public authority doesn't even know itself what official documents it stores in its archives? If a "document" is no longer a "document", then something has gone terribly wrong.

The problem that surfaced at the hearing was not unknown. In the 1960s a law-making committee had paid attention to the new, electronic media and pointed at some of the basic difficulties that they were likely to give rise to in the future. Soon thereafter, in 1971, the Supreme Administrative Court dealt with the question of whether magnetic tapes for computers should be seen as "documents" according to the basic regulation of access rights in Chapter 2 of the 1947 Freedom of the Press Act.[2] A county administration had refused to hand out such tapes on the ground that they were not to be seen as "documents" but rather as "tools" or "instruments" that could be used to produce "documents". The Supreme Administrative Court, however, chose to regard the magnetic tapes as "documents". The Court emphasised that a decision in the opposite direction would mean that increasingly large volumes of information would move beyond the reach of the access rights legislation. It would enable public authorities to steer away from openness by choosing non-document, electronic format for the storage of information. The Supreme Administrative Court found such a development unacceptable and, in consequence, construed the document concept broadly. By naming the new electronic media "documents", the Court aimed to tame them, to place them securely into the traditional legal framework. However, the issue of the scope of the decision immediately came to the fore. Briefly, did the right of access include a right to obtain computer readable copies of the tapes or just paper printouts?

2 The challenges of ICT

The 1971 decision of the Supreme Administrative Court opened a gate, and the data files of public authorities were made accessi-

[2] RÅ 1971 ref. 15. See also RÅ 1965 ref. 25 and RÅ 1969 ref. 11.

ble to the public. It did not take long for the lawmaker to confirm the action and revise certain relevant sections of the Freedom of the Press Act. Basically, ICT posed two kinds of challenges.

One challenge was the one noted by the Supreme Administrative Court, *viz.* that more and more information in public administration moves into the electronic environment of computers and data communication. Therefore, in order not to put the right of access in danger, it is necessary to let electronic media pass as "documents" and be treated in the same way as traditional media, i.e. eye-readable media such as paper documents, drawings, and photographs.

The other challenge concerns the new characteristics of the electronic environment. Not only is information registered and stored in new ways, it can also be processed and communicated in new ways. The question is: what does this mean for access rights? For example, automation enables new kinds of searches for information and if information is handed out in electronic format it may be used for purposes that differ considerably from what is possible with ordinary paper media.

The Swedish lawmaker has always been aware of the last mentioned, more far-reaching effects of information technology, and this awareness has found expression in three guiding principles:

(a) The use of ICT in public administration should not be allowed to erode the right of access and reduce openness.

(b) To the extent that ICT strengthens the right of access, such a development is to be welcomed.

(c) The purpose of the right of access is to enable control of the activities of public authorities and to support the rule of law. However, it is also intended to make all kinds of public information resources available, resources that are of value for public debate and for the understanding of various matters in society.

The three principles may seem simple and rather uncontroversial in a democratic society, but in practice they involve complications and conflicts of interests.

3 Documents, data, information

Some of the difficulties have to do with the shaping of the regulation of access rights in view of the new, electronic environment. After all, naming is not such an easy task. For one thing, there is a need for *neutrality* and *independence* in relation to technology. The discussion of such needs tends to be a bit confused. Basically, different types of media ought to be treated in the same way. And the legal regulation ought not to be tied to a particular state of the art so that it needs continuous revision as media and data processing methods change. The meaning of such a striving for neutrality and independence can differ from one area to another. For example, in order to make a regulation technology-neutral it may be necessary to go into details that are contrary to the interest of technology-independence. There is also a constant need for awareness of what may be called the practical impact of technological developments on a particular regulation. To illustrate, consider the difference between obtaining only a paper printout of a computer file and obtaining a computer-readable, digital version of the file. Or consider the difference between manual searching of paper index cards and automatic searching of a modern electronic, relational database. Viewed in this perspective, a regulation that is formally both technology-neutral and technology-independent may still be strongly affected by the technological setting. It has even been put in question whether legal regulation can ever aspire to be neutral and independent in relation to information technology.

The Swedish naming operation began with the decision of the Supreme Administrative Court to construe the concept "document" so broadly as to include electronic media in the form of magnetic tapes. Ensuing revisions of the access rights regulation in Chapter 2 of the Freedom of the Press Act have elaborated on this scheme. Thus, according to current law there are two categories of documents. One category is made up of traditional, visible media such as pieces of paper and x-ray photographs. The other category comprises "recordings" that one can read, listen to or comprehend in another way only by means of technical aids. The regulation does not spell this out, but one can group such "technical recordings" into two categories. One consists of *simple recordings* such as microfilm and the other of *complex recordings* where the technical tool plays a significant role with regard to retrieval, selection, arrangement, transformation, presentation, and so forth. Basically, computer recordings may be said to be complex recordings.

The complex nature of computer recordings has made it necessary to try to pin down more precisely what is a recording in the digital environment. Two borders have to be considered. One concerns the upper limit where an entity of information ceases to be *one* document and needs to be regarded as several. The other concerns the lower limit where one encounters the components that together make up a document. The two limits are not unknown in the context of traditional media but it is mainly in the digital environment that they become a practical concern. Thus, in the "paper" environment the dividing lines appear natural and self-evident – a letter is *one* document even when it consists of two pages and an appended drawing. In the electronic environment, the physical clues lose their obviousness whereas the logical structure of the information becomes important. For example, a chain of comments on a specific topic or a sequence of hypertext links may or may not be considered to make up *one* document.

The definition according to Swedish law of a recording in the context of automated data processing is 'any meaningful compilation of data'. The requesting party decides what is meaningful and, since he or she is not compelled to disclose the purpose of the request, one may conclude that a digital recording may in fact equal 'any information stored in a digital format'. Obviously, such an all-embracing and amorphous object of access needs some further limitation. One possibility could be to refer to the storage medium as such, but today's storage media do not lend themselves to restrictive and clear definitions of what is a document (a handy "memory stick" may, for example, store many megabytes of data). Instead, limitations are to be found mainly in the notion of "keeping". Only recordings that are being kept by a public authority can be requested. The notion of keeping in its turn presupposes that the recording (the compilation of data) can be made available through *routine measures* and with the aid of technical equipment that is used by the public authority itself. It is not necessary, however, that the public authority itself should have any interest in producing the requested compilation of data, nor that it should ever have produced it before. In other words; according to Swedish constitutional law, the public has a right to request and obtain access not only to pre-existing documents kept by public authorities but also to what are called *potential documents*, i.e. documents that may be produced by compiling data. It has to be emphasised that the right to gain access to potential documents exists only with regard to recordings and not with regard to traditional, "non-technical" documents. One can say that, almost invisible in the text of the statute, there exist two

categories of access rights, one for traditional media and one for digital media. Fixation and stability put their mark on the first kind, flexibility and flow on the second. There is a tension between the two, a tension that has to do with the fundamental question of what kind of access rights a democratic society needs.

4 Fixation and flow

The Swedish regulation of access rights came into being in 1766 in what may be called a steady-state world of information management. In this world, recording information and moving it around took time. This made it natural for the right of access to focus on information frozen in ledgers, letters, diaries, dossiers, protocols, and so forth. At about the same time (in the late 18th century), modern ideas of archives also began to be developed. Here too, frozen information was at the centre of attention, and the so-called principle of provenance was beginning to establish itself as the basis for the creation and structuring of archives. Briefly, the principle of provenance means that materials in archives should be kept and structured so that later they can be accessed and used with the fullest possible understanding of their original, functional context. Thus, archives ought to be organised so that they reflect the historical organisation and activities of the source. Archives, in sum, were looked upon as frozen information reflecting "how it actually was". The principle of provenance is still very much alive and puts its mark on today's archive theory.

The notion of frozen information can never be fully true and pure. To continue expanding the metaphor, there is water under the ice and flowing water does not freeze. Change seeps into the world of fixed media. To take a trivial example: a letter may refer to other information and to circumstances that no longer exist and are known. Thus, the interpretation of the text of the letter becomes uncertain and will have to be based on guesswork and reconstruction of its original meaning. What purpose did the sender of the letter have in mind? How did its recipient understand the letter? Meaning is elusive. Meaning means many a thing.

Modern electronic media tend to emphasise the fluid nature of information. They lend themselves to processing that involves rapid changes, diverse uses, deconstruction and reconstruction, and so forth. In fact (and to take the metaphor one step further),

digital media *vaporise information* and in that sense may be looked upon as information steam engines working at high pressure and at a high speed.

So, what are the consequences of the growing use of electronic media and the introduction of "technical recordings" and "potential documents"? The question has more than one answer. To begin with, the information units that may be the object of access rights have become fuzzy. The discussion above on the upper and lower limits of documents, and the remarks about the fading away of simple, physical delimitation criteria illustrate this. When a document may consist of "any meaningful compilation of data" and the keeping of the document is defined as the capability to make the data visible or audible through the use of "routine measures", then the situation is certainly more fluid than in the traditional "paper world" where the existence and location of documents is simpler in nature. In the "paper world" there are no potential documents, there are only pre-existing documents, fixed in form and ready to be fetched from a shelf or a drawer.

Secondly, in the electronic world it is practical and easy to process fragments of information in the form of data snippets and to relate them to one another. The spreadsheet is a well-known example. In a spreadsheet, each so-called cell may contain either data or code, i.e. instructions that describe how certain data are to be processed. For example, cell A10 in the matrix may contain a number whereas cell B10 contains a procedure such that a certain percentage of the value stored in cell A10 is calculated. The spreadsheet concept may be looked upon as a general model of modern, electronic data processing, characterised by complex interdependencies among parts and an intricate mesh of static and dynamic elements. The old filing system based on paper index cards, microfilm or some other static carrier of data has all but disappeared. Today, access rights apply or may apply to dynamic information systems where information patterns rather than information units are of interest to the information seekers. Increasingly, the information systems function in real-time, and access therefore tends to be concerned with short-lived and momentary information as well as (and sometimes rather than) historical.

Thirdly, the organisational structure of public administration changes, due to increasingly widespread and intense use of ICT. The phenomenon is sometimes labelled convergence, i.e. the floating together of things and activities that used to be separate and different. There are many aspects to be noted. There is, for example, the convergence of different administrative activities, of different administrative organs, of public sector activities and private sector activities, and so forth. Activities become multi-

contextual. Bureaucratic, rigid organisations give way to what Alvin Toffler in "Future Shock" (1971) labelled ac-hocracy. Generally speaking, administrative structures become more fluid, with ensuing difficulties for access rights. For one thing, their aims become uncertain. What are they for? Critical examination of the activities of public authorities or something more? And is the existing regulation capable of dealing with hot information steam of the kind produced by electronic information and communication technology?

5 Minimalism and maximalism

Minimalism here means a cautious attitude to openness and digital media, maximalism means seeking new solutions and a striving to strengthen the right of access. The minimalist tends to advocate a narrow kind of access right aimed at controlling the doings of public authorities. The maximalist emphasises the value of openness in general. We can approach the issues from two directions. One has to do with efforts to modernise the terminology and structure of access rights regulation. The other has to do with a possible expansion of the right of access, i.e. a content-oriented reengineering of the regulation.

In 1997 a legislative committee, the Data Legislation Committee chaired by Supreme Court Justice Staffan Vängby, proposed a radical change of the basic concepts in the right of access regulation in Chapter 2 of the Freedom of the Press Act. The proposal (SOU 1997:39) strove to distinguish between two kinds of information, *viz* on the one hand fixed or static information, and on the other dynamic or changeable information. The proposal recognised that the medium as such does not necessarily decide the nature of the information that it carries. A traditional paper medium, an index card file, for example, may contain information that is intended to be changed. On the other hand, an electronic medium may contain fixed information, such as write-protected numerical data or the finalised minutes of a meeting stored in a text database.

The Data Legislation Committee took it for granted that electronic media are on their way to dominating the information processing of public authorities. One consequence of this development is that fragmentation of information will become more and more visible and common. In other words, the previously mentioned definition of technical recordings as "any meaningful compilation of data" ought to be made visible in the text of the

statute and ought to serve as the basis for the regulation. This reasoning led the committee to propose that the object of access ought to be, not "official documents" but "official data". The concept of a document was to remain in the statute as one kind of "storage space for data" and a document as a storage space was to be characterised by its fixed nature. In the words of the committee, a document had "a defined content", *viz.* the content which was originally ascribed to it and which was not intended to be changed. Changeable "storage spaces" were called "databases". Databases, typically, contain data that are continuously updated and that may be presented in different combinations and formats.

The merits of the proposal may be discussed. Ultimately, it did not meet with success, above all because the idea of substituting "official data" for the well-known "official documents" proved to be too radical (too much ahead of its time?). In addition, a number of details of the proposed regulation were unclear. A subsequent legislative committee, The Committee on Openness and Secrecy, chose a more cautious strategy, marked also by a certain reluctance to acknowledge the notion of "potential documents". Its proposal (SOU 2001:3) reserved the concept "document" for fixed entities of information ("a certain information content in uncorrupted form") regardless of whether the information is stored on traditional or electronic media. Leaving details aside, it may be noted that, according to the committee, the key issue concerned the significance of so-called "routine measures" as a prerequisite for the accessibility of electronic recordings (see above). According to the committee, fixed electronic documents (such as the finished text of a decision) must be made available upon request regardless of whether this requires *more* than routine measures on the part of the public authority, whereas compilations of data (i.e. potential documents) must be made available only to the extent that this presupposes *no more* than routine measures. It may also be noted that the committee shaped the right of access to compilations of data as a sort of a secondary right. Neither the committee's proposal nor the Government Bill that implements it (2001/02:70) let the relevant provisions of the Freedom of the Press Act explicitly state that there are two kinds of electronic documents, the "fixed" ones and the "potential" ones. The Council on Legislation, which commented on the bill, considered this an unfortunate lack of clarity. The reason behind it is to be found perhaps in a persistent uncertainty, even uneasiness, with regard to potential documents and "fluid" access rights.

Thus, the latest revision of Chapter 2 of the Freedom of the Press Act continues to struggle bravely with the tension between fixation and flow. The struggle is bound to go on. It will involve continued work with basic concepts such as "potential documents" but also with basic policy issues regarding a possible strengthening of the right of access aimed at making full use of the potential of electronic media. A few remarks may suffice to sum up. They concern (a) the right to use information that has been obtained, (b) the situation of computer programmes, and (c) the development of information infrastructure.

Access rights do not only involve inspection of documents etc. Their value often depends on *how the information can be used*. Electronic media strengthen the interest in this aspect of access, for the simple reason that they lend themselves to much more extended and varied use than traditional media. For the minimalist this may seem more frightening than beneficial. For example, extended use rights tend to collide with the protection of the individual's data privacy and with intellectual property rights. The maximalist welcomes extended use, supports the idea of giving access to computer-readable data, and is critical of different kinds of data ownership that may stand in the way of using data obtained from the public authorities. Both views are reasonable and they have to be balanced against one another.

Computer programs are at the core of the concept of fluid information. In Sweden the right of access does not include a full-fledged right to examine functionality. There are certain obligations to document computer systems and the Personal Data Act of 1998 regulates a right to learn about the logic behind certain automated decisions. Computer program descriptions (including flowcharts and written code) are accessible as documents according to Chapter 2 of the Freedom of the Press Act. But there is no right to obtain computer readable copies of computer programs. Above all, there is no right to require that a public authority execute a computer program with input data supplied by the applicant. From the maximalist point of view one may ask why not. The only way a program can be understood is by running it. Reading lists of source code or, even worse, object code doesn't make anybody the wiser.

The information infrastructure can be designed with varying regard for openness interests. The electronic environment is sensitive in this respect. To elucidate, it is essential to design the information systems of public authorities so that they can support the kind of aims that access rights legislation seeks to achieve. As a simple example, consider a system that only permits retrieval of particular registered information items (e.g. decisions

with a diary number). Or consider a system where data of different kinds and belonging to different categories are stored in such bad order that all requests require time-consuming fishing expeditions and lead to frequent refusals, due to difficulties of assessing whether documents are official or not. Consider, on the other hand, systems that have been designed with a view to actively supporting openness interests – even when this involves extra costs and system functions that are not in the direct interest of the public authorities themselves. Such systems may contain personalised, cross-agency information services, alert services (e.g. for non-government organisations), databases for particular purposes (e.g. educational databases and statistical databases), and so forth. It may be objected that such extended services go beyond access rights as they are traditionally understood and that access rights have to do with more narrow purposes mainly involving control of public authorities. This is the minimalist view. The maximalist view is that electronic media enables a new vision of access rights. Why stick to the minimalist 'peep through the keyhole' kind of access? The modern knowledge society can and ought to have far more ambitious goals. In short, one of its key obligations should be to develop a rich notion of universal information services based on the traditional concept of access to official documents. For knowledge to grow, information must flow.

Claes Gränström*
Archives of the Future

1 Traditional perspective of archives

The conception of what archives are and constitute has changed throughout the centuries. This conception differs also between countries. The purpose of archives/records administration, similarly, has changed through the centuries. To begin with, the state authority regarded archives and archival administration mainly from a constitutional and legal perspective, as a safeguard for rights of property and ownership and as evidence of diplomatic and other proceedings. With archives thus viewed, it was only natural that access to them should be restricted.

Archives at this time consisted of clay tablets, papyri, parchment and, later, of paper documents. The mass of documents was unimpressive, and they could be mastered with relatively little difficulty. By the same token, inventorying, authenticity, search tools, appraisal etc. did not seem to pose problems. This, more or less, was the situation prevailing from the medieval era until the eighteenth and nineteenth centuries all over Europe. But in the nineteenth century things began to change. As administrations grew and the production of documents increased, special bureaucratic traditions developed. In the twentieth century, we saw real mass production of documents in the archives, especially during the two world wars. One dominant factor, of course, was the swelling of administration as a result of public sector expansion. The dominant medium of information was still paper, even though other media such as microfilm were beginning to be used. In most countries, even in democracies, access to documents in the archives was restricted.

After the Second World War, the situation changed. In many countries, the developed ones especially, the appearance of

---

* *Claes Gränström* is deputy director general at the National Archives Sweden. He has served on many governmental commitees as an expert on matters of, among other things, electronic archives. He is author and co-author of reports and books on archive legislation etc. He is currently chairman of the International Council on Archives (ICA) Committee on archival legal matters and has been working with legislative matters regarding electronic documents in several capacities within the European Union, amongst others the Document Lifecycle Management (DLM) Committee since 1995.

societies dominated, to a greater or lesser extent, by social engineering generated huge quantities of information and archives expanded accordingly. Electronic documentation entered the public service in the sixties and seventies, the idea being that a better and more advanced society could be created through greater production of information made more accessible.

One reaction against the collection of vast masses of personal data and social engineering took shape in the sixties and seventies, resulting in various kinds of data protection legislation all over Europe and also in many international conventions, recommendations etc. on the subject of privacy. Archival affairs were greatly affected by one aspect of this new trend, namely the deletion of personal data after its having been used for its primary purpose.

2 The four factors of decisive importance for archival work

2.1 Technological development

The technological development means that we have to deal with enormous masses of data. It is easy to talk of megabytes, gigabytes, terabytes, petabytes and even exabytes. But in more palpable terms, the National Archives of Sweden, for example, have taken delivery of some 2 terabytes of electronic records, containing 20,000 files and stored on about 10,000 data carriers, usually tape cassettes, corresponding in hard copy terms to 100,000 shelf-metres. Printing out on paper eliminates the possibility of automatic processing, whereas large volumes of data can now be transmitted from one place to another all over the world.

One important factor is that ICT development has resulted in the development of new areas in science and medicine, for example, which only a decade ago would not have been possible. New hardware and software is developing rapidly. The archives of the CERN laboratory in Switzerland contain hundreds of terabytes of data. In 1999 the pharmaceutical company Smith Kline Beecham were archiving 2 terabytes a year, and 2 gigabytes of regulatory documents are added daily: growth is on a logarithmic scale. This company will soon reach 1,000 terabytes.

This development will raise problems as to what documents are, how to store them, how to migrate them (i.e. to change their technical format without compromising neither contents nor context), and problems of authenticity. The difference compared to

the paper world is that in this ICT world you cannot wait: you have to plan and act even before the information is created.

2.2 The democratic process

Today, and perhaps in Europe especially, we are faced with a new situation. It can be argued that we have a new society, one in which people have become more educated and critical. They have become independent and are taking a growing interest in the way society is administered. This, coupled with the rapid development of ICT and within the European Union, is making citizens much more interested in matters regarding democracy and access to documents, which is seen as a right and not as a privilege (see about Article 255 in the Amsterdam Treaty below). The growth of historical interest can furthermore be linked to these issues, as the societal function of historians is to describe and explain the past, both the more distant but, not least, the recent past.

The situation up to the end of the last century was that the degree of openness and the extent to which documents kept by Governments, agencies and archival institutions were legally available to the public varied a great deal, depending on differences in national traditions, rooted as they were in historical experience and inherited concepts of right and justice. Access to documents is in many countries today seen as a democratic right and as the best way to inspire confidence in the public administration. Arguably, this also enhances legitimacy.

2.3 Internationalisation

As we have already seen, attitudes and legal positions regarding access and protection of privacy varied from one country to another. Not so today. The most important factor in Europe is the European Union. Much legislation is harmonised through its directives etc. Perhaps the best-known directive is the so-called Data Protection Directive from 1995 (95/46/EC), which should have been implemented in 1998. This directive is meant to facilitate transfer of personal data between EU countries and so-called third countries, which have the same level of protection as set within the EU. Another important directive is that on certain aspects of copyright and related rights in the Information Society (2001/29/EC), which has implications regarding the preservation and availability of information.

Then there is Article 255 of the Amsterdam treaty of the European Union, laying down that the citizens of the Union shall have a right of access to documents in the EU institutions. Regulations regarding this right have been elaborated and were adopted in May 2001. In the Green Paper on Public Sector Information: A key resource for Europe, it is said that public sector information plays a fundamental role in the proper functioning of the internal market. In this paper a comparison is made with the United States, where – ever since the Freedom of Information Act (which went into effect in 1967) – the federal administration has pursued a very active policy of both access to and commercial exploitation of public sector information.

2.4 Changing structures in society

Formerly, we lived in a more stable society whose institutions and structures seldom changed. Today, we are living in a rapidly changing society. Old structures are giving way quickly. The privatisation of public functions has become more frequent all over the world. Furthermore, the role of the nation-state is questioned and new types of transborder structures are emerging. This tendency of rapid changes and supranational structures will most likely accelerate in the future. It has affected archival work in many respects and to a considerable extent. Not least, there are changes in mentality in that public authorities are becoming more open to the public. In Sweden the ongoing development of so-called '24-hour agencies' can be seen as an example.

3 Some elements of archival work

3.1 The concept of a document/archive

It used to be easy to determine what a document was. It was usually a paper with information, which was stable and difficult to manipulate. It had been either received or drawn up by an agency or private body, i.e. an archive creator. The agency or body was also easy to distinguish and the routines were relatively stable.

Today a different situation applies. In the electronic world of large databases, it is not so easy to determine what is a document and which agency/body is the archive creator or is responsible for the information. The Regulation of the European Parliament and of the Council of 30 May 2001 regarding public ac-

cess to European Parliament, Council and Commission documents gives the following definition:

> – "document" shall mean any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility.

This definition may be clear concerning the more stable and fixed paper documents. But regarding electronic information it is not enough. In Swedish legal doctrine, another type of document has emerged since the 1970s, namely so-called potential documents, which can be said to exist only on demand and do not exist in advance. They constitute official documents and are thus available to the public. Now a new Government bill has proposed that better predictability should be established – that is, that there should be existing and finished documents in the electronic environment. This proposal cannot resolve all difficulties, and more work will have to be done to elaborate more detailed rules. As we see it now, this puts more emphasis on the registration, the establishment of metadata etc. at the records creation phase, where it must be decided even in databases what constitutes existing and established documents which are accessible to the public. It should be mentioned that in Sweden archives consist of official documents, which means that the archival authorities have to deal with older records as well as documents of today. Definitions of what a document is and what an archive consists of vary but it is necessary for each country to choose and apply *one* clear definition of these phenomena in the electronic era.

I believe this to be the only solution. Otherwise, it may be impossible five or ten years after an event to decide what kind of combinations of data were accessible to the creator of the archive and therefore constitute official documents in an electronic environment.

3.2 Arrangement and description

When it has been established what constitutes a document, this document must be registered or catalogued so that the information will be available both to the agency itself and to the public, and also in the long run for research and evaluation. How this is done differs from one country to another all over the world. In countries with a tradition of freedom of information, registration

and cataloguing of documents have a stronger position. This is clearly shown by developments within the European Union and the Council of Europe.

If registration and cataloguing in the paper world could be done without too many difficulties, the situation in the electronic world is quite different, owing of course to the four factors mentioned above, in subsection 2.

3.3 Appraisal/deletion

Appraisal, which means the evaluation process of what documents to destroy and what to save for perpetuity, and deletion, which is the destruction of documents, are rapidly becoming one of the toughest tasks of archival work. Obviously, we can't keep everything, even though the price of data carriers is steadily falling. The difficulty of this task is compounded by the factor of privacy, which has become so manifest in recent decades. Take, for example, the EC directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, where the main principle is to destroy personal data after they have been used for their primary purpose. If this were to be fully realised, the result would be disastrous for free access and research possibilities. A balance must be struck between the conflicting interests.

In Sweden, the National Archives has defined deletion as follows:

- deletion of official documents,
- deletion of data in connection with transferring information to other data carriers, if this means
  - loss of information,
  - loss of possibilities to combine data,
  - loss of possibilities to recognise or find data,
  - loss of possibilities to establish the authenticity of the information.

A clear definition of deletion of this kind is necessary in the computerised society. Moreover, I believe that the definition should be set down in law.

The need to keep data is also growing rapidly in a world where human beings can influence the climate so very much and where so much can be done in the medical field.

It also has to be remembered that these electronic documents form part of our cultural heritage. UNESCO, in its Mem-

ory of the world programme, realised this need and has initiated several projects for preserving our digital heritage.

3.4 Authenticity/migration

Matters of authenticity are creating quite new problems regarding electronic documents as compared to paper documents. In many cases today, you have no paper documents, only electronic ones. In addition, the transborder data flow both in the public and in the private sector has made it necessary for norms of authenticity and legal validity to be agreed at the international level. Then again, the fact – that in many countries electronic documents are now being transferred to archival institutions much earlier than the paper documents were – means that these institutions have to guarantee validity and authenticity of the electronic documents in the long run through migration etc.

4 Future

It has to be recognised that archives are created and kept for certain purposes. Initially, they served the interests of king and government. Today, the more democratic interests prevail, i.e. public access. Furthermore, documents of extreme importance, for example regarding the environment or regarding the individual (such as patient files), will in the near future exist only in electronic format, which generally means that they must be kept in this way. The archival/records administration must adapt accordingly.

Furthermore, the principles of archive maintenance prevailing until now, i.e. the principle of provenance, can be questioned but apparently still holds good. According to the Swedish interpretation, this means that both text (information) and context (the original structure, in which the text was created) must be preserved. This has become even more important in the electronic environment. This interpretation has been acknowledged in many research projects all over the world. Very simply, it is a matter of order and discipline in the archives/records administration throughout the lifecycle of the document.

It must also be stressed that electronic documents form part of our cultural heritage. It is generally easier to conceive of clay tablets or parchments letters as a part of that heritage, but it should likewise be evident that electronic documents have fundamentally the same purpose as paper ones, namely that of stor-

ing text on a data carrier in a certain context. The problem is that we now have, and will continue to accumulate much more data, and data of enormous complexity. This linked with the fact that electronic documents are much more fragile and transient by nature, makes the future very exciting. Looking centuries or millennia ahead and trying to foresee what kind archival of information we will have access to, one is easily bewildered. It is almost like science fiction, on the lines of Asimov's Foundation books describing the knowledge-based planet Terminus, where all data from the Universe are going to be kept, so that civilisation can survive the fall of the empire.

Part IV:
ICT in Commerce and Work

Christina Ramberg*
Contracting on the Internet – Trends and Challenges for Law

1 Anonymity versus community

In the childhood of the Internet, many anticipated an open cyberspace where anybody could participate and no one would know who was acting at the other end of the line. Cyberspace was furthermore thought to be a lawless Paradise where no legislator or national state could reach out to regulate or punish certain behaviour. In an open environment it is technically complicated to ascertain the identity of senders and receivers of electronic messages. And without identity there is no incentive to behave honestly, since dishonesty cannot be pinned on a person deserving of punishment. Many feared that the Internet would become a lawless inferno and that doing business on a basis of honesty and trustworthiness would be impossible as long as there were no means of identification and no authority of law.

However, we have not seen either the lawless Paradise or the lawless inferno emerging on the Internet. Actually, what is now happening in cyberspace is not dramatic at all – but instead very similar to what we see in the traditional physical world ('cyberspace unplugged'): We see closed communities where deals are concluded between people who know and trust each other. Not everyone is allowed to participate in these communities. And misbehaving participants are severely punished by blacklisting and/or exclusion from further participation. What I mainly have in mind are closed B2B marketplaces where buyers and sellers in certain products meet to conclude a deal.

Another feature of the Internet of today is that, instead of being lawless, it is overloaded with law. Now every national state claims to have jurisdiction over everything that occurs in cyberspace. The national state has proven surprisingly successful in enforcing its regulations against Internet activities concerning its national interests. National states have also been very keen to regulate activities on the Internet.

---

* *Christina Ramberg* is a member of the IT Law Observatory. See presentation in Annex 1.

In the following I will describe how legislators have responded to these trends on the Internet. I will also try to identify the lessons to be learned from attempts hitherto at regulating e-commerce.

2 The threat of anonymity

The fact that persons may act anonymously on the Internet is extremely frustrating from a legal point of view. We may pass thousands of legislative acts stating that promises should be kept, that we are not allowed to lie about each other and that we must not defraud others, but law serves no purpose if there is no practical way of tracking down the law-breakers.

Everybody knows that law is not the best guarantor of obedience to the norms of society. Instead the most important tool is social pressure. The risk of being branded as untrustworthy by family, friends and business partners is far more effective than any legislation. Our society has gradually become larger and more complex. The expansion of markets has made it increasingly difficult to ascertain the trustworthiness of potential business partners. This, in turn, has made law an increasingly important supplement to social pressure. When we enter into transactions with people whom we do not know and whose reputation is unfamiliar, we trust that they will behave honestly since they do not wish to take the risk of being punished by legal sanctions.

If on the Internet we do not know whom we are dealing with and we cannot establish their identity after a deal is made, after a promise is broken, after a lie has been put about, or after we have been defrauded, neither social pressure nor the law will serve as a means of preventing dishonest behaviour. This is indeed a great challenge to law. How can we preserve honesty in a cyberspace where anonymity flourishes?

As a response to this anxiety, the technology of digital signatures came as The Perfect Solution. Digital signatures based on the concept of Public Key Infrastructure (PKI) make it possible to create electronic identification. With the help of a certificate issued by a third party – i.e. someone other than the person who needs to establish someone else's identity – the identity of the sender of an electronic message can be ascertained. The level of security varies, depending on the technology used, the security routines of the third party or its subcontractors and – most importantly – the means whereby the third party initially identifies the certificate holder. In short, the party needing to identify the sender of an electronic message can choose to rely, not on the

sender himself, but instead on a third party certifying the sender's identity. Some five or ten years ago many believed that PKI digital signatures would solve the fundamental problem of lack of trust in cyberspace and provide a necessary infrastructure for commercial transactions on the Internet. But it has turned out that digital signatures are not in high demand.

There are many reasons why digital signatures are not widely used. *First*, it has turned out that electronic transactions are not made in the open cyberspace between total strangers. Instead most transactions are made in closed communities where the parties' trustworthiness is a requirement for access and where the parties have 'met' before and by contract decided how to make future transactions. In such communities there is less need to put trust in a third party that issues certificates and less need for extremely secure identification methods. *Second*, digital signatures are cumbersome to implement since they require that third parties be recognised widely by the users, which has turned out to be quite complicated to achieve in practice. *Third*, to establish a high level of security with PKI is costly and there are other less secure – but secure enough – methods that can be used in closed communities and are less costly. In closed communities, the high and costly security that the PKI technology provides is not always necessary.

3 How law responds to the threat of anonymity

The legislators' response to the threat of anonymity is interesting to study. Quite early on in Sweden (in 1996) the Ministry of Justice held a hearing and asked business to what extent legislation was needed in relation to digital signatures. Not many found it worthwhile to attend this hearing. The representative of the International Chamber of Commerce strongly argued against legislation and claimed that the market forces would evolve slowly and that it was crucial to preserve flexibility. He said that legislation most likely would prevent development instead of helping business. The persons present at the hearing who argued that legislation was needed were mostly technical experts representing the digital signature industry. They argued that people were unfamiliar with the idea of electronic signatures and would not dare to engage in electronic transactions unless the legislator explicitly stated that such transactions were legally valid and had sufficient evidentiary value. At that point the Swedish Ministry of Justice decided that Sweden need not take any legislative initia-

tives within the area of electronic signatures. In my opinion this was a wise decision, although I must admit that at the time I was surprised that business outside the digital signature industry did not ask for the legislator's help.

Internationally the approach was different. UNCITRAL (the United Nations Commission on International Trade Law) embarked on a new project in 1997 relating to digital signatures. That work was initially much inspired by the already enacted Digital Signature Act in Utah and the proposed legislation on digital signatures in Germany. There was a heated discussion at the first meeting as to whether legislation on digital signatures was needed and the importance was emphasised of not favouring one technical solution at the expense of others. The US delegation strongly questioned whether any regulation was needed. Since the same delegation at an earlier meeting had spoken in favour of regulating digital signatures, this intervention caused some confusion. The UNCITRAL negotiations lasted for four years, and the Model Law on Electronic Signatures was adopted in 2001. Throughout the negotiations the necessity and purpose of the Model Law remained a moot point. There was a constant struggle concerning the extent to which the rules should be technologically and media neutral. The influence from the industry representing certain types of technology (mainly PKI) was very strong. Another discomfort in the negotiations was the slowly emerging awareness among the delegations that the vision of the open anonymous Internet was not coming true with respect to electronic commerce.

On the European Union level there was great eagerness to show that actions were being taken to facilitate electronic commerce. It was thought that the way to facilitate for electronic commerce was by quickly enacting directives. The European Union would then be promoting legal certainty and harmonised law within the Common Market. It should come as no surprise to learn that the directives on electronic signatures and e-commerce achieved the exact opposite: legal uncertainty with respect to the legal effects of electronic signatures, disharmony within the Member States since the implementation of the ambiguous directives differs from one Member State to another, and obstacles to technological development and business flexibility, since the directive on electronic signatures indirectly favours a particular technological solution (PKI).

4 The threat of closed communities

As described above, the anonymity of Internet transactions posed a fundamental threat to society and it was feared that commercial dealings and trade would become impossible in the new electronic medium. However, the markets themselves circumvented this threat. Instead of using high security PKI technique for identification among strangers, markets developed closed communities where it was possible to establish the trust among participants that is necessary for commercial dealings. This initially unexpected development also poses threats, but of a less fundamental nature than the threat of anonymity:

a) When commerce is carried out in closed communities there is always a risk of the market forces becoming distorted. If not all potential buyers and sellers are allowed to participate in a market, competition may become inefficient. As we all know, the importance of competition and anti-trust law has increased considerably in recent decades, due to the idea that efficient competition is crucial for societies based on a market economy.

b) There are concerns that closed communities may become so dominant within their sphere of commerce, that they abuse their dominant position against participants in the marketplace.

c) Also within the individual closed community, efficient competition may be distorted by participants manipulating the price-setting mechanism by forming auction rings or by other collusive behaviour.

d) Another threat of closed communities is the single individual's inability to conduct business in a situation where he is not allowed access or is expelled from the closed community. The increasing use of different black-listing and white-listing schemes may severely damage the reputation of individual persons and businesses and in effect prevent them from engaging in Internet transactions.

The problem of anonymity on the Internet is to a great extent solved by the closed communities. At the same time, they entail negative implications mainly with respect to questions of efficient competition.

5 How law responds to the threats of closed communities

Legislators have been much less eager to take action against the threats of closed communities as compared to the threats of anonymity. This is not surprising. The threat of anonymity is aimed at the very foundations of society, whereas the threats of closed communities are less severe. Traditional law is fairly well suited to deal with the problems that closed communities entail. There are examples from German and US competition authorities where the transactions carried out in closed Internet marketplaces have been examined from an anti-trust law point of view. But we have not seen any initiatives to specifically regulate the risk of anti-competitive elements in Internet marketplaces as opposed to traditional physical marketplaces. Competition law is media-neutral and thought best kept that way. The challenge for competition law is to harmonise worldwide in order to avoid the problems of determining the law applicable to activities carried out in non-physical marketplaces and ensuring that that law is enforceable.

Many of the other legal difficulties in relation to activities in closed communities are best solved by the marketplace itself by contractual regulation in the Membership Terms and Conditions of Sale. There still remain areas where national law may create obstacles – such as requirements of licensing or form for auctions, and approval by authorities for certain types of transactions. Another problematic area is mandatory national consumer protection law and its differences between different states, for example as regards the extent to which a consumer is entitled to cancel a deal made by electronic auction. These examples, however, are of minor importance, and will hopefully be sorted out by the slow but inevitable process of gradual harmonisation of law. These are problems which are likely to be solved, not by new legislative efforts, but rather by minor amendments to the existing national law.

6 The lessons to be learned

6.1 Be reactive – not proactive!

It was already observed by Aristotle and has been repeated many times since, that a sovereign's possibility of influencing citizens' behaviour by legislation is very limited. This is particularly so in

the field of private law. The role of legislation in that area is mainly to codify already existing conduct – not to proactively steer behaviour in certain directions. There was, understandably, great concern that the threat of anonymity would make commercial dealings in cyberspace impossible. However, the legislators' initial attempts did electronic commerce more harm than good. Eagerness to establish legal certainty – to assure the markets that electronic transactions were legally valid – led to favouritism of a particular technology (PKI). The legislator gave the misleading impression that for a transaction to be legally valid it had to be effected by PKI technique. And since business was not prepared to pay for the excessive security and cumbersome administration that this technology entailed, the development of e-commerce actually became slower than necessary.

The legislative experiment in relation to electronic signatures has taught us a lesson. It is better to be reactive than proactive within areas that have not yet matured with respect to business models, usages, technology and actual practical problems. I agree with the initial approach taken by the Swedish Ministry of Justice: Let us wait and see if there is any real need for regulating electronic signatures. Let us wait and see if any particular problems or abuse arise before we take legislative action. Let us trust that the general law is able to handle the most urgent and most fundamental issues. If we see a need for particular regulation, we will be able to do something about it in due course. The legislator should not take the lead and try to steer development. It is better to be reactive and take action when there is a real existing problem, than to be proactive and try to foresee the possible problems and regulate before they have come into existence. A proactive legislator may do more harm than good by misleading the citizens to believe that there is Only One Single Solution to a problem that may be solved more efficiently in other ways than the one suggested and regulated by the legislator.

The fundamental issue of trust in a marketplace can be resolved in many ways. It was initially believed that the only way to create trust was to enact legislation on electronic signatures. In the event, however, the markets found other means of establishing trust and confidence. The lesson to be learned from this experience it that the role of legislation is not to create trust, but merely to support already existing trust.

It is my hope that the present fallacy among businessmen that the PKI technique is essential in order to create legally valid contracts, will soon fade away. I am, however, concerned that this may take many years and in the meantime cause unnecessary

investments in a costly infrastructure, as well as slowing down the development of e-commerce.

6.2 Be media neutral!

Another lesson to be learned is that the problems in contract law are eternal and exist independently of the medium used to perform the transactions. The eternal problems are, among others, when and how a contract is formed, and the liability for fraud, mistake and delayed or defective performance. It is not wise to regulate these issues specifically for electronic transactions, since the problems occur in all types of medium used. In the future, it will be almost impossible to distinguish between transactions made by electronic means of communication and others. Transactions will to a large extent be a mixture of electronic and non-electronic communication. It would be devastating to have legal regimes addressing the same problem differently, depending on what medium was used to conclude a deal.

6.3 Harmonise law internationally!

The third lesson to be learned is that cyberspace is not a lawless inferno or Paradise. At present cyberspace is overloaded with law – which most persons associate more closely with Hell than with Paradise. All national states claim to have jurisdiction at the same time and in parallel in cyberspace. The solution to this problem is to harmonise law worldwide. It makes me very optimistic to see how greatly the efforts and success of international harmonisation of contract law have increased during the past decade. Electronic contracting on the Internet has helped to speed up this development of harmonisation and is likely to go on doing so.

Agne Lindberg, Henrik Bengtsson*
Database-Aided IPR Due Diligence

1 Introduction

In an interesting new book, *Rembrandts in the Attic – Unlocking the hidden value of patent* (McGraw Hill 2001), Kevin Rivette, chairman of Aurigin Systems, and David Kline highlight the need for corporate strategies aimed at identifying, protecting and commercialising intellectual property rights. Basing their analysis on in-depth studies of how major companies such as IBM, Gillette, Microsoft, Xerox and Lucent have succeeded – or failed – partly as a result of their intellectual property identification and protection strategies, Kline and Rivette draw the conclusion that there is an enormous potential for companies in maximising their intellectual property right assets. Kline and Rivette quote IBM, among others, as an example of how an aggressive IP strategy can help in boosting IP-related revenues from $ 15 billion in 1990 to more than $ 100 billion in 1998. On the other hand Kline and Rivette tell the story of Kodak, which in 1960 embarked on a long patent litigation journey aimed at disqualifying Polaroid's Instamatic patents, a litigation which cost Kodak more than $ 40 billion and ended in failure.

Since the US patent system takes a more liberal attitude towards the patentability of business methods and technology, patents form more of a core role in a US IP strategy. In Europe – and Sweden – patents will not serve such a central role, due to the fact that the Swedish legislator and the European Union, and in particular the European Patent Office and the Swedish Patent and Registration Office, do not have as generous an attitude as the US Patent Office when it comes to affording software and methods patent protection. The same considerations as apply for patents do, however, also apply to other intellectual property rights such as copyrights, trademarks and tradenames, design rights and semi-conductor rights, which, if identified and duly

---

* *Agne Lindberg* is a member of the IT Law Observatory. See presentation in Annex 1. *Henrik Bengtsson* is an associate with Delphi & Co Law Firm's Stockholm office. He specialises in IT and intellectual property law. Among other things, he has worked as in-house counsel with the Internet consultancy firm Framtidsfabriken AB where he gained particular experience in analysing companies' possession of intellectual property rights.

protected can serve as a major competitive advantage and be of great commercial value.

In the course of our daily advising of clients, in particular IT, telecommunication and media clients, we have experienced an increase in the importance of intellectual property rights for a successful market penetration and a method of successfully keeping competitors on a distance. In order to be able to give clients qualified advice on the management and strategic handling of intellectual property rights, as practising lawyers we have devoted substantial efforts to developing a method for taking an inventory of intellectual property rights, the specifics being that a so-called IPR Due Diligence needs to take all intellectual property aspects into account and that it addresses issues such as multiple and over-lapping protection of intellectual property rights. The result is a computerised database aimed at managing the great amounts of information, which emerge as a result of an IPR Due Diligence. The overall contents of the IPR Due Diligence method will be described in short in this article. The ambition of this article has, however, primarily been to describe the general issues posed in an IPR Due Diligence and to, very briefly, exemplify the legal issues with examples from different intellectual property law areas. Finally, the article aims to provide an example of how legal practice today involves extensive use of Information Technology.

2 Briefly on accounting issues and intellectual property rights

One major reason for the necessity of performing an IPR Due Diligence is that intangible assets in many cases are not visible in a company's balance sheet. Although many voices have been raised, calling for intellectual capital to be made part of the balance sheet, current accounting rules do not provide for intellectual capital and least of all for intellectual property rights to be stated in the balance sheet, apart from exceptional cases. Trademark rights, for example, may not be entered in the balance sheet at all. Consequently, if no IPR Due Diligence has been performed within a company, you will not be able to find any comprehensive documentation listing its intellectual property assets and visualising their strength. Instead the information, if any, about the company's intellectual property rights is normally scattered, and stored in different departments. This being so, an over-

all review is often necessary in order for intellectual property rights of interest concerning such a company to be identified.

3 The overall purpose of conducting an IPR Due Diligence

Due Diligence procedures are normally carried out when one company is about to acquire another. Such procedures are very often performed within narrow time limits and normally are aimed only at identifying certain documentation, whereof intellectual property rights form a minor part. The purpose and methods of performing an IPR Due Diligence differ in many respects from due diligence procedures performed in connection with a company acquisition, since the primary aim of an IPR Due Diligence is to ascertain which intellectual property assets exist and which are used, and only at the second stage to establish whether there exists any documentation regarding the intellectual property rights. In a word, our primary objective when performing an IPR Due Diligence could be compared to a financial SWOT analysis[1], but this time aiming to:

1. identify the value of intangible assets not accounted for in the balance sheet;
2. identify the intellectual property rights forming the company's core values;
3. identify intellectual property shortages;
4. ascertain the possibility of otherwise of registering or otherwise protecting the intangible assets;
5. establish future routines for the identification of intellectual properties;
6. establish a future IPR strategy to be adopted by the board;
7. identify the measures are necessary to compensate intellectual property shortcomings.

Furthermore, an IPR Due Diligence differs from a traditional M & A due diligence insofar as the IPR Due Diligence will often be helpful in other situations than an M & A situation.[2] For example, a company may gain advantages by performing an IPR Due Diligence before the launch of a new product. By identifying the intellectual properties connected with the product in question, the company will be able to achieve more comprehensive protection

1 **S**trength, **W**eaknesses, **O**pportunities, **T**hreats.

2 Merger & Acquisition.

of the product and thus a market advantage, since it will then be able to keep its competitors at a comfortable distance. Other situations where a company could gain advantages from having identified and listed its intellectual property assets are for example:

1. when procuring insurance coverage;
2. when signing licence agreements which are of core importance to the company;
3. when procuring capital, for example by a new issue of shares;
4. when acquiring a product.

If a company has performed an IPR Due Diligence before entering into the aforementioned transactions, its possibilities of negotiating better commercial conditions and achieving greater legal certainty will be correspondingly increased.

4 How to identify the rights concerned and the protection afforded

As mentioned above, the purpose of an IPR Due Diligence is firstly to ascertain which intellectual property rights exist and are used within a company. Hence, in the initial phase of an IPR Due Diligence procedure, the primary objective is to identify, for example, the material and symbols and words used by the company in its market activities, but also to identify the software products, databases and other technology products the company depends on. Once such critical elements are identified, the next stage of the due diligence procedure is to ascertain whether:

1. the elements are protected by intellectual property rights;
2. if so, the scope of such protection;
3. the elements are used within the scope of such protection;
4. the elements infringe third-party rights.

In order to ascertain whether an element is protected by intellectual property rights, we have to ask a wide range of questions, ranging from practical issues such as whether the company provides for restricted computer access to documents stored in computer networks (the answer to that question is necessary, for example, in order to establish whether information is protected as trade secrets) and whether the company has stored marketing ma-

terials (necessary, among other things, in order to establish whether a trademark is protected by means of acquired distinctiveness on the market or whether the trademark has been used in the past five years and consequently is not in danger of deregistration).

In addition to the aforementioned identification of material and information supporting the existence of intellectual property rights, a range of searches of publicly available patent, design, trademark and tradename registers is necessary in order to establish whether an element has obtained protection by means of registration, and in that case, the scope of the protection. Such searches will not only extend to searches of national registers: a search will also have to be made of international registers such as the trademark register of the Office for the Harmonisation of the Internal Market (OHIM). Such searches must not be limited to the registration certificate as such, but must also be more detailed and for example analyse whether a trademark registration is dependent on third party consents submitted to the Patent and Registration Office or OHIM.

5 Has the company duly acquired the rights?

Having established which elements are of interest in the due diligence procedure, it is of the utmost importance to analyse whether the rights have been duly acquired from third parties and if the elements are surrounded by restrictions as to their use. As regards copyright, for example, the general principle under Swedish copyright law is that the copyright stays with the originator unless otherwise agreed. Works developed as part of an assignment are to some extent licenced to the assignee, but if the parties have not agreed on a full transfer of copyrights, the assignee is only granted a limited licence to use the works. Similarly, since the Anglo-Saxon copyright "*work for hire* principle" does not apply under Swedish copyright law, copyright (with the exception of computer programmes and supporting material) instead remains with the employee. This means that employment agreements and consultant agreements have to be analysed in order to establish to what extent the employer has acquired the copyright in works created by the employee. Since the use of employees hired from manpower rental firms has become quite common, arrangements of this kind will also give rise to complicated copyright assignment issues.

Similar principles also apply under patent law where the employee, depending on the kind of invention and whether it has been developed in the employee's spare time or not, is entitled to remuneration for patentable inventions.

Summing up, in the course of a due diligence procedure, it will be necessary firstly to ascertain where the intellectual property right has originated and if and how it has been acquired by the company. In many cases, employment and assignment agreements can be used as the basis of such an analysis. It is, however, very important not to simply identify the written existent agreements and to base an analysis on such facts, but also to go beyond the written documentation and to identify verbal agreements and other factors which indicate the intellectual property rights have been acquired in a certain manner.

6 Are there any limits to the intellectual property rights as such?

Once having identified which elements are of interest to protect and whether the rights to such elements have been duly acquired, the next stage will be to ascertain whether the rights are limited as such. The possible limitation of an intellectual property right can be instanced with a trademark registered in connection with a disclaimer excluding part of the trademark from protection. Another example is trademarks of a descriptive or possibly generic character, which gives them low distinctiveness, thus limiting the scope of protection to more or less identical symbols or words. Similarly, patents need to be analysed in relation to the product which it is intended to protect, in order to establish whether the patent claims mirror the actual product or whether there are any limitations in the patent protection as such.

Once any limitations of the intellectual property rights have been identified, the findings can be used as the basis of a strategy to strengthen the protection of intellectual property rights which are limited in scope. The findings will also strengthen the awareness of possible infringing consequences of the company's use of intellectual property rights, which is limited as such.

7 Present or future threats towards the existence of the intellectual property right

Apart from the fact that an intellectual property right may be limited in its scope due to disclaimers or other such limitations, it is also highly interesting to analyse the relative strength of an intellectual property right in order to establish whether it is able to resist attacks from competitors or, possibly, infringers as a defensive measure in infringement proceedings.

Industrial property rights in particular face the risk of de-registration or invalidation, due to their having been registered despite the existence of impeding rights or other absolute grounds for registration refusal. A trademark could be de-registered, for example, on the grounds of degeneration, partial or full non-use during the last five years or the fact of its having been registered despite the existence of a confusingly similar trademark. These risks of de-registration also apply to patents, where, especially in patent proceedings, there is an imminent risk of an alleged infringer claiming that the patent is invalid due to formal shortcomings preceding the registration. One very common counterclaim in such proceedings is that the patented invention was not new, due to the existence of other similar inventions or due to the inventor having made it available to the public before submitting the patent application, when it was patented. The same principles apply to registered designs. Hence, in the course of the IPR Due Diligence it is important to identify any such potential threats against registered industrial property rights and, if any formal shortcomings existed before the date of registration, to take steps to offset them.

8 Maintenance of an intellectual property right

Where industrial property rights are concerned, it is particularly important to monitor actual and potential competitors' applications for patents, designs or trademarks falling within the protective scope of the company's industrial rights. Hence, it is often important that a company has established routines and structures enabling it to react to possibly infringing applications for the registration of new industrial rights. Such routines are of increasing importance, since the public scrutiny of industrial property applications has decreased and will decrease further (cf. the proposed new Swedish Trademark Act, under which the registered trademark proprietor is solely responsible for monitoring applications

submitted to the Patent and Registration Office and for opposing such applications within a certain length of time period). Consequently, the scope of an IPR Due Diligence would also need to include the identification of routines for the monitoring of intellectual property rights.

Intellectual property maintenance routines could also take the form of trademark use instructions where the users of the company trademark are instructed to use the trademark in capital letters and in connection with the TM-symbol or the registered trademark symbol ® so as to avoid degeneration of the trademark and to establish bad faith on the part of trademark infringers.

9 Intellectual property infringements

An intellectual property right is of little or no use if it cannot be enforced in relation to third parties. Thus, an IPR Due Diligence should aim at identifying whether the company concerned is, or has been, subject to intellectual property rights infringements and how it has responded to them. In this regard it could be of interest to analyse the company's standard procedures, if it has any, for attacking infringements. In Swedish case law, there are examples of rightholders who have tried to enforce rights in a dubious way and where, as a result of infringement warning letters, the alleged infringer has counter-sued and successfully claimed that the sending of warning-letters amounted to unfair marketing.

On the other hand, an active counter-infringement policy is important since the legal consequences of not instigating procedures towards an infringer could be the right-holder losing its right to request interim measures, or, at worst, the parallel use of an infringing trademark being recognised in court.

10 Limitations as to the use, assignment or modification of intellectual property right protected elements

Finally, since intellectual property rights could in many respects be subject to limitations as to their use, assignment or modification, an IPR Due Diligence report needs to take into account whether such use, assignment or modification is subject to limitation. One obvious limitation to the use of intellectual property rights could be stipulated in licensing agreements for the intellectual property right in question. Common examples of such restrictions are the format in which the intellectual property right

may be used (such restrictions are often, implicitly or explicitly, stated in copyright and trademark licences), whether the licence may be assigned or sub-licensed and whether the works subject to the licence may be modified by the licensee, such modification being subject, among other things, to mandatory copyright rules on modification and moral rights.

The method for establishing the limits of the permitted use, licence and assignment is firstly to analyse licensing agreements entered into by the company. Secondly, such rights could be evident from the licensor's and licensee's historical behaviour, which may indicate that the licensor has consented to certain forms of use or certain possibilities of modifying the licence object – such information to be gathered through interviews with employees of the company familiar with the historical licence situation.

11 Use of databases to structure IPR Due Diligence information

The IPR Due Diligence database developed in our IPR team is aimed at making the IPR procedures more efficient and able to cross-reference the findings of an IPR Due Diligence in a more sophisticated manner than would be possible if the material had only been categorised in manual files. There are a number of advantages in using database structures when gathering and analysing the vast number of documents and other information emerging in the course of an IPR Due Diligence procedure. Firstly, the material may be cross-referenced so as, for example, to generate a report on which intellectual property rights are connected to a certain product. Secondly, if a flexible database structure is used, it is possible to generate a number of reports which are useful in the future strategic management of a company's intellectual property rights, such as reports indicating which intellectual property rights are about to expire, which products that have not been protected in the best possible way available and which agreements relate to the licensing or sale of a certain intellectual property rights. The use of a database structure also simplifies matters in the event of a separate product or department of a company being sold to a third party, since the intellectual property rights and agreements affected by such a sale can then be identified immediately.

Furthermore, if a database is used as the information-gathering instrument in the course of an IPR Due Diligence pro-

cedure, the risk of personal aberrations if the analysis is performed by several different persons is less than if the procedures were to be performed manually, since that would allow the individuals more scope for using their own methods for analysing the material. If a database is used, the technology can be used to streamline the way the information is analysed, and the provision of support functions such as explanatory texts will make the analysis far easier.

In the rapidly developing technology environment, it could also be observed that the technology could be used for developing database supportive functions like that described above. Voice recognition and optical character-reading mechanisms are good examples of technologies which could be used to enhance the information content of a database. Extended search engine and hyper-linking possibilities could also be used to enhance the possibility of quickly cross-referencing, say, trademark registrations with licensing agreements for the trademark at issue. Databases of the said kind can also be connected to scanning facilities, so that information today stored in a manual format will be readily available within the framework of the database, which in turn will make the management and administration of intellectual property rights far easier. With the extended possibilities of making databases and information available via web interfaces and intranets, the information contained in an IPR database could also be distributed within an organisation in a manner which is quite different from the use of paper-based documentation systems.

12 Concluding remarks

Summing up, the corporate importance of intellectual properties seems to be growing as companies head into more service-intense areas of business where intangible assets are of crucial value to them. At the same time, with the intellectual property law field growing more and more complex, it is often difficult for a company to obtain an overview of intellectual property rights issues which really matter. Many companies are therefore faced with a situation where it is necessary to adopt a new attitude towards intellectual property rights and to adopt procedures and strategies ensuring that the elements eligible for intellectual property right protection are identified and are registered and upheld to the best extent possible. This also means to say that intellectual property issues will become more of a focal consideration

in a company's daily board work and possibly also at meetings of shareholders, since the existence of a certain right could be crucial to the whole existence of a company.

The main objectives of an IPR Due Diligence procedure are to establish:

1. which elements are of interest for the review;
2. whether those elements are afforded intellectual property right protection and – in that case – which protection and to what extent;
3. whether the company has duly acquired the rights;
4. whether there are any restrictions on the intellectual property right at issue;
5. whether there exist any present or future threats to the intellectual property rights identified;
6. whether there are any restrictions on the use, modification or assignment of the intellectual property right at issue.

Once these facts are established, the company which is subject to the IPR Due Diligence procedure will have an overview of the intellectual property rights which are crucial to its operations and of its intellectual property weaknesses and strengths. Further, the company will be able to identify the measures necessary in order to uphold and strengthen the intellectual property rights in question.

If a database instrument is used in the performance of an IPR Due Diligence, major advantages are achieved by comparison with manual filing systems, since a database enables the user to generate reports containing the summarised specific information on certain objects of interest to the user. The use of databases will also simplify the dissemination of information, thereby making the management of intellectual property rights more efficient in the long term.

Mikael Pawlo*
Efficiency, Innovation, and Transparency – The Future of Intellectual Property Rights

– *Why are they after me?*

> In the movie Antitrust, Tim Robbins, with his usual excellence, plays the part of the Bill Gates character. When the Robbins character blurts out his desperation it is because the US Department of Justice is on his tail, exploring the innermost secret of the code in Robbins' computer programs. In one of the crucial scenes where Robbins' character eventually loses control over his code, Robbins still cannot understand why his protégé Ryan Phillippe's character is working against him. After all, the code is mine, Robbins' character concludes. Should not Robbins as the copyright proprietor be able to decide just what to do with his computer programs? Should not the legislator protect the Robbinses of our world from the efforts of self-appointed Phillippe freedom fighters to release and reveal the Robbins code to the world? Only to a certain point.

1 Experimental copyright in action

The number one full-scale experiment on intellectual property in history is now in practice. I am referring to the new types of licenses for computer programs: free software and open source. We are looking at an experiment that will define the future of intellectual property.

Free software, as defined by Richard M Stallman, rests on four foundations:

- You are free to run the program, for any purpose.
- You are free to modify the program to suit your needs. (To make this freedom effective in practice, you must have access to the source code, since making changes in a

---

* *Mikael Pawlo* is an associate with the Stockholm office of the law firm Lindahl where he specialises in IT law, commercial law, and intellectual property law. Among other things, he has been chairman of the Swedish professional organisation of on-line vendors of contents and services (BitoS). He is also the Swedish editor of the Nordic Intellectual Property Review (NIR).

program without having the source code is exceedingly difficult.)

- You are free to redistribute copies, either gratis or for a fee.
- You are free to distribute modified versions of the program, so that the community can benefit from your improvements.

Free software is very simple in its construction. It uses the provisions of copyright law whereby the author has an exclusive economic right in his work. In copyright law, computer programs are regarded as literary works. Thus, the author of a computer program can enter into any agreement regarding his work. One such agreement is the GNU GPL. GNU GPL stands for GNU General Public License, while GNU is a "recursive" abbreviation of Gnu's Not Unix. GNU is the manifestation in practice of free software and Richard M Stallman's attempt at building a free Unix system. The most famous part of the GNU system is the kernel developed by Linus Torvalds under the name Linux. The GNU GPL that lays the foundation of free software is enforceable both under the principle of freedom of contract and through copyright law. According to Stallman's legal counsel, Professor Eben, the GNU GPL has yet to be successfully challenged. As I write this, in the spring of 2002, in a decision handed down in Boston, US District Judge Patti B. Saris has ruled on the preliminary injunction motion in MySQL AB vs. Progress Software Corp. That case is often referred to as the first test in court of the GNU GPL. It is a complicated case with several components. In the matter of Progress's distribution rights under GNU GPL, Saris did not grant an injunction. In the public hearing, Judge Saris made clear that she sees the GNU GPL as an enforceable and binding license, but that as long as Progress Software appears to be presently in compliance with the GNU GPL, there is probably no irreparable harm being caused to MySQL AB, and therefore no case for a preliminary injunction.

Open source is different from free software. Open source is based on a definition designed by Eric S Raymond and Bruce Perens. The basic idea behind open source is simple: when programmers can read, redistribute, and modify the source code for a piece of software, the software evolves. People improve it, people adapt it, and people fix bugs. And this can happen at a speed that, if one is used to the slow pace of conventional software development, seems astonishing. Raymond and Perens designed the open source definition. Open source is less restrictive than GNU GPL and free software, but it does not just mean ac-

cess to the source code. Open source is not a license, but a set of rules that any license claiming to be open source must follow. The most important clause in the open source definition requires the distribution terms of open-source software to comply with the following criteria:

"The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost – preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed".

The Open Source Definition is described as a bill of rights for the computer user. It is not a developed philosophy like free software, but maintains a more pragmatic hands-on approach.

It is often said that Rome gave civilisation the law. That may be true, but someone else invented intellectual property law. According to Stewart – an acclaimed scholar on international copyright law – the early Greeks and Romans had a developed notion of authorship, which was confined to the desire of teachers and philosophers to be credited for their own teachings. This was a moral question, thus not regulated in law.

Most people agree that the first copyright law was the English Statute of Anne passed in 1709. The system used today in most Western societies derives from the Berne Convention of 1886. Some things have changed over time, but only in favour of stronger protection of the author and the copyright holder. The one common principle is simple and almost globally applicable: with few exceptions, you need the copyright holder's permission if you want to make new copies or create a work deriving from the author's work within seventy years of the author's death.

2 Freedom of speech challenged

The Romans took a broad view of contract law and other essentials of civil law. Details may vary over time and between jurisdictions, but there is little controversy about the basics. Copyright, however, is widely debated these days. American scholars

Lawrence Lessig, Jessica Litman and Siva Vaidhyanathan produced the most famous recent works in the area, following a long European tradition of debating the author's rights. You may think that the time for copyright protection – life plus seventy – is too long. You may think that fair use is too limited. You may think that the Russian programmer Dimitry Sklyarov should never have been prosecuted under the DMCA (the Digital Millennium Copyright Act) for designing an anti-circumvention device for e-books. You may think all these things, and Lessig, Litman and Vaidhyanathan very eloquently put them all, but I think the issue of copyright protection of computer programs – of code – is different in principle. In his book "Code and other laws of cyberspace" Lessig has demonstrated that code, i.e. programmed functions of computer systems, can be more important than law.[1] Computer programs should never have been protected as literary works in the first place. That just happened. But now that it is time for a change, I think the great experiment that we are all taking part in is a wonderful way – through freedom of contract – to experiment towards a new legal take on code.

Free software and open source could together be described as open code. With open code, I mean that the source code is available to the user and the development of the computer program is decentralised. It is often argued from the experience of Linux, Apache and Sendmail that the distributed development process of open code is good for security, speed of development and interoperability.

Lessig argues in his book "Code" that code could be more important than law, when it comes to free speech in computer networks. Lessig concurs that we should think about the architecture of cyberspace – its "code" – as a kind of regulator; that this regulator is likely to regulate more than law does today; that "doing nothing" is to lose some of the freedom the Internet now guarantees. The code – by not being transparent – may threaten freedom of speech. What if the code in itself makes certain types of expression void? Freedom of speech would then be stifled through the architecture of the online, Internet or IT environment. And this could happen without any political debate.

Furthermore, open code is good for consumer and customer confidence and trust. Would you trust a product that you are not allowed to disassemble? What if the product carried all your personal data? The trust and transparency argument is in my opinion the strongest argument for open code legislation.

---

[1] Lawrence Lessig, *Code: And Other Laws Of Cyberspace*, New York: Basic Books 1999.

3 Open code legislation

One of the big issues of free software during 2001 was whether Richard M Stallman was for or against a codified GNU GPL. Hence, did Stallman – the father of free software – propagate a law to support his beliefs?

Tim O'Reilly tried to press the issue in a couple of articles and seemed convinced that Stallman and his colleague Bradley M Kuhn were for GNU GPL legislation. O'Reilly suggested a system where developers themselves choose the rules under which they release software, not very much different from the system in effect today. Eric S Raymond wrote a satire to prove how wrong Stallman and Kuhn would be to suggest a GNU GPL law. Raymond posed Stallman and Kuhn the question whether they would get a law passed making proprietary licenses illegal if they could. Stallman and Kuhn leaned slightly towards the legislative point of view, but never gave a straight answer whether they were for or against a codified GNU GPL. Stallman and Kuhn wrote: "We believe, though, that with time, as more and more users realize that code is law, and come to feel that they too deserve freedom, they will see the importance of the freedoms we stand for – just as more and more users have come to appreciate the practical value of the free software we have developed."

As stated above, copyright law is often questioned. In an article in Wired 1994, John Perry Barlow wrote that copyright was not designed to protect ideas or bits of information but only to protect ideas as expressed in fixed form. Hence, according to Barlow copyright is dead in the digital age.

Copyright was made to create an incentive for authors and scientists to create and explore and give them a guarantee that they would profit from their creations. A copyright system that is too strict in favour of the authors will work as a hinder and not an incentive for creativity. In the epilogue of his book Copyrights and copywrongs Siva Vaidhyanathan states that "a looser copyright system would produce more James Bond books, not fewer. Some might be excellent. Other might be crappy. Publishers and readers could sort out the difference for themselves. The law need not to skew the balance as it has."[2]

[2] Siva Vaidhyanathan, *Copyrights and Copywrongs*, New York: New York University Press 2001.

4 “Lagom” copyright for computer programs

In Sweden we have one word that I have yet to find anywhere else. The word is “lagom” and it defines the space between too much and too little. Lagom could be translated into “moderate” or “just right”, it is the situation where the glass is not half-full or half-empty – it is lagom filled. We need “lagom” copyright for computer programs because computer programs are written incrementally. That means that it is important to be able to reuse previously written code. Hence, you need to be able to write the computer program without the original author being present in your project. The aforesaid is a strong argument for a codified GNU GPL, since one of the cornerstones of GNU GPL is the right to reuse previously written code. Further, examination of the code is important for interoperability. Interoperability means that computer programs should contain interchangeability, one should be able to substitute one computer program for another, and connectability, that is the ability of one computer program to function with another.

The European debate on interoperability ended in 1991, when the European Union introduced a directive on the Legal Protection of Computer Programs. The directive exempts ideas underlying any element of a computer program, including its interfaces, from copyright protection. It also specifically permits disassembly of computer programs in order to achieve interoperability. Transparency is therefore ensured, but without access to the source code of the computer program it would still be hard to disassemble and interpret the functions of the computer programs. The GNU GPL wants to solve this by always forcing the developer to disclose and distribute his software.

Would not a modern democratic society benefit from a plurality of irreconcilable and incompatible doctrines? We need the GNU GPL, but we also need proprietary software and open source software. That would make the case for GNU GPL legislation void. However, as Lawrence Lessig concludes in his book Code, the code may in itself work against plurality. If we choose to believe Lessig we might want to reconsider regarding computer programs in the same way as literature.

In his book “The Future of Ideas” Lessig suggests a reform of software copyright law forcing computer programmers to disclose their source code when the copyright expires.[3] Lessig would protect computer programs for a term of five years, re-

[3] Lawrence Lessig, *The Future of Ideas*, New York: Random House 2001.

newable once. Copyright protection would in Lessig's proposal only be granted if the author put a copy of the source code in escrow. The source code should be disclosed to each and everyone when the copyright expires, perhaps through a server with the U.S. Copyright Office.

That much said, Lessig is very reluctant to make open code a law. In The Future of Ideas, Lessig states that the government should "encourage" the development of open code. Such "encouragement" should not be coercive. According to Lessig there is no reason to ban or punish proprietary providers. But this view is hardly consistent with Lessig's view on the future of software copyright law. In Lessig's future system proprietary providers are severely punished. They lose about 100 years' protection, which is life of the author plus seventy years compared to five plus five years and then full disclosure. Lessig's system is very similar to WIPO's proposed system of 1970 where copyright protection should be traded for putting the source code in escrow. However, the European development of copyright seems to have been founded on two principles:

1. more copyright (stronger IP laws) is good,
2. everyone should think 1, if only through harmonization.

Lessig's ideas are not new from a European perspective, but they have revitalized the European copyright debate. In Europe, the debate over the copyright system has not been as intense as the US debate in the recent years. This is probably because the European debate over copyright has been ongoing for the past century and the US debate is quite new. The focus of the European debate on intellectual property development concerns patents on life and software. The European patent system is influenced by the US patent system and more things can be patented in practice than the legislator intended. This creates an interesting situation where the strong European copyright is exported to the US and the strong US patent system is imported, thus creating stronger intellectual property rights in both the US and Europe respectively. The strong US patent was a consequence of the relatively weak copyright protection. Therefore the new legislation creates a situation where the intellectual property protection of computer programs is stronger than ever. But is it good for innovation, and how will it affect the society's need of transparency?

In an article published in the Stanford Technology Law Review, Mathias Strasser argues that any move towards more open code would be highly undesirable from societal point of view, as it would destroy the market-based incentive structure that cur-

rently encourages software producers to develop code that consumers find attractive. By applying the utilitarian incentive theory and the Lockean labour-desert theory[4], Strasser tries to explain why the current copyright system is the best.

Stallman and Moglen have yet to convince me that the GNU GPL and free software philosophy is the final answer to intellectual property protection of computer programs. However, I am not convinced that neither Strasser nor Lessig is right in their view of the software copyright. But I choose to believe Lessig when he states that code is law. The two fundamental principles of European copyright development do not address this issue. The code layer in the networks may in my opinion affect the freedom of speech at large. I do not think that copyright is dead in the sense Barlow told us in 1994. Copyright is still around, and even if it's not effective in the digital age – as observed by Barlow – the courts enforce copyright. Therefore, we need to find a new way to deal with copyright protection of computer programs. The U.S. Digital Millennium Copyright Act, the Infosoc EU directive (2001/29/EC) and prohibition on reversed engineering is not the right way to develop copyright. We need more transparency, but still we need to consider the points raised by Mathias Strasser and Tim O'Reilly. It is important that the incentives for larger businesses remain even if the code is more open through a change in the copyright law. If such a change is made, we need to consider the unique characteristics of computer programs. We should not continue to compare computer programs to literary works. Books are not software.

What we need is balance. What we need is "lagom" copyright protection for computer programs. I guess you should take the main parts of the current patent and copyright system and catalyse these systems into the new "lagom" copyright directive. We need to start thinking about these issues soon if we're not aiming to keep our grandchildren stuck with the current system for life.

5 Music and the threat of efficiency

In the past, legislators have designated a private sphere in the life of each individual as unregulated. In your private sphere, you

[4] According to the labour-desert theory, natural resources were given to people by God and title may be lost or abandoned, but anyone might gain title to anything, even resources held in common, if one used labour to convert the natural resources into something useful.

could do many things, as long as they concerned only yourself and maybe some friends. The private sphere was considered your home. You could exercise your fair use rights to copy music and papers for personal or academic use. The Internet tampers with this ancient tradition.

Your means of communication are much more efficient than legislators could have foreseen when the copyright statutes were designed. Making a copy of something for your friends is completely different in the Internet age. You can send the copy to a thousand of your friends with very little effort at a very low cost. It is extremely efficient.

Legislators did not want to regulate the private sphere and did not recognise a need for doing so. Ten years ago, when the Swedish Copyright Act was revised, this was still the position held by the legislators. They were aware of the common practice among friends of copying and distributing mix tapes of favourite songs. Swedish legislators reasoned that it was not a good thing to try to regulate the private sphere, since the legislation would be very hard to enforce. In regulation, one should try to refrain from creating rules that cannot be enforced, since they erode the populace's confidence and trust in the law as something logical and beneficial to society.

But the digitalisation of copyright and the Internet have made it much easier to obtain control over and monitor copyright violation, even if such activities are conducted in the private sphere.

In the mix tape example, there was a physical barrier preventing the communication from reaching efficiency, since distributing the tapes en masse would be prohibitively expensive. When Xerox introduced the copier in 1959, several smaller printing houses were forced to close. In 1966, Xerox introduced the Telecopier (now known as the fax machine). Xerox made copying possible over the physical barrier of distance, but it was still possible to make money on printed works. The improved means of communication and distribution of information represented by the copier and fax machine did not put all journalists and writers out of work, and neither machine was prohibited. Still, it looks like the musical equivalent of these Xerox machines – Napster and its followers – will be prohibited or at least sued out of business. Some intermediaries will die because of the new technology, just like the smaller printing houses died out when the copier was invented. But is this really an argument for prohibiting technical progress as such?

So, what is the proper balance between the music industry's wishes and the sanctity of your personal sphere? How efficiently

will copyright holders and record companies allow us to communicate with each other?

6 Compulsory licensing

For the record, I do not think that music should be free as in free beer. But I do think we need compulsory licensing to stimulate creativity and innovation. Music would then be free as in free speech (but that is another story). It is important that the legislators – and the courts – give users the freedom and the right to a private sphere. Even though enforcement and control of the private sphere could increase with new technology, I do not want record companies and Microsoft to become a private alternative to the Orwellian surveillance state. Stay away from my hard drive. Please. And let me communicate in the most sophisticated and efficient way available, even if it means that you risk losing money from my possible contributory or direct copyright infringement.

To ensure that the record companies still obtain revenues, it is important that the developers in the post-Napster era create commercial alternatives to the user-driven free beer networks. With the right commercial package, I am certain that record companies and artists can find a future in the post-Napster era without monitoring everything in the private sphere. After all, the fact that the record companies would stay away from my hard drive wouldn't mean that they waive all rights to digital music.

7 The future of intellectual property

Communication is important, and no matter what your favourite lobbyist and favourite lawyer tell you, technical progress and innovation should not be sacrificed on the altar of copyright. We need a balance between users and authors where Tim Robbins' character in Antitrust has good incentives to innovate, but where society at large is not too restricted due to Robbins' previous innovations. We also need a copyright commons where innovators may innovate and create without having to call their lawyer before they strike a chord on the guitar.

All this may sound easy to agree upon in theory, but in practice these propositions raise a lot of important questions. What should you do with current intellectual property proprietors? How will you keep incentives for very costly types of innova-

tions, like drugs, computer programs and big screen movies? In theory, it is easy to stifle innovation through limiting copyright protection, regardless of area. In practice, it is more complicated as the case for “lagom” copyright illustrates.

The conversation continues.

Lena Olsen*

Children and Internet Trade

1 Introduction

When children surf the Internet they often visit web sites belonging to big companies with a profile directed towards children. There they enjoy games or other interactive activities. Other web sites could also be of interest, depending on the age and the particular interests of the child concerned.

However, there are many concerns as to what children meet "out there" in cyber space. Thus, children's safety has been addressed, not only in the Swedish governmental report SOU 1999:106 ("The Consumers and IT"), which has not yet led to legislation, but also in soft law created by the Nordic Consumer Ombudsmen and the International Chamber of Commerce (ICC). The protection of children in relation to their use of IT has also attracted the interest of the European Union, which has addressed these matters mainly through soft law. It might be of interest to take a general look, through the medium of this soft law, at the IT problems which children encounter, but also at some of the possible solutions.

A number of issues appear as possible dangers to children. One first issue concerns the movement as such of children on the Internet. The problems include such questions as whether children should be allowed to access the web in the first place, and what role their parents should play. A second issue is whether children should only be protected from advertising which targets them or whether there should be some sort of protection in other situations as well. This in turn begs two more questions, *viz* at what age such protection should be afforded and, secondly, the relevant level of the protection planned or afforded. A third issue concerns the child's conclusion of contract and a fourth issue, finally, concerns various privacy aspects.

Before going any further into these issues, let us briefly review the general arguments in connection with children. Perhaps

---

* *Lena Olsen* is associate professor and lecturer in private law at the Faculty of Law, Uppsala University. Her publications include works on liquidated damages, remedies for breach of contract and a number of consumer related topics. She is also director for the research program "Children as active parties".

the prime source on this subject is the UN Convention on the Rights of the Child (UNCRC, in the following "the Child Convention"), passed in 1989. That convention includes a number of important rules such as the principle of non-discrimination, the best interests of the child, and participation of children in different decisions affecting them. The convention also includes a number of political and social rights. There appear to be no rules directly relating to children as consumers. The existence of the Child Convention also raises questions about the child itself and its relationship with its parents.

2 General remarks on the child and its relationship with its parents

As has already been remarked, the protection of children includes a number of issues. The first question that could be discussed is who the relevant child is. This depends on the legislation in question. Article 1 of the Child Convention refers to "every human being below the age of eighteen unless under the law applicable to the child, majority is attained earlier". The age of 18 also applies under Swedish law, although a child of 16 may dispose freely of his/her income from employment.

Hopefully, however, children do not stand alone. The Child Convention requires the parents have to take care of the child in accordance with the principle of the child's best interests. This means that the parents have the main responsibility for the upbringing of the child, taking into consideration the child's age, maturity and development. Step by step the child should be prepared for adult life through decision-making and respect for its views. In this connection mention should also be made of Article 12 of the Child Convention, concerning the right of the child to be heard. That provision is considered to include a general requirement as to children's rights to influence and responsibility.

One problem of fundamental importance facing the legislator or rule maker is to what extent parents should be responsible for rulemaking and the protection of children. One extreme view is not to regulate these questions at all but to leave everything to the parents. Another is to put the whole protection of the child in legislation or soft law. Normally the solutions actually adopted will be somewhere in between, but it is important to recognise the scale, and there are differences. Thus, in Swedish law children may not conclude any contract before the age of 16 without

parental (or equivalent) consent. In other countries children may conclude necessary contracts.

Another problem related to the child/parent relationship is the picture of the parents in advertising material of different kinds. This problem has also appeared in relation to TV-advertising and Article 16 of the Television-without-Frontiers Directive[1] thus provides that, as the aim of the rule is that TV advertising should not cause moral or physical detriment to minors, it should not encourage minors to nag parents or others, nor should it exploit the special trust between parents and children. In the soft law regarding children and the Internet, this is not found to be a great problem as yet. However, there are rules to prevent traders in their relation with the child from undermining the relationship and the trust between child and parent. In this connection it might be worth mentioning Article 29 paragraph 1c/ of the Child Convention, which lays down that education should be directed to the development of respect for the child's parents, although this provision refers to education through the public sector school system.

3 The movements of the child on the Internet

There are no signs in the different sets of rules that children should be stopped totally from accessing the web. This is in conformity with the Child Convention, as it expressly provides for a freedom of expression which includes freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice (Article 13). However, there are certainly dangers connected with the child's surfing the web. The Child convention does provide for some restrictions in the right of the child to gain information, i.e. for the respect of the rights or reputation of others or for the protection of national security, public order or public health or morals. This should include restrictions in relation to children's possibilities to reach the sites of pornographic traders. The relationship between the child and mass media is also dealt with in the Child Convention Article 17, although in a weaker form. Thus the child should be protected from information and material injuries to his or her

[1] Council directive (89/552/EEC) of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of Television broadcasting activities.

well-being through guidelines. Such restrictions are also in conformity with the general ambition within the European Union to create confidence towards the net.

One important issue in this regard is the role of the parents. The duty of upbringing includes helping the child to develop its capacity to take part in matters of society. In the relevant soft law the view of the parents' duties varies considerably, and this also affects the duties of the trader. Thus it could be considered a parental duty to sit beside the child in front of the computer. In such a case it might be considered the trader's duty to encourage the parents to do so, which raises questions as to what the traders are obliged to do in order to achieve this. Another view of the parents' role is that they should in other ways take care to ensure that the child does not meet dangerous material while surfing the web. In such a situation the duty of the trader could be to help the parents by means of appropriate hardware or software. A third possibility is to regard the parents as not present at all, which is probably the commonest situation, as many parents still do not have the knowledge to interfere. In such a case, the relevant duty on the side of the trader should be to act in such a way that children are not harmed. It is obvious that the duties of the traders are considerably lower with a competent adult on the other side than with only a child as their opposite number.

4 The protection of children surfing the commercial parts of the Internet

Of fundamental importance for children is the definition of the advertising target group, i.e. whether the target group includes children or exclusively consists of children. There are not many items of legislation in Swedish law concerning the protection of children in connection with marketing, but there is a ban on television advertising directed at children under twelve, and there is an interesting case to illustrate the effects of it.[2] A decision of the Swedish Market Court (MD 2001:5), concerned a television advertisement for the Walt Disney version of Cinderella. The trailer consisted of sequences from the animated film and pictures of children apparently enjoying the movie. The speaker voice, however, used words which were not regarded as particularly directed towards children. Furthermore, the trailer was transmitted at four times which were not believed to be peak viewing hours

[2] Radio- och TV-lag (1996:844) Chap. 7 § 4.

for children, and in connection with programmes having adults as their presumed primary audience. The relevant times were 15.10, 21.00, 19.30 and 15.35. The advertisements were not considered by the majority to be directed at children and were therefore not covered by the Swedish prohibition of marketing directed towards children. Another case of the Market Court could be mentioned in contrast, namely MD 1981:5, which concerned a whole-page picture in Sweden's biggest morning paper of a child about 10-12 years old eating a hamburger, with a text about unappetising school lunches. The advertising came next to the editorial page, where nothing else of general interest for children is to be found, but the court found that the advertising generally could reach children as well, and this influenced its reasoning. The cases illustrate the difficulties in relation to mixed messages. Legislation that only covers advertisements specifically directed towards children may be a waste of effort.

However, there are also other methods to solve the problems connected with mixed messages. One way is to provide for a minimum protection that all advertising should live up to. Another approach is to require that advertising should be adapted only to one target group. In that case there will be no mixed messages and it is possible to have special requirements for advertising directed towards children. A third approach might be to combine these methods.

All these methods have been used in the relevant soft law to protect children from dangerous material within the commercial parts of the web. Such dangers could involve pornography or violence and could appear in pictures and texts in advertising as well as being a part of products and services of different kinds. A minimum level of protection for children could be to recommend that advertising should not contain any element which might result in harm to children or cause moral, mental or physical detriment to children. A similar solution is also used in connection with television. Thus, Article 22 of the Television-without frontiers directive prohibits TV-programmes which might seriously impair the physical, mental or moral development of minors. Such minimum rules are also used in the different items of soft law. The other solution, i.e. ensuring that advertising is not construed in a mixed form, appears to be used, although in a less clear-cut form. What is required is that the advertising should be adapted to the relevant target group. However, in my view achieving such a goal must be an almost impossible task.

There are also interesting differences as to how the different items of soft law describe the duties of the trader. Such duties could be ascribed the trader or the commercial communication as

such (cf. “code subscriber may not...” with “codes should…”). Furthermore, the duties could be described as a positive obligation, (e.g. to encourage young children…), or as a prohibition or something similar (e.g. children should not be tempted… or do not encourage…). The rules could be comparatively precise (e.g. entertainment should not be combined with or punctuated by advertising messages) or very imprecise (e.g. do not encourage children to buy a product by exploiting their sense of loyalty). Even a comparatively precise positive obligation could constitute a weak safeguard for children if the trader’s only duty is to identify material intended for adults only, if it is not also required that such material should be clearly separated from material intended for children or young persons.

In this connection it is also important to mention the risk of the trader having links to unsuitable material from his web site. This is particularly dangerous when the web site is directed towards young persons. But in other situations too, such links could be highly inappropriate. One way to regulate this is perhaps to consider such a link as an encouragement to enter such pages. However, it is still debatable whether a mere link is sufficient proof of encouragement.

Protection could be more difficult to achieve when pornography or violence is used as a marketing device for other products, considering that such means could be quite effective marketing in relation to teenage boys. However, this is more of a general marketing problem and is preferably solved by such rules. Generally, according to Swedish law, it is required that marketing, also in relation to children, is of good standard and does not exploit children’s or young persons’ natural credulity or inexperience. Even children’s illusions are protected in one of the soft law systems. Generally, there is also a requirement that advertising should be clearly identifiable as such, which could involve a difficulty in connection with the construction of a web site. What is advertising and what is general information about the company? It is not acceptable for games or other forms of entertainment to be interrupted by advertising messages.

5 Children’s conclusion of contracts

National legal system generally develop forms to keep children from concluding contracts they are not allowed to conclude. However, as we have now seen, the national rules as to the capacity of children vary considerably. It might also be difficult to

ascertain which legal system should be applied. Thus general EC rules concerning legal signatures are one measure which also protects children.[3] However, these are still at the implementing stage and it is still impossible to evaluate the result. By comparison with the present situation it could involve an important change for the better. Another measure to protect children is to have the same soft law regulating the problem. In the soft law discussed there are suggestions that traders should not accept orders from minors without the explicit and verifiable consent of the parents/guardians. This might in my opinion be going too far even if it perhaps may be justified through the particular dangers to children which Internet contracting entails. However, it is a good solution for those countries where children are hardly allowed to conclude any contracts at all without their parents' consent. It might also be a good solution as a precaution to ensure that children do not pretend to be someone else, which might be an important problem, given the anonymity of Internet.

So far we have been dealing with the situation when a contract is about to be concluded. But another interesting point is how the child reaches that point. Not seldom it has been encouraged to do so by marketing. This matter is also dealt with in the relevant soft law, although in varying ways. Generally, minors should not be encouraged to buy, and, more specifically, should not be encouraged to conclude a contract of credit. It is unclear what kind of encouragement is covered by such provisions. Probably their main target is web sites aimed at children and including special offers or using hidden techniques as an inducement for children to buy or to conclude other contracts.

6 Privacy aspects

The privacy of the child or the family as a whole could be endangered if the child is lured into providing the trader with information of different kinds as to the habits of the family, who does the shopping and so on. Dangers in relation to privacy are recognised, for example, in Article 8 of the European Convention on Human Rights, and they have also been realised in the different items of soft law. Thus traders are recommended not to encourage children or young persons to give information about themselves, the household or any other person. It is also recommended that the provision of information should not be made a

[3] Directive 1999/93/EC on a Community framework for electronic signatures.

condition for gaining access to certain content. However, also on this point there are different views as to the role of the parents. Thus traders recommend that the parental consent should be obtained and that the relevant traders should take reasonable steps to ensure this. However, there seems little point in any such requirement if no particular proof of consent is necessary.

7 Conclusions

A number of conclusions may be drawn. First, the Child Convention is an interesting piece of legislation, even though it does not expressly deal with the consumer market at all. The provisions concerning the best interests of the child, the right to be heard, freedom of expression and the right to information may specifically be mentioned in this regard. Secondly, the Internet may to some extent be compared with television, and the problems concerning children and e-commerce have a great deal in common with the problems occurring in connection with television advertising. One such problem is connected with mixed messages, and on this point it is important to continue discussing the best ways of protecting children while also giving them a fair opportunity of searching for information on subjects that interest them. However, there are also differences compared with television advertising, in particular the mobility of the child in different spheres of the web, interactivity, and the particularly anonymous situation of the child, together with the possibilities of concluding contracts on the web. This problem also appears to have been the most difficult one on which to achieve general agreement. Another problem generally connected with the Internet is the disappearance of geographical boundaries. However, such problems generally affect only older children, due to the language difficulties. One measure in this regard is probably the use of such items of soft law as have been discussed above. However, in my view we are only at the beginning of development in this respect. Many problems for children on the Internet could be eased through different technical measures. It is also important that at least some level of common agreement be reached, for example, as to the role of the parents. It thus remains to be seen what problems remain or will be added in the future versions of the soft law produced by the Nordic Consumer Agencies, ICC and the European guidelines.

Gustaf Johnssén*
Bits or Balloons? The Need to Rethink Tax Concepts and Principles on the Internet

> Those who will benefit least from this new invention will be the tax-collectors, who henceforth will never be able to prevent the passage of contraband. The walls of our towns will prove no obstacle, and it will require an army of officials to walk round the districts, day and night, to inspect newly-arrived machines.[1]

1 Introduction

The above comment was made in 1784 following the invention of hot air balloons. But air balloons, boats, cars or aeroplanes, were not destined to fundamentally challenge the tax system, which today is fundamentally the same as it was in 1784.

The impact on the tax system of electronic commerce and other uses of information and communication technologies is not likely to be less significant than that of air balloons. Nonetheless there seems to be little doubt among tax authorities and tax lawyers that the new forms of commerce can be dealt with within the current tax system. Most seem to have full confidence in the system itself.

As I see it, the tax system will be confronted with major challenges in the not too distant future. The economy consists to a growing extent of transactions in digital networks, whereas the tax system is still founded on manufacturing and distribution of physical products. In this paper, I will make some comments on the tax system of today and its chances of survival in the digital economy.[2] I will argue that in order to provide for a smooth-

---

* *Gustaf Johnssén* is an adviser at the Swedish Agency for Public Management (Statskontoret), working primarily with ICT and administrative reform. He has also served at the ICT Commission and at the Ministry of Justice.

1 *Lettre à M. De Saint-Just sur le globe aérostatique de M.M. Montgolfier, Paris 1784*, quote from The Romance of ballooning: The Story of the Early Aeronauts, New York: The Viking Press 1971, p. 53.

2 Below manufacturing and transactions of information in digital networks will be labelled e-commerce for short.

running tax system, it is necessary to rethink some of the fundamental assumptions underlying the tax system.

The basis of my discussion will be the general debate on taxation of electronic commerce, which has been going on for several years among legislators, practitioners and academics. I will outline some problems that have been identified in the debate: enforcement, classification, and localisation problems. I will then offer some concluding remarks concerning the lines along which further work in this area could be carried out.

The IT Law Observatory has issued two reports concerning taxation, one dealing with VAT, and one dealing with general matters. This paper is to some extent founded on both reports.[3]

2 Enforcement problems

There are considerable problems for tax enforcers in the digital environment. The possibilities of hiding transactions are vast and the possibilities of identifying parties to a transaction are in many cases virtually non-existent. The opportunities for tax evasion seem endless.

The debate so far has been mainly concerned with enforcement problems. The general opinion seems to be that existing tax rules are applicable and should be applied in a digital environment. The problems caused by new forms of communication are not seen as new problems, only as bigger ones. From this perspective, problems with control and enforcement outweigh more fundamental problems.

Discouraging as the enforcement problems may be to tax authorities worldwide, it is my conviction that these problems are trivial compared to the more fundamental problems concerning the basic concepts and principles of today's tax system.

3 Classification problems

The problem of classifying digital products has been a subject of attention for several decades, and has become more important with the arrival of e-commerce.

---

[3] Philip Hallenborg, *Elektronisk handel och indirekt skatt* (IT Law Observatory Report 14/2000), Gustaf Johnssén, *e-skatt? i-skatt? o-skatt?* (IT Law Observatory Report 18/2000). References to sources and further reading relevant to this paper can be found in the latter report.

In taxation, it is often necessary to classify a transaction or the object of a transaction. Transactions are classified, for example, as income from employment or from royalties, and the objects of the transactions are classified, e.g. as products or services. I will focus here on the classification of products and services.

Traditionally, distribution of information has depended on the distribution of the media. When the information has been fixed, e.g. on a CD, the information has been distributed in fixed form. These transactions have traditionally been taxed as transactions in goods, without regard to the fact that the actual object of the transaction is the information contained in the physical product. In these cases the information product is an object that exists and can be observed in the physical world.

The classification problems connected to e-commerce are primarily related to the principle of neutrality. An information product, e.g. a music album, can be delivered either physically, in the form of a record, or digitally. According to current tax law, the same information product will be taxed differently depending on how it is delivered. It is hard to find a way to classify information deliveries within the framework of current tax law, which at the same time satisfies fundamental taxation principles and considers the characteristics of information.

Classification problems occurred in the traditional physical environment. As long as information was distributed mainly in physical form, these problems were of little importance. As production and distribution move out into the networks, the problems grow more pressing. In the end, the neutrality problem may seriously endanger the legitimacy of the tax system. The dominant view among the tax subjects is or will be that the two forms of delivery are just that: different forms of delivery of the same product. The law, which treats them as different products, will then seem out of touch with the real world.

These problems may to some extent be problems of terminology. But underlying them are more fundamental assumptions of tax law. These assumptions are deeply rooted in the history of tax law and its connection to trade in goods. The discussion regarding classification can contribute to the discussion of information taxation mainly by highlighting the fact that products in networks are neither goods nor services in a traditional sense. Information simply does not fit into tax law, because tax law is rooted in the production and distribution of physical products, and not services, still less information.

This is even more evident from the discussion of localisation problems.

4 The problems of localisation

Much of the debate has concerned international taxation. In fact many argue that international issues are the only problems related to electronic commerce. A representative position could sound like this:

> The expression [Cyberspace] risks overshooting. A person, transaction, income or other fiscal fact, whether physical or digital, is situated in a country (or in two or three etc. countries, or in a country that does not impose tax), not in some extraterrestrial realm. As a tax concept the expression can only highlight the jurisdictional problem of determining in which specific country or countries electronic commerce and its players are situated and how much profit must be allocated to that country. [4]

In my view, this is a flawed approach.

Several taxation concepts relate to the physical or geographical location of a person, a company, or a transaction. This is due to the fact that taxes are national. It is therefore always necessary to attribute a transaction to a certain geographic location. The aim is always that the creation of value should be taxed where the value is actually created. The connection can be formal, e.g. connected to where an organisation is registered. It can also be based on where a transaction is regarded as taking place.

One instrument for allocating a transaction is the concept of permanent establishment. In one of the most influential tax documents, the OECD Model Treaty, permanent establishment is defined in the following way:

> 1. For the purposes of this Convention, the term "permanent establishment" means a fixed place of business through which the business of an enterprise is wholly or partly carried on.
> 2. The term "permanent establishment" includes especially:
> a) a place of management;
> b) a branch;
> c) an office;

[4] Luc Hinnekens, *The Challenges of Applying VAT and Income Tax Territoriality Concepts and Rules to International Electronic Commerce*, in *Intertax*, vol. 26, 1998, p. 54.

d) a factory;
e) a workshop, and
f) a mine, an oil or gas well, a quarry or any other place of extraction of natural resources.

The application of this provision to e-commerce is one of the main themes in the debate.

It goes without saying that the definition primarily refers to traditional manufacture of and trade in physical products. This does not mean that the provisions cannot be applied to new phenomena, but it seems far-fetched to apply it to non-physical objects. The discussion of this provision has been mainly concerned with how transactions in computer networks can be connected to physical objects and thereby to states where those objects are located. This calls for a method of unambiguously connecting the transactions in the networks with physical locations.

In the debate, many more or less elaborate attempts have been made to find a connection between physical and logical infrastructure. In these attempts it often seems as if the networks are perceived merely as the means of delivery. Information is treated as if it were transported through the networks. One is looking for information factories and information shops in the networks. The server is seen as an information-tap, where information flowing through the network can be drawn off.

In some sense this is correct, since the information is in fact transmitted from one physical point to another through the physical network in the form of electromagnetic impulses. The problem is that this view sees distribution of information as distribution of physical goods.

In the case of physical distribution, an object is transported by physical persons and delivered to other physical persons. The transactions comprise distinct physical components: the object, the persons involved, and the place where the transaction takes place. The relations between the object, the persons and the place are self-evident and uncomplicated. The reason for this is that the transaction involves distinct, physical phenomena, such as human beings.

In e-commerce the relations between the parties involved are less clear. The physical infrastructure, computers and cables, is as tangible as the physical infrastructure for distribution of goods. The information “is” in some sense in the networks, but it forms its own infrastructure, which does not follow the physical infrastructure. Information is not matter that can be pumped through the networks like oil being pumped through a pipeline. The server is not a warehouse where information is stored on a

shelf. It would be more correct to say that if information is a good, then information is the warehouse as well as the transport workers. Information is the logical infrastructure's equivalent of trains and railways, ships and the sea, balloons and the air.

One possible strategy from the enforcement point of view is to trace the transaction back to the persons and companies involved, thereby bypassing the several middlemen and ambiguous constellations. The problem with that strategy is that it overlooks the specific character of e-commerce, that it blurs traditional structures and makes legal categories irrelevant. The risk is that the taxation will be alienated from the economic reality. You may solve one problem by finding a tax subject, but at the same time create a new one. The purpose of the international tax rules is to mirror the transaction and tax it where it takes place. By connecting taxation to traditional tax subjects, the opposite is accomplished. The parts of the transaction where value is created are bypassed.

5 Conclusion – The need for a new approach

As I have outlined, the discussion so far has been carried on mainly within the current legal framework. The main concern is how to enforce taxes in the digital environment. Some attention is given to the problems of application of traditional concepts to new phenomena. But there is hardly anyone who questions the concepts or the fundamental principles of tax law.

The problems I have outlined are of three kinds:

- Enforcement problems.
- Application problems.
- Principal problems.

The enforcement problems are obvious. These are the problems that have been most thoroughly analysed. They are also the problems most urgently needing to be solved. The application problems have also been recognised, and received their due share of attention. The principal problems, those concerning the fundamental principles and assumptions of tax law, have not been thoroughly analysed. In fact they are not recognised as problems. I have tried to show that these problems are more alarming than the problems of enforcement and the problems of application, but that they tend to be overshadowed by these more easily grasped problems.

This conservative approach may be justified from the point of view that one should not jump to conclusions. In the long run, however, it will not be tenable. The strain on traditional tax concepts will eventually result in the breakdown of the tax system. If we do not address the fundamental questions, but wait and see, we may wake up one day and find that the tax system has been so alienated from the economic and technological reality, that applying the rules is not just hard but downright impossible. The tax system will lose its legitimacy, which will benefit nobody.

Such a breakdown could be avoided if the problems are recognised as problems and included in discussions among legislators.

The questions that should be addressed include:

- Can information be a relevant category in tax law?
- If so, how can it be defined in a way that is adequate from a legal, as well as an economic, and technological perspective?
- Should traditional taxation-principles be abandoned?
- Should the tax system of the future be developed at a national or an international level?
- In what ways is the design of tax law dependent on other areas of law?

Anders R. Olsson*
Freedom of Speech and the New Media

1 Introduction

The value of free speech is like the value of freedom itself, it is independent of context – not just a legal order we find suitable for a limited number of purposes. We have no problem identifying purposes, however. A huge majority can agree that free speech is necessary for a people building democracy, for a society "*where every citizen who wants to improve the world around them and be heard on important public issues can participate in public life with freedom and the right to act on their sense of public responsibility*", as Steven Clift, founder of E-Democracy in Minnesota, exhaustively puts it.[1]

In such a society, only democratically supervised authorities – national, regional or local – are allowed to use coercion. Legal provisions safeguarding free speech, then, focus on the protection of citizens against authorities using coercion to silence or unduly influence the speech of individuals, organisations or the press. Protection for free speech is protection against the state.

If one citizen tries to limit or suppress the speech of another, this is usually dealt with through criminal law. Threatening behaviour is penalised in most settings, as are unlawful detention, theft or destruction of manuscripts, recordings, technical equipment etc – and basically all other ways of preventing someone from speaking or publishing.

That's the theory. For more than 200 years, it has served Sweden and other democratic societies well. Certainly, speech has been suppressed many times, in many places – and still is – but suppression has never become broadly accepted. Even the most benevolent state must present strong motives, and have its actions critically monitored, to be allowed to disturb the free flow of information.

---

* *Anders R. Olsson* is a freelance author and journalist who has written numerous works on issues of fundamental rights and freedoms in the IT society, among them books on e-voting and electronic democracy. He is also involved in research activities with partners such as The Swedish Institute for Computer Science (SICS).

1 From: http://www.publicus.net/articles/future.html.

I will now argue that this model for the protection of speech needs rethinking, or at least supplementing. There are two reasons for this.

One. The Internet has emerged as an important mass medium for which no nation, body or institution is responsible. Some of its qualities – being interactive and multijurisdictional – have caused much legal and political confusion. Special interest-lobbyists, not least the ones working for intellectual property-holders, have been extremely successful at the expense of ordinary citizens. (For an in-depth analysis of how and why this is happening in the US, see Jessica Litman's book Digital Copyright. Prometheus Books 2001.) If the Internet today can be characterised as "free", this describes qualities inherent in the technological design rather than a legally defined order. There is virtually nothing given about this technological structure. In fact it is continually redesigned – under pressure from security and business interests.

Two. Yesterday the largest multinational corporations could use their lobbyists, lawyers and media consultants to strongly influence the media. Today they *are* the media. Commercial and technological strategies – they can hardly be separated – of companies like AOL/Time Warner, Microsoft, Intel and Motorola, will affect the very structure and qualities of the arena where citizens are supposed to speak out and do politics.

There is nothing particularly Swedish about these issues. We have, however, a strong press freedom tradition and constitutional free speech guarantees since 1766. Swedes may therefore be particularly sensitive to emerging legal and technological structures that tend to undermine free speech guarantees. So far, though, and this may also stem from tradition, our focus has been on national legislation and protection only from the state. The internationalisation of free speech issues is rarely discussed. Therefore, a number of the references here will be to literature and conditions in the US, where societal, media-related trends often appear some time before they are visible in Europe.

2 The power of money

The problem is as old as society itself: with money comes power. In the information society, the source of power is, to a large extent, the control of information. If a company is big enough somewhere along the chain of production-distribution-sale of media-products, its decisions will undoubtedly affect how reach-

able – from a practical point of view – some speech will be and how invisible other.

In the US, the possibility of being exposed in major stores depends on whether your magazine or video production is, or looks to be, within the boundaries of "family values" – not explicitly sexy, not politically provocative, etc. Companies like Blockbuster, Wal-Mart, Kmart and most other supermarket chains in the US have, claims Naomi Klein in her book No Logo, "*a policy refusing to carry any material that could threaten their image as a retail destination for the whole family*." (p. 166)

In Sweden, the dominating media company is Bonniers. It owns not only many newspapers and magazines but also (together with Allers and Egmont, two large competitors) Tidsam, a company with a de-facto monopoly of the distribution of papers and magazines to kiosks, department stores and other important outlets. Tidsam has, not surprisingly, been heavily criticised for favouring the products of its owners over independent papers and magazines, thus refusing the latter access to the market.[2]

Then there is what Klein calls "censorship in synergy". The huge media corporations systematically exploit cultural artefacts (be it Star Wars, Pokemon or Harry Potter) from their introduction to a myriad follow-up products (films, books, computer games, collectors items, T-shirts, etc) carrying the names, logos or symbols. Furthermore, the media giants also own the papers and magazines whose journalists are supposed to report, critically and independently, on the cultural sphere where Star Wars, Pokemon and Harry Potter appear. Although many editors may try to defend the integrity of their staff, it is naive to think that a major media corporation would, in the long run, allow one company within the group to seriously criticise or otherwise hurt a "product" in which another has invested heavily.

There is also the commercially motivated political suppression of speech. Strategies applied by media companies eager to enter the Chinese market offer clear examples of this. (Klein, pp. 168-174) The commercial logic is quite clear. Why would a businessman like Rupert Murdoch risk a multibillion-dollar satellite communication contract with China by having one of his media companies doing the kind of journalism that is likely to anger Chinese leaders? Klein stresses that most of the damage is done by self-censorship – by editors and producers second-guessing, everywhere and all the time, the wishes of top executives, and in doing so having every reason to steer clear of the commercially and politically controversial.

---

[2] Johan Ehrenberg, *När ska du ta ditt ansvar?* Aftonbladet 2001-11-15.

One aggressive strategy applied by many powerful companies is harassment of critics – under the cloak of copyright and trademark protection. The continuous strengthening of intellectual property laws, aimed primarily at regulating the Internet, is, according to law professor Lawrence Lessig, a growing problem from the free speech perspective.[3]

One of his examples is the "notice and take down provision" for web sites of the US 1998 Digital Millennium Copyright Act (DMCA). Increasingly, according to Lessig, companies trying to protect themselves from criticism have used the notice-and-take-down-provision to silence critics. He tells the story of a British pharmaceutical company that got tired of complaints from an animal rights organisation. In August 2001 the company invoked the DMCA in order to force the company providing the Internet connection (the ISP) to shut down the animal-rights site. The ISP stated publicly that "It's very clear [the British company] just wants to shut them up". It had no incentive to resist the claims, however – it could be liable if in fact there was a violation – and thus closed the site. (Lessig also tells the story in Foreign Affairs, November-December-issue 2001, but chooses, both in the magazine article and in the interview, not to name the British pharmaceutical company.)

Sweden has an Electronic Bulletin Boards Liability Act (1998:112) with similar provisions. So far, there has been no report of efforts to use it to silence critics, but as long as an ISP can be made responsible for what customers publish, the risk is obviously there.

3 Free speech and privacy

In "Code and Other Laws of Cyberspace", a book that has attracted much attention, Lessig stresses that the Internet is in many ways more effectively regulated by computer code than by law. Although a number of, to most people, unknown Internet organisations with names like ISOC, ICANN, IAB, IETF and W3C work – or so they claim – to promote safety, openness and maximised accessibility on the net, there is no democratic structure or "constitution" for the technical development of the Internet. This development, then, takes place very much under pres-

[3] Personal interview with Lessig 2001-10-26, at Stanford University, California. He expands on the subject, and provides more practical examples, in his latest book: The Future of Ideas, New York: Random House 2001.

sure from powerful political and commercial actors who feels no responsibility for the promotion of free speech.

The issue of "free speech and Internet code" is immensely complex. It involves exercising power over speech both directly and indirectly. Indirectly in this context relates to identification as deterrent. Citizens are likely to abstain not only from speaking but from seeking/receiving/forwarding controversial information on the net if whatever they do will be registered and possibly monitored by others.

As demonstrated by Hunter, this is a problem not just for citizens with extreme or unusual convictions. Using cookies, online donation forms and political mailing lists, Internet-based campaigns can gather tremendous amounts of information about citizens' political preferences. The creation and sale of detailed voter profiles raises one of several serious questions about the future of political privacy and the democratic process.[4]

4 Filtering

Filtering is but one aspect of the broader problem of "speech regulation through code", highlighted here because it usefully demonstrates how private institutions can suppress speech.

Filtering is automatic blocking of information. It can be done at the PC level, allowing the individual Internet-user to avoid having some particularly nasty (pornographic or otherwise offensive) material downloaded. It can also, however, be done at a higher (server/router) level in a way that leaves the individual with no way of understanding or controlling the functions of the filter.

Filtering-software can operate in different ways, but today it seems unrealistic to achieve precise filtering – blocking what is intended and nothing else – without precise rating (classification) of Internet content. The questions of how to rate and who should do the rating are still unresolved among filtering supporters, but the demand for solutions is strong in both Europe and the US. The EU Commission, to mention just one important actor, has a "Safer Internet Action Plan" with a budget of 25 million euro. As one of three "action lines" it has "*Developing filtering and rating*

[4] Christopher D. Hunter, *Political Privacy and Online Politics: How E-Campaigning Threatens Voter Privacy*. http://firstmonday.org/issues/issue7_2/hunter/index.html.

systems, *facilitation of international agreement on rating systems.*" (underlined in the original).[5]

The general problem with rating is that even though a system may have been created for the most noble purposes – i.e. protecting children from hardcore-pornography – there is no way of assuring that it won't be used for others. The more precisely communicated Internet-content is classified, the easier it will be for authoritarian states (or ISP's whose owners care more about lucrative contracts with those states than free speech-principles) to filter unwanted content in servers at jurisdictional borders. It may also, in the US and Europe, be a commercially sound policy for ISP's to block, in the name of "political responsibility" or "decency", Internet-speech that is legal but offensive to a majority of customers.

5 Solutions?

In a perfect world, a sufficient majority of nations would agree on an international free speech-convention for the IT-era, with technical as well as legal provisions, and enforcement mechanisms effectively blocking attempts by both states and private sector-actors to unreasonably limit or influence citizens speech. In that world, media companies that did not safeguard the integrity of its journalists and other content-producers would see its customers turn elsewhere for fair and balanced information. Our world is far from perfect, however.

At present, we seem to have a choice between the devil and the deep blue sea.

EITHER no regulating of any importance is done on the international level to safeguard free speech, which would leave the arena open for governmental agencies, multinational corporations and resourceful special-interest groups to control or block mass media content in their own interest.

OR some kind of regulation is negotiated, where the nature of international politics is likely to cause the agreement to be, not a free-speech guarantee but rather the opposite. No international body will be able to reach consensus about free speech – except concerning trivialities – because in all nations there is some speech which is considered unacceptable. All the representatives in such negotiations will demand exceptions which are necessary in order to get the agreement approved by their parliaments or, in

[5] http://europa.eu.int/information_society/programmes/iap/index_en.htm

less democratic states, politically dominant forces. How much free speech the world needs will obviously be, at best, a secondary issue. Thus, to successfully negotiate an international free speech-agreement, it would have to contain or at least allow for restrictions on pornography, defamation, hate-speech, instigation to terrorism or other criminal acts, sharing of copyright-protected works, denying of the holocaust, communist propaganda, anti-Christianity, anti-Islam and anti-anything that some influential portion of a people consider sacred.

The devil or the deep blue sea?

I opt for the deep blue sea. My argument for an international free-speech treaty is that it would, after all, make the issues visible to ordinary citizens in many countries. As long as the problems are not discussed publicly, the actors manoeuvring to limit and control speech can fight with far fewer scruples.

Before the Napster/MP3 controversy, citizens of the US did not know they had a copyright problem. Because of the publicity, people opposing the new, strongly control-oriented copyright legislation could suddenly be heard, loud and clear. The more citizens who understand that they are stakeholders in such a conflict, the more likely that a legislative process will result in a balanced and reasonably fair law.

IF free speech is put on the international agenda – within the United Nations or elsewhere – and IF journalists manage to cover the issues, then it is more likely that a treaty will come to include at least some decent provisions. Even a thoroughly bad treaty, however, would put the issues on the table. A treaty would in itself confirm that international decision-making is necessary, and when the practical consequences of a bad treaty became apparent, it would get increasingly difficult for leaders in Europe and North America to avoid responsibility.

I'm sure that most hackers will disagree with me. They seem to instinctively oppose regulation and prefer to fight it out on a technological level, confident that they, in co-operation, will have the upper hand in an arms race against the forces of control. That may be true. Hackers will keep cutting fences in cyberspace, hack access-control systems and circumvent new, yet to be invented, technological defence mechanisms. They will more often than not be able to speak, find and share information – but the 98 per cent or so of Internet-users lacking their skills will not.

And free speech for two per cent is insufficient.

Håkan Hydén*
Self-employed – The Problem of Societal Development and Adequate Legal Concepts

1 Self or employed?

Within the IT Law Observatory, several hearings have taken place over the years discussing the phenomenon of self-employed. The main focus of these hearings has been the question of whether a separate legal institution is needed for this category of workers. From a practical point of view there are two different kinds of self-employed: those who are self-employed of their own volition and those who have self-employment more or less forced upon them. The first group consists of the strategic persons that companies want to hire. These people can choose their own jobs. The work of the other group is less central jobs that companies try to get rid of by placing a contract for them, so-called outsourcing. Most of the discussions have been about self-employed in this second case. The focus is on the need for protection of this more or less vulnerable group. An aspect which has not been discussed all that much is the relation between self-employed and the new information society. Is there a need for a legal institution covering the self-employed for the sake of stimulating the new economic structures?

We are said to be moving from a hierarchically organised society to a horizontal network-society.[1] The majority of the labour force in the advanced economies is under salaried conditions. But the diversity of the levels, the unevenness of the process, and the reversal of the trend in some cases call for a differential view of the patterns of evolution of the occupational structure. When networking and flexibility become characteristic of the new economic organisation, and as new technologies make it possible for small business to find market niches, we witness a resurgence of self-employment. The occupational profile of the information society will be far more diverse compared to the industrial society. The data show a growing proportion of the la-

---

* *Håkan Hydén* is a member of the IT Law Observatory. See presentation in Annex 1.

1 Manuel Castells, *The Rise of the Network Society*, Malden: Blackwell Publishers Ltd. 1996/2000.

bour force tending to leave salaried status in most countries between 1983 and 1993. Different data sources seem to indicate an accentuation of this trend in the late 1990s.[2] The trend was particularly intense in Italy, with approximately 30 % of the labour force, and in the UK. It appears that economies in various countries try different forms of flexibility in working arrangements, depending on their labour legislation, social security, and tax systems.

The new system is people working for themselves. In the USA 33 million people make their living as free agents today.[3] Thus, one American worker in four is already a free agent. There are different work values behind this development, such as having freedom, being authentic, i.e. doing your own job, putting yourself on the line and defining your own success. Instead of up-and-down loyalty, free agents practise a new side-to-side loyalty. Seen from an economic point of view, free agency is, in effect, a form of just-in-time staffing, where companies are hiring the exact number of people they need for a project or job. In this way the risk of ups and downs has shifted from the company to the free agent's shoulders. Balancing between the corporate need of flexibility and the workers' need of employment security will in this situation be subordinated to the joint efforts for both to gain by the construction. In this situation there is a need for legal changes and innovations. The background is the following.

2 From natural law to legal positivism

2.1 The example of juridical persons

When the industrial society in the 19th century entered a phase of large-scale production, the legal system faced a number of challenges. The need for accumulation of private capital for the growth of large companies called for an introduction in the legal system of a new kind of person. There was an interest of limited liability among the owners in order to stimulate the industrial growth. This created in the mid-19th century a tension within the legal doctrine surrounding company law.

---

2 Martin Carnoy, *Sustaining Flexibility: work, family, and society in the information Age*, Cambridge, MA: Harvard University Press 2000.

3 Daniel H. Pink, *Free Agent Nation. How America's New Independent Workers Are Transforming the Way of Life*, New York: Warner Business Books 2001.

Until that time some companies could be granted limited liability as a privilege given by the state. This system can be traced back to the East-Indian Companies in the beginning of the 17th century. Limited liability was at that time related to public law and not company law within the civil law system. The associations that existed until the mid-19th century were treated in the perspective of the legal doctrine about persons as societas, using the Roman law term. Societas expressed a relation of law of contracts among the participants. The company relation, however, constituted a community based on the law of property (communio). This transition took a long time to complete.[4] The natural law theory had to be substituted by legal positivism.

As long as persons were observed through the scheme of societas, supra-individual persons could not find their place within the legal system. The first step in the transition was to think about a company in terms of a person with its own legal capacity built on the parallel to natural persons, individuals. Companies could be seen as juridical persons. This fiction started with an acceptance of juridical persons not being a person according to the commonly known criteria of persons but still useful in order to place the phenomenon within the legal system. The process of change in legal systematising was initiated by making analogies between natural and juridical persons. But there are differences. Juridical persons cannot feel and act as such. They do not exist in the natural world. In other words, they are fictitious.

In this situation there was a need for legal constructions. Parallels with natural persons were no longer enough. The juridical person had to have its own existence within the legal system. This called for an expansion of the cognitive scope of legal perceptions. The law had to change its relation to its environment. Legal concepts had to be based on legal positivism instead of natural law. The difference is that of going from linear explanations of legal concepts to recursive arguments. The definition of law became circular as a consequence of legal positivism. Law is created out of law. There is for legal positivism no such thing as natural rights or natural persons. The cognitive effect of the circular model of explanation instead of the linear is the increased variation and flexibility.

Legal positivism, by breaking with natural law thinking, opened up for legal constructions. It was only by making a dis-

---

[4] Jan Torpman, *Rättssystemets lärande*. (The Learning Capacity of the Legal System) Diss., Stockholm: Stockholm Business School 2002 (in press).

tinction between natural and juridical persons that the *fiction* of supra-individual persons could become redundant. Society is regarded as separated from nature and law regulated society. Law had become the positive law, which responded to and actually changed with societal development. The discovery in the legal system of its own sovereignty made the legal fiction possible as an arbitrary legal construction so long as it provided functional solutions in society. This acceptance of the fiction opened the way to new ways of projecting social systems in legal terms. The topology of legal theory was changed in an almost paradigmatic manner. The construction of the juridical person represents the association of co-operating individuals and thereby substituting what was earlier understood in terms of relations among the same individuals.

Thus, the concept of juridical person was not created by the state and the political system, but by the legal system. Also the state is a legal category and constructed by the law. By the innovation of the juridical person, the legal system has been able to bring forth a theory of persons that has had revolutionary implications in society. Within the legal system, as a consequence, an almost exponential growth of norms has taken place. The legal system has through many cognitive innovations and a capacity for learning expanded its ability to observe its environment and thereby successively provided more effective structures as the need arose. The creation of the innovation is in most cases, as in this one, a question of a long process with many influences. With the concept of juridical person, the legal system both expanded its capacity to observe changes and developments in society and was able to retain and develop existing (Roman law) legal doctrines. The concept of juridical person made the expansion of large-scale industrial society possible. Companies got an identity of their own and as legal constructions became power centres with a rationality which goes beyond the interaction of the co-operating individuals. These social and legal changes could take place without alterations in legal reasoning.

2.2 The example of collective agreement

A similar problem in relation to the growth of the large-scale industrial society was the need for a collective agreement in order to create self-regulative mechanisms on the labour market. The problem was if the collective agreement could be legally accepted. Even if the perception of contract was decisive when the collective regulation of working conditions via trade unions

emerged, it was not given that the legal system could accept collective agreement as a contract in a private law sense. Could rules of contract and claims be applied to collective agreements? The nearest analogy was to treat collective agreements as reciprocal binding contracts, but the law of contract and torts, based on Roman law, was too individualistic to fit the purpose of labour market regulations. The main problem was that contracts only had legal consequences for the parties directly involved. The personal will was conclusive; personal contracts could break through collective agreements. Another important aspect was about the binding force of the collective agreement. To be effective it had to be binding not only on the contracting parties, the organisations, the employers and the employees, but on the members in the trade unions as well.

At the time of the growth of collective agreements in practice, in the late 19th and early 20th century, legal positivism, as we have seen, already had been established in legal thinking, and the lawyers gradually came to accept collective agreements as a legally binding contract with adequate legal consequences. By use of legal constructivism, collective agreements were given a special status with priority over individual contracts and they also became exceptional in having binding force even for those not being directly parties to the contract.

3 From legal positivism back to natural law design. The example of self-employed

When someone buys job performance, they use a labour contract. This can in its turn within the Swedish legal tradition be subdivided into two forms of contracts, contract of employment and contract of commission. Collective agreements complement the contract of employment in determining the working conditions, while in the contract of commission the parties to the contract have to decide on what has to be done and under what conditions in terms of payment, etc. The question is if work by a self-employed should be regulated by a contract of employment or of commission. In the present situation the answer is that if you perform the work in terms of an individual, natural, person, the work relation is regarded as employment, and if you do it as a juridical person and/or private firm it is regarded as contract of commission. In the first place you are regarded as an employee and in the second as a business firm. In the latter case you have to bear the burden of payroll tax and social security charges as if you are an

employer. Being self-employed, you are from a legal point of view either an employer or an employee; actually, you are something in between.

The legal system does not accept a natural person performing a job without being employed. If you would like to be self-employed, you have to be employed within your own firm. The structures supported by legal positivism have in our time created a mentality and a legal superstructure that create new paradoxes. What from a natural law perspective appears as the most natural thing, namely for an individual to conclude an agreement about work without being regarded as a juridical person or a firm, is in the positivistic era of law not possible. The legal constructions void it and force the work into the black market. In order to bring the phenomenon back into the acceptance of the legal system, a deregulation has to take place within company law and tax law.

The contract of commission is an existing and a relevant legal institution for regulating the work of self-employed. There is, though, a need within tax law for getting rid of the fiction of the self-employed being a firm and thereby the fiction of the self-employed being an employer, a specific fiscal subject. The self-employed could fairly well pay tax on the income he gets for his work but, since he is organising his own work, be free from overhead costs. In order to match the practical needs of the information society, the mental structures of legal positivism first have to be replaced by the natural law construct of self-employed. A person is a person who is capable of concluding a contract of commission on his own.

Anders Victorin*
Electronic Plumbing – Building the Telecom Infrastructure

1 Introduction

Like any other human activity, computing and networks of computers need access to space on the ground, in this particular case for wires, optical fibres or even radio masts and transmitters. Whenever such need is to be satisfied, the IT-world has to face the old problems of access to land by contract or by various forms of expropriation – IT law meets real estate law. This paper will discuss some of the problems that have transpired in this junction of legal structures. Due to the particularities of different legal systems, the problems may concern different aspects in various countries, although the basic issues remain the same. In this paper, however, Swedish law will be the main subject of discussion.

The basic requirements of operators of electronic services and owners of such networks are the same as for all commercial activities, i.e. the property concerned must be the subject of clear ownership and be made subject to normal commercial transactions – the rights to land should be secured, the property should be eligible as collateral for loans, it should be possible to lease it, etc., and such transactions should of course be protected under property law.

Unfortunately, this is easier said than done under real estate law as far as the physical components of such networks are concerned. First, Swedish law has not even considered many of the issues, e.g. leasing a pair of optical fibres in an optical fibre cable, until now. Secondly, much of the applicable legislation has been created with the needs of public utilities companies in mind. Therefore it is adapted to the needs of publicly owned, *de facto* monopoly enterprises, having little regard for the more commercial aspects referred to above. Therefore, the fundamental problem concerns the adaptation and reshaping of old legal structures

---

* *Anders Victorin* is a professor of private law, specialising in real estate, valuation, and building law, at the Faculty of Law, Stockholm University, and the Royal Institute of Technology (KTH). His publications include works on housing law and real property as well as labour law. For the IT Law Observatory he has written reports on the legal aspects of the physical infrastructure of the information society.

to new needs created by new applications in combination also with privatisation and deregulation of the old monopolies.

2 A note on legal development of access to land for electric and telephone cables and wires

Like many other European jurisdictions, Swedish real estate law operates under the *numerus clausus* principle as far as property rights to land are concerned. Only certain contracts with regard to right to land are awarded property law effects. Since personal easements are not recognised under property law in Sweden, the contract by which electrical companies have secured the right to land has traditionally been easements in which the power station was the dominant real estate unit. The Swedish National Telecommunications Agency (Televerket) was not able, however, to use such a method, since it was considered that no proper dominant real estate units were to be found. Consequently the Televerket was left forced to use the contract form of (partial) right of use. This contract, however, was much less suitable than the easement, primarily because it could only be made for a limited period of time – 25 years in areas subject to detailed planning, i.e. densely populated areas, and 50 years in other areas. In fact, the privatised Swedish telecom company Telia now faces severe problems because thousands of contracts for base stations are on the verge of running out or have already done so, not to mention hundreds of thousands of contracts for telephone cables and wires.

In order to remedy the situation new legislation was enacted in 1973 – the Act on cables, wires and conduits (*Ledningsrättslagen,* hereinafter referred to as the Utility Easements Act)[1]. This Act is a simplified version of the Expropriation Act, and it has a narrow area of application. It applies only to certain kinds of cables, wires and conduits, which are used for certain purposes. Moreover, it must be construed narrowly, because it has an expropriative character. It devises a particular land-surveying procedure whereby land can be taken for the establishment of such property. The landowner is given compensation for the infringement according to the principles of the Expropriation Act. As a result, a certain right is awarded to the owner of the cables, etc., *ledningsrätt* (which accordingly may be referred to as a utility

[1] The terminology is problematic here. The Swedish word “ledning” means “conductor” or “conduit” in the general sense of the word, i.e. anything that leads electricity, air, liquids, etc.

easement). It can properly be regarded as a personal easement created by expropriation-like proceedings. Hence, it is not limited in time and, moreover, it cannot be touched by any private law actions, short of an agreement between the holder of such a right and the owner of the land that the right shall cease to exist. In fact the protection is stronger than any protection given by property law rules. – To be sure, land can also be expropriated for the same purposes as the Utility Easements Act, but the expropriation procedure is much more expensive and time-consuming.

However, the Utility Easements Act, as already indicated was created with a view to the needs of public utility companies. Even recent amendments have been made in accordance with this inclination of the Act. This, coupled with the narrow field of application of the Act creates problems for the IT infrastructure and that is the subject of the following discussion. Much of what will be said is subject to litigation and heated discussion in Sweden, mainly for three reasons. First, the landowners request more compensation than is given under the Utility Easements Act. When a new IT infrastructure is built it is no longer a matter of public utilities, they claim, but of profit-making business. Secondly, the building of the 3-G mobile telephone network is under way and must be finished before the end of 2003. The shortcomings of the Utility Easements Act must not stand in the way. Thirdly, it is not unlikely that one or more of the owners of computer networks will go bankrupt sooner or later, and by then a number of property law issues should have been straightened out.

3 The coverage of the Utility Easements Act

The Utility Easements Act is purposely restricted to cables, etc., of a certain kind, used for a particular purpose. In this context the relevant statutory text (sec. 2, para. 1) indicates that the Act applies to "a telephone line included in a telecommunications system for public use and [also] a public low voltage line for signalling, remote control, data communication or some similar purpose."

From this definition it is immediately clear that it is doubtful whether optical fibres are at all covered by the Act, since they certainly are not "electrical" in the normal sense of the word – they are indeed conductors, but of light, not electricity. Curiously enough, this particular angle of the problem has never been tested. And the reforms of 2001 certainly put a stop to the discus-

sion. Those reforms made it possible for electrical power companies to hang fibre optical cables in their existing power line pylons and distributing poles without obtaining a new or extended permit.

Recently, however, a more serious problem has surfaced. It concerns the radio masts for the 3G cellular phone system. These masts are not interconnected by way of electrical cables or even fibre optical cables at all – they communicate with the various base stations by way of radio signals. However, the operators insist that the rights to such masts be protected by way of utility easement. In order to solve the problem, the land surveying authority has come up with a perhaps too ingenious solution: the masts themselves and the receiver-transmitter equipment are to be regarded as "cables" under the Act, since they are part of an integrated communications network.

The matter is now a subject of litigation, but it is not unlikely that the Swedish Parliament will have to intervene by way of new legislation so that the building of the 3G networks is not bogged down in the courts.

The present author's main observation is only that the discussion serves to illustrate the difficulties involved in adapting old legislation to new technical development. The main mistake of the framers of the Utility Easements Act was to restrict it to certain kinds of cables, wires and conduits.

4 Using existing infrastructure for fibre optical cables

The Swedish legislator has wisely assumed that the most efficient way to propagate fibre optical cables is to use existing infrastructure, i.e. mainly roads and power pylons. As far as public roads are concerned, the technique is quite simple, since the Roads Act allows the road owner (the Swedish National Road Administration, a government agency) to sublet space in the road bank for various purposes. Unfortunately, the landowners are not very happy about this. The right of road is formally a right of use, similar to the utility easement, and the landowners naturally want part of the compensation the road owner stipulates for granting such a subletting of space.

As far as power pylons are concerned, new legislation has been introduced. As already indicated, a new section (3 a) of the Utility Easements Act prescribes that holders of utility easements for electric power lines are entitled to use the space also for telephone wires and other electric wires for signalling, etc., accord-

ing to sec. 2 (1) of the Act (cf. above). This solution is problematic for several reasons.

First, it becomes impossible for the electrical power company to transfer the optical fibre cable without at the same time transferring the power cable and the utility easement. The Act expressly prescribes that the cable cannot be transferred without the utility easement.

Secondly it becomes impossible to use the fibre optical cable alone as security for credit. The security must, for reasons just indicated, consist of the utility easement plus the power cable and fibre optical cable.

Thirdly, the new legislation presupposes that the whole power line is secured by way of utility easement, but this is not always the case. More commonly, the power line is only partially secured in this way, whereas the remainder may be secured by an ordinary contract of easement. If the latter is the case, the power company cannot transfer the power line or the fibre optical cable at all without transferring the dominant real estate unit.

Fourthly, it is certainly possible to lease the fibre optical cable to an external party, but it is difficult to say what kind of a lease it is. A power line may partly be regarded as real property – this is the case when it is protected by means of a contract of easement or when the utility easement has been declared a fixture to real estate (sec. 1 of the Act). In such a case a lease of an optical fibre cable is to be regarded as lease of real property (Ch. 2 sec. 1 of the Land Code). If this is not the case, the utility easement as well as the cables is to be regarded as a movable. The rules, particularly as regards property law, are entirely different depending on how the property is classified.

In the opinion of the current author this complicated situation requires a better solution. One possibility is to create a new legal figure for the lease of fibre optical cables, for instance a by giving the owner of the utility easement a possibility to create a personal easement in that right. Another possibility is to provide regulation of such leases along the same lines as leases of real property, regardless of its character of fixture or movable. The details will not be elaborated here. The same solution could apply also as far as lease of space in roads is concerned. However, the situation is clearer here, since the right of road is technically a movable.

5 Lease of dark fibre

A fibre optical cable may consist of hundreds of pairs of fibre optical wires. Many enterprises are interested in leasing one or several of such pairs for their own particular use, thus excluding any one else from using them. It is, however, difficult to conceive of a situation where such pairs are transferred with property law effects – the pairs of fibre optical wires cannot be separated from the cable without being destroyed. They can, however, be effectively individualised and marked.

The question is what kind of protection one wishes to bestow upon such a lease. If the cable is to be regarded as a movable, legal protection in the event of transfer of the cable is nonexistent, short of a claim for damages against the transferor for not reserving the right of use, as is the safeguard in the event of the cable operator going bankrupt. On the other hand, if the cable is to be regarded as a fixture, extensive protection is given in such a situation. In the present writer's opinion, the interests of enterprises that have leased dark fibre deserve extensive protection, regardless of whether the property should be regarded as fixture or movable. These interests primarily consist in the right to use the property on a continuing basis, so as to guarantee computer communications in a safe way. For many enterprises this interest is as essential as the leasehold of office space in a building.

6 Co-ordinating the interests of several users

The so-called Service Directive (96/19 EEC) requires that new actors in the telephone market in certain cases be given access to existing canalisation or telephone poles created by existing telephone organisations on reasonable terms. The directive concerns only existing infrastructure created by means of utility easement or similar legal measures, which appears somewhat questionable from a rational point of view, but perhaps inevitable from a legal point of view. It is well known that the co-ordination of the activities of the various actors poses severe practical problems, and also some legal problems.

As the present author sees it, there are two main solutions to the problems of co-ordinating the activities of several operators using the same infrastructure (although using different cables and wires). One solution is to consistently regard the first installation of fibre optical cables, power lines, etc., as primary in regard to

the subsequent installations. This is a metaphor derived from real estate law, where the rights of subtenants always are dependent on the rights of the primary tenant. Should the primary tenant's right of use cease to exist, the rights of subtenants are also extinguished. Their only sanction is a claim for damages against the primary tenant. The main argument is that the right of the primary utility easement holder is a right in relation to the landowner. He has no relationship to the holders of secondary rights. This is also a practical point of view – if the canalisation, power pylons or telephone poles are abandoned by their owner, it becomes practically difficult to create a procedure whereby such property is taken over by the holders of secondary rights. Admittedly, it is possible to conceive of a situation when the secondary tenant takes over the lease of the primary tenant, even against the will of the landlord. However, the property involved is that of the landlord and not of the primary tenant.

A second solution is perhaps more imaginative. It is based on the principles of partnership (or even co-operatives, such as co-operative housing, a useful metaphor in this context). The ownership of the infrastructure is transferred to a partnership or co-operative, which will act in relation to the landowner (and the authorities). The matters of rights to use the various cables (or pairs of dark fibre or contracts for transmitting capacity, etc.,) will be administered by the partnership. This seems to be a more rational solution than granting the various users separate utility easements and certainly more rational than granting 96 different utility easements in one fibre optical cable, as has been done by the Swedish Land Surveying Authority. Such a solution does not solve the problem of who is in authority when technical problems appear, when the cable requires repairs, etc.

7 Conclusion

The problems discussed in the foregoing are real and of great concern for all parties involved. This has prompted the Swedish government to give terms of reference for a government investigation (dir 2002:17, dated February 8, 2002), which is to propose solutions to all the problems indicated above (and some more). What is unfortunate, however, when IT-technology meets real estate law, is the fact that the making of new real estate legislation takes time. It could well be that the creation of the 3-G system will be finished before the new legislation is in place, something which will only benefit the landowners.

Part V:
Security and Vulnerability

Sören Öman*
Protection of Personal Data – But How?

1 Historical background

The right to protection of privacy in connection with processing of personal data is seen as an outflow of the right to respect for private life. The latter right is regarded as a fundamental human right, protected according to several national constitutions and international instruments, most noticeably Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Since the 1970s special legislation has been developed for the protection of privacy in connection with processing of personal data by automated means (in computers).

The first national legislation aimed at protecting the informational privacy of individuals when their personal data are processed in computers saw the light of day in Sweden in 1973. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerised registers. The Act did not contain many material provisions on when and how the data should be processed, or general data protection principles. Instead, the Act required for each computerised personal data register a prior permit from a new data protection authority – the Data Inspection Board. When a permit was given, the Board issued tailor-made conditions for that register.

Several Western European countries followed Sweden's example and in the 1970s adopted special data protection legislation and instituted special data protection authorities. When several countries provided differing restrictions on the processing of personal data in computerised registers, this became a hindrance to international trade. Provision of goods and services across borders requires automated processing of personal data. The need for international harmonisation became evident. Work on international instruments on data protection commenced within OECD and the Council of Europe.

This work resulted in the 1980 OECD recommendation on guidelines governing the protection of privacy and transborder flows of personal data and the 1981 Council of Europe Convention 108 for the protection of individuals with regard to auto-

* *Sören Öman* is a senior legal advisor commissioned by the Swedish government go make a review of the Swedish 1998 Personal Data Act.

matic processing of personal data. The aim of those international instruments was twofold: (i) To provide an international standard for the protection of privacy in order (ii) to facilitate international trade through free flow of personal data across borders. The OECD recommendation is a non-binding instrument, while the Council of Europe Convention is binding for those states which have acceded to the Convention.

The Swedish approach with tailor-made conditions for each register could not work in an international environment, due to the absence of any international body to make the conditions and to the drastic increase in the number of computerised registers. Instead, fundamental data protection principles were developed, taking into account the developments in the other countries which had enacted data protection legislation. As an example Article 5 under the heading "Quality of data" in the Convention could be mentioned:

> Personal data undergoing automatic processing shall be:
>
> a. obtained and processed fairly and lawfully;
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
> d. accurate and, where necessary, kept up to date;
> e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

The principles contained in the international instruments were not confined to processing of personal data in computerised registers. The principles were instead applicable to more or less all automatic processing of personal data. As soon as a single piece of information relating to an identifiable individual was keyed into a computer, all principles were to be applied. When the principles were developed in the 1970s and early 1980s, this distinction did not have much practical importance. Personal data were processed in computers almost exclusively in the form of traditional registers. Computers at that time, for example, were not used for everyday production or dissemination of text.

In 1995, after some five years of discussion, the European Union adopted a directive on data protection (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 Data Protection Directive draws upon, elaborates and strengthens the principles contained in the Convention. New principles are

also introduced, most noticeably an obligation to inform the registered persons about the processing in connection with the collection of personal data. The principles in the Directive cover all automatic processing of personal data and manual processing of such data which form part of a filing system or are intended to form part of a filing system.

The Directive should have been implemented in all Member States not later than in October 1998. A new Personal Data Act, based on and implementing the Directive, entered into force in Sweden at that time (SFS 1998:204). For various reasons, however, many Member States, Sweden among them, have had difficulty in implementing the Directive. France and Ireland, for example, have yet to implement it fully.

2 Data protection principles and the handling of text

The situation has changed radically since the principles in the international instruments – and the Swedish 1998 Personal Data Act – were developed.

A quarter of a century ago, the automatic processing of personal data was almost exclusively conducted in the form of traditional registers by authorities and corporations with large resources. Personal data registers were instituted after careful deliberations and cost-benefit analysis. The registers were designed and handled by a limited number of persons. A small authority in Sweden could at the beginning of the 1970s lay down conditions for each of the then existent, relatively few registers.

Today, word processing of text, which has not been structured in order to facilitate retrieval of personal data, is one of the most common forms of automatic processing of personal data. Such processing is now being done every day by almost all enterprises, large and small, and by almost all the millions of office employees in Europe. The production of text in computers is now an everyday activity for everybody. The text produced could be for correspondence, for publication on the Internet or for an internal memo or a draft decision. The development of international telecommunications networks, such as the Internet, has made it possible for small corporations and even private persons to publish text internationally at little or no cost. Restrictions for processing of personal data in computers therefore have a more direct and acute implication for the right to freedom of information and expression. It is in this context interesting to note that the three references for a preliminary ruling on the interpretation

of the EC Data Protection Directive which until now have been made to the European Court of Justice all concern proceedings resulting in publication of personal data.

When the data protection principles were developed some twenty years ago, the bulk of (the) word processing (of text) was done by non-automatic means and therefore not covered by the principles. But technological development has also moved the everyday production and publication of text into computers. Thus, the scope of application for the principles has been extended to areas for which they were not originally developed. It is interesting to note that the EC Data Protection Directive extends the application of the principles to include manual processing of personal data, but in this case restricts the application to personal data in traditional registers.

Are the data protection principles adequate for the processing of personal data which goes on today when computers have become an everyday tool for everybody and everything?

I think almost everybody will agree that the principles in themselves are by and large as relevant and adequate today as when they were developed some twenty years ago. The principles work well when it comes to automatic processing of large amounts of personal data contained in traditional registers where the data are structured in order to facilitate retrieval of personal data. The principles were developed with such cases in mind. The application of the principles helps to enhance the public's confidence in the processing carried out by state authorities and large corporations such as banks and insurance companies.

But are the principles also adequate for the "new" forms of processing, namely the handling of text which has not been structured in order to facilitate retrieval of personal data? Since each of the data protection principles seems reasonable in itself, I do not think that anybody can with reason argue that the principles are not also adequate per se for the handling of text containing personal data. Who, for example, could argue that personal data in the text should not be adequate and relevant in relation to the purposes for which they are stored? I nevertheless think that we need a modified – simplified – protection for personal data in connection with the handling of text. It is the technological development in the last twenty years, and the accompanying widespread and diversified use of the technology, which necessitates a modified protection. The principles themselves may well be reasonable, but the strict application of them to the handling of text may not be.

The application of the comprehensive rules derived from the data protection principles is in my opinion not practical, not nec-

essary and too cumbersome for the today commonplace and highly volatile activity of production and other handling of text in computers carried out by virtually every office employee. For every piece of personal data, the data protection principles would require the employee producing the text – for instance an internal memo – to go through all the steps required by the principles: what is the purpose of processing that piece of personal data, is that piece of personal data adequate and relevant in relation to that purpose etc.? In my opinion, it is not reasonable to have such a bureaucracy, nor the expense it entails, for the everyday handling of text. The lion's share of the text handled is probably totally harmless to the persons mentioned in the text. It is therefore hard to understand why bureaucratic, and costly, rules and routines have to be applied to all handling of text just to prevent the few cases where the processing could be harmful. Anyone with the least knowledge about the realities of office work today also realises that any attempt at strictly applying the data protection principles to all processing of personal data in the course of the everyday handling of text would be futile. In fact, I believe that the principles in practice are not, and will never be, strictly applied when it comes to such processing. An overzealous application of the principles on the everyday handling of text would effectively paralyse any organisation.

If the data protection principles are applicable in situations where this is not reasonable, and the principles therefore are not applied in practice, the overall respect for the principles and their acceptance in the society is threatened. In fact, several of the respondents to a recent survey in Sweden believe that the application of the principles every time someone produces text is absurd (Ds 2001:27).

It is well-known that the application of the data protection principles, and the bureaucratic rules and routines derived from them, including the supervision of the application of the rules by a data protection authority, to the publication or other dissemination of text undoubtedly impede the enjoyment of the right to freedom of expression. Due to the new network technology and the widespread use of international telecommunication networks, the conflict between data protection and the right to freedom of expression has become acute. Today, almost anybody can instantly publish text worldwide at hardly any cost, simply by pressing a button. In such an environment the rules on data protection should be more expressly synchronised with the right to freedom of expression.

I have made here a distinction between personal data contained in – or intended for – traditional registers and such data

contained in text which has not been structured in order to facilitate retrieval of personal data. I realise that such a distinction can be criticised for not being distinctive or realistic. Today, text can also easily be searched through or organised in order to retrieve personal data. Sweden's experience, not least, of trying to apply the 1973 Data Act, which was based on a similar concept of personal data register, to the technological developments of the 1990s shows the difficulties involved. I nevertheless think that the distinction is valid even today. There is, regarding data protection aspects, a fundamental difference between the situation where the controller of the file focuses on personal data and its easy retrieval and the situation where focus of attention is on the text, whether or not it contains personal data. The data protection principles, and certainly the EC Data Protection Directive, already contain several vague concepts which we can live with. And I think that the distinction outlined between a register and text would be as clear and useable as many of the existing concepts. I would, however, like to make clear that the situation where someone in fact is using the text to search for and compile information about an individual should be treated according to the rules applicable to processing of personal data in registers.

For the reasons stated, I believe that we need a different approach to data protection as regards the handling by automatic processing of text, which has not been structured in order to facilitate retrieval of personal data. What we need is a system that affords effective protection for the vital interests of the data subjects' right to respect for private and family life and at the same time is easier to understand and handle on an everyday basis. I think that a new system of data protection should concentrate on preventing abuse of personal data rather than on regulating every step in the processing of such data. As I see it, there should be a shift in focus from the handling of every piece of personal information to the ultimate goal, preventing abuse. I would like to give some examples of what I mean.

3 An abuse centred approach to handling of text

First, I would like to make clear that I think that the data subject's right of access to his or her data is fundamental also when it comes to personal data contained in text. This right enables the data subject to control, at his or her discretion, what data are used and to make objections. One problem with the right of access, especially concerning personal data contained in text, is that the

controller of the file could have difficulties finding all personal data about an individual contained in text. The right of access must not lead to a situation where controllers design tools, which they otherwise do not need, to retrieve personal data in text. It should therefore be made clear that, in response to an access request, the controller is obliged to use only existing tools and make only reasonable efforts to locate personal data, taking into account *inter alia* the information provided by the data subject. The data subject's right of access must also be balanced against the rights and interests of other data subjects and of the controller. One piece of text can contain personal data about more than one individual, and the controller should not be obliged to disclose data about other individuals than the one requesting subject access. In certain situations the controller's interest in keeping the data secret outweighs the data subject's interest in having access to his or her data. This can be the case concerning for example text containing communications between the controller and his or her solicitor in connection with a law suit against the data subject.

I think it is fruitful to distinguish between two different situations: The internal handling of text by the controller of the file and the controller's intentional or unintentional dissemination of the text to external recipients, including publication of text as well as disclosure of text to a limited number of recipients.

The internal handling by the controller of the file of text containing personal data, which has not been structured in order to facilitate retrieval of personal data, is seldom problematic. It is principally two situations that need attention.

Firstly, a controller should not be allowed to collect an unreasonably large amount of text about an individual without a legitimate reason. Even if the controller does not use the collected data in any way, most people would probably think of such an accumulation of personal data as an invasion of privacy.

The second situation is when the controller is using text containing personal data to base a decision which significantly affects the data subject. In this situation the data subject could use his or her right of access to the data to check what personal data have been used as a basis for the decision. What could be required is a right for the data subject to have the decision reevaluated by the controller in the light of any objections raised by the data subject. An alternative, or supplementary, strategy would be to require that the controller beforehand communicate to the data subject all data on which he or she intended to base a decision.

The more problematic situation is when the controller disseminates or discloses text containing personal data. Most countries with data protection legislation probably already have legal protection against defamation, slander and libel. What is necessary apart from that is a general protection against the dissemination or disclosure of text containing personal data in a way that harms the data subject. The dissemination of text to a wider audience (publication) should, however, be allowed, if the controller was obliged to give an opinion or if the dissemination is otherwise justifiable having regard to the public interest. Harmful disclosure of text to one person or a limited number of persons should in addition be allowed insofar as the disclosure is justifiable, having regard to the legitimate interests of a natural or legal person, including the controller.

Per Furberg*

Dealing with Computer Crime. A Critical Review of Legislative Reactions to Computer Crime

1 Computer crime

The development of information technology (IT) has opened up a whole range of new possibilities, enabling the storage and transmission of all kinds of communication. However, these new functions for information management have also brought with them new types of crime and the commission of traditional crimes by means of new technologies. Internet, websites and other communication facilities have made such criminal behaviour possible, independently of geographical limitations and national boundaries. The worldwide spread of computer viruses and similar malicious codes has provided proof of this reality.

These new threats are challenging existing legal concepts, cf. the description above in Part II, "Lawmaking and IT" of the dematerialisation in the IT-environment and its effects on current legislation. The use of metaphors from the "real" world is even more illustrative in the field of penal law, where the wordings and descriptions normally reflect views originating from a different technical culture.

Another problem is the useful and, outside the penal law, often recommended analogisms. According to the principle of legality, a criminal law provision may not be given a more extensive area of application than its wording permits. Legal measures to prevent and deter criminal behaviour must be clear, at the same time as the introduction of IT in almost every sector of daily life calls for a minimalist approach in order to avoid two different sets of rules and regulations depending on whether a transaction is supported by IT or executed in the traditional environment.

---

* *Per Furberg* is a member of the IT Law Observatory. See presentation in Annex 1.

2 Legal harmonisation

National laws have gradually been adapted to IT, normally as a result of actions taken by various international organisations. Computer-related crime was discussed by an ad hoc committee of the OECD who in 1986 suggested a list of acts, which could constitute a common denominator between the different approaches taken by member countries. The work continued within the Council of Europe where expert committees elaborated recommendations on computer-related crime (N°. R (89) 9) and on problems of criminal procedural law connected with information technology (No. R (95) 13). These reviews of European criminal laws and the recommendations to concerted actions formed the basis for the IT-related amendments in 1986 to the Swedish criminal law provisions regarding e.g. fraud, usury, unlawful use and breach of data secrecy (Government Bill 1985/86:65).

It is true that similar amendments were introduced in other European countries and resulted in a co-ordination of national penal law concepts, but only a binding international instrument may ensure the efficiency in the fight against these new phenomena. Consequently, the Council of Europe established a Committee of Experts on Crime in Cyberspace to provide such an instrument.

The committee carried out a comprehensive analysis of cyber-space offences and the new dimensions created by IT. The sometimes detailed considerations can be instanced with the special attention paid to the criminal law aspects of electromagnetic emissions radiating, for example, from monitors. In November 2001 the outcome of the committee's considerations – a Convention on Cybercrime – was opened for signature. It aims at harmonising the domestic criminal law in the area of cyber-crime, providing domestic criminal procedural law powers for the investigation and prosecution of such offences as well as other computer-related offences and establishing fast and effective international co-operation in this field.

In the following, some examples will be given of the corresponding domestic debate and the need from a legal perspective for a deep understanding of the prerequisites given by IT. The background is the findings of

- a committee, established by the Government, which in December 1992 issued the report "Information and the new **I**nformation**T**echnology – criminal and procedural legal aspects" (SOU 1992:110), and

- a commissioner (Jörgen Almblad), appointed by the government to consider the need for IT-related amendments in the aforementioned environment (Ju 1997:A), who tabled a memorandum of March 17, 1998, "Penal law and information technology – a basic inventory of the need for legislation".

3 Fundamental differences

The aforementioned committee started from a description of *data* and its character – demonstrating that the difficulty in understanding the IT-related legal issues is partly due to the fact that we are moving in the borderland between concrete and abstract objects. Some of the self-evident presumptions underlying a traditional viewpoint do not exist in the IT-environment. The committee assigned this digital category the term *quasi-material* and endeavoured to interpret or suggest amendments to the law, headed to avoid artificial concepts with too little attention paid to IT.

The commissioner, on the other hand, took his starting point in the traditional physical objects, and was apparently non-committal on the subject of technical IT-related issues. He found no need for any new specific criminal law provisions and recommended considering only a few minor amendments to the existing penal law. Other matters were to be solved within current legislation, according to the commissioner's findings.

None of these approaches have yet been adopted by the Swedish legislature, but most likely it will have to come to a decision as a result of the Convention on Cybercrime, which has been signed by Sweden and numerous other states.[1]

4 Documents

The penalty clause on falsification of a document is a good example of an area where the choice of approach to IT will be significant for future legislation and case law. The definition of "document" according to Chapter 14, Section 1 of the Swedish Criminal Code includes several "concealed demands" as a part of the word "document". It is an implicit qualification within the document that it shall give *self-dependent existence* to the infor-

[1] See http://conventions.coe.int/treaty/EN/cadreprincipal.htm

mation and via its physical bounds provide a clear distinction from other physical objects. Additional demands to qualify a record as a document are that it must have certain *durability* and the ability to *convince of its authenticity*, i.e. to give the reader reason to believe that the document originates from the individual who, according to the document, is seen to be the originator.

The need for legal acceptance of signed electronic *data* formed the basis for the aforementioned committee, which focused on legal protection for the authenticity of electronic substitutes for traditional paper based originals. The commissioner, on the contrary, argued that criminal law protection emanating from such IT-routines was unnecessary and that it would be far-fetched to compare electronic signatures with traditional signatures. Instead the commissioner recommended an approach based on who could be regarded as issuer of the data *carrier*. When a record is transmitted, e.g. via electronic mail, the commissioner mentioned, as one possible solution, considering the sender as issuer of his hard disk and the addressee as the issuer of his storage *medium* – he should be regarded as "communicator of the information in its present state" on the computer where the received copy is stored. Further, the commissioner stated that electronic mail, deleted after being read by the addressee, has more in common with a conversation over the telephone than with traditional paper documents.

However, taking the issuer of the storage *medium* – furnished with numerous (signed) electronic messages – as starting point, would bring back an outdated approach and the penal sanctions would probably be fictitious as the user normally does not know on which physical disk the message will be stored, where it is held and who owns or otherwise has right of disposition of the data *carrier*. The protected interest is the need to be able to trust the statement on the origin of the text, not the genuineness of the disk drive. Many have not fully understood that all information is broken down to ones and zeros and that the unique aspect is related to a unique pattern of data rather than to unique physical examples; c.f. the implicit qualification within the document that it shall be an original.

A few years later the committee's stress on the protection of *data* and its authenticity, more or less independently of its storage, was given support by the EC-directive (1999/93/EC) of the European Parliament and the Council on a Community framework for electronic signatures. Further, a contribution to the legal recognition of electronic documents has been given by the Convention on Cybercrime, which imposes an obligation to establish as criminal offence the input, alteration, deletion, or suppression

of computer data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic. The focus on the difference between data and the data carrier used to perform processing of the data is already evident from the convention's choice of terms (Art. 1).

The principles of how to determine whether a record is authentic have for decades been a moot point of legal doctrine. The aforementioned commissioner's statement – that it in principle does not matter whether the sender or receiver of a record should be considered the issuer of the copy stored on the receiver's hard disk – is obviously not correct. In Swedish law, very simply, the authenticity of a traditional document is judged by asking who, according to the document, is the guarantor of the original physical example. If this information is true, the document is authentic.[2] This physical approach is not compatible with the quasi-material character of data and the Svea Court of Appeal has recently confirmed this by rejecting a count on document forgery consisting of issuing unauthentic telefax print-outs or electronic records produced by word processing programs.[3] One may compare with German penal law, according to which the judge will have to decide who is the issuer of the *text*, a scheme compatible with IT and adopted for the Swedish laws on (signed) electronic documents for the customs and taxation legislation.

Consequently, the difficulty in adapting the legislation to the IT environment partly derives from the need to reconsider traditional legal concepts, debated even before the introduction of computers.

5 Protected electronic places

Another area where the approach to establish legal protection in the IT field will be especially decisive for the lawmaker is whether the criminal law protection shall be based on

- the existence and location of an electronic substitute of a certain physical place, the integrity of which is reserved for the possessor (spatial integrity) independent of the sensitiveness of the stored data, or

---

2 This should not be confused with criminal acts committed by making false statements in an authentic document (cf. false certification, Chapter 15, Section 11 of the Criminal Code).

3 Svea Hovrätt sentence of 31 May 2002, docket number B 5358-01.

- the customary limitation in the IT environment to *immaterial* information as such independent of its storage space.

The difference between rules and regulations applicable to immaterial information on the one hand and a person's protected custody of digital data and documentary evidence on the other hand seems too have been neglected.[4]

This distinction, however, is reflected in the Convention on Cybercrime, ordering legislative measures to establish as a criminal offence unauthorised *access to* the whole or any part of a *computer system*. The protection of computer data is addressed in other sections of the convention. The survey of the European countries' penal laws, carried out by the Committee of Experts on Crime in Cyberspace, showed the Swedish choice of a divergent approach, namely that of giving legal protection by a penal provision regarding breach of data secrecy, formulated as unlawful *access to a recording* for automatic data processing. Should this provision be understood as a regulation regarding information as such or does it make certain methods of obtaining information a criminal offence?[5]

Another problem concerns the interpretation of the notion "unlawful". Is it meant to exclude liability when *consent* is given, when there exists a "lawful" dealing (e.g. statutory handling of protected information) or will this restriction have a bearing on the legal concepts of authority versus competence? Consider the example in chapter of a press reporter who hacks into a computer, pleading that the constitution relieves him of criminal liability.[6] Will the Swedish constitutional protection apply or will the criminal law protection be valid, regardless of the electronic environment?

The aforementioned commissioner has suggested two alternatives; (1) a criminal law protection of physical objects such as disk drives and (2) the protection of information as such. A report recently issued by a Swedish Governmental Committee tasked with considering the protection of personal data in working life has proposed that, as a general rule, there should be a ban on employers knowingly making themselves acquainted with the contents of an employee's private electronic mail.[7] However, it is not clear whether the criminal code penalises such an act and to

---

4 See also my other contribution to this anthology, *Lawmaking and IT. Reflection on the Need for New Concepts and Categories of Thought*.

5 Cf. *ibidem*, part 2 on "Electronic places and digital bearers in the legal system".

6 Cf. *ibidem*, part 3.

7 Personlig integritet i arbetslivet, SOU 2002:18.

what extent, if any, an enactment of the proposal will have effect on the interpretation of the criminal code. Some employers state that they may read anything stored on their computers. Their adversaries refer to the Human Rights Convention and the Swedish constitutional protection from search of letters or other confidential items of mail and from secret wiretapping.

The aforementioned committee chose a more complex approach, covering the protection of data carriers, data representing (immaterial) information and the (virtual) "custody", analogous to traditional physical places of storage.[8]

6 Closing lines

It is necessary to clarify to what extent (virtual) electronic places and electronic instruments are protected by criminal law and to tie the legal protection to the infrastructure in cyberspace. Technical and administrative solutions to these needs are already in place, by way of passwords, cryptographic procedures to furnish with strong authentication of users, advanced electronic signatures, digital rights management systems, and the like.

The taking of physical objects as a starting point, as suggested by the commissioner, will strike a discordant note with the actual usage of IT. The new dimensions created by IT and the virtual substitutes for traditional instruments and closed places of storage need to be taken into consideration by the legislator and in case law, to give legal effect to the borderlines and protecting mechanisms already accepted by the users of IT.

8 See *ibidem* part 2 on electronic places.

Part VI:
Legal Machinery Matters

Cecilia Magnusson Sjöberg*
The Melting Pot Paradox of Structured Documents

1 A platform for true action

Sticking to documents as a basis for a discussion on development trends in information society might be regarded as somewhat old-fashioned. But for all the growing impact of multimedia on the legal domain, the document concept still plays an important role as a basis for legal discussions, above all because law is still produced in the form of text entities commonly referred to as documents. Typical document instances are acts and ordinances, decided cases, contracts and clauses, conventions and so forth. Actually, a more appropriate expression in this context would be virtually tangible documents, meaning that these kinds of objects representing law may occur in electronic as well as in paper formats. The introduction and application of IT has, furthermore, led to a state of art where the boundaries of legal documents are not necessarily defined beforehand. The Swedish Principle of Publicity, for instance, is characterised by a right of access to dynamic constellations of data.

This presentation sets out to show that structured documents accomplished by means of standardised markup languages ought to be regarded as a highway route on the map of an information security characterised by security. The somewhat obscure title "The melting pot paradox of structured documents" is chosen in order to capture the embedded and intended contractions in the approach advocated here, viz order achieved by encumbering text with <tags> (mainly elements and attributes) and static views of structures as a basis for dynamic actions.

The grooves and moves in this context are trusted public and business activities in terms of information retrieval, knowledge management, automated decision-making, e-commerce, etc. Trust implies information security conventionally comprising the criteria of availability, confidentiality (secrecy), integrity, ac-

---

* *Cecilia Magnusson Sjöberg* is professor at the Faculty of Law, Stockholm University and Royal Swedish Academy of Sciences Research Fellow. She gained her doctorate in 1992 with a thesis on legal automation in the Swedish public sector. She is currently managing a research project that investigates the possibilities of cross-fertilisation of advanced methods for security enhancement and applications of XML in the legal domain.

countability and non-repudiation. Clearly, these building bricks of security have legal implications both in terms of system design and management as well as regards applicable rules and regulations. In the following it will be sufficient to let these concepts serve as a general framework for the discourse.

2 The mission

Structured documents, as a tool for legal validity in a security context is the mission. This statement may in itself be regarded as a content-heavy expression that can be the object of an analysis resulting in marked-up elements *and* attributes. A supporter of standardised markup languages is thus expected to take a dynamic approach to text, while those not yet informed of the potentials of the W3C Recommendation XML (Extensible Markup Language, http://www.w3.org/XML/) might still be stuck in thinking only about flat representations of key words attached to the beginning of a document or search words inserted in an (inverted) index file.

3 Why markup languages?

3.1 XML explained

It is high time now for a brief explanation of what document markup is all about. An XML document may be *well formed* or governed by a DTD (Document Type Definition) or schema. A *document type definition* defines the composition of a set of documents (e.g. laws and court cases). It contains information about document elements, the logical order of these elements and their frequency, etc. A DTD is expressed in XML and may be stored in a data file outside the document.

There are different ways of explaining the underlying meaning of a DTD. One could focus on the purpose of a DTD as a method of *structured information description in context*. This implies that a DTD does not necessarily have to be related to a certain type of document but rather to some particular kind of information. A skilfully designed DTD with corresponding markup makes it possible to adjust the use of a particular document to a variety of purposes, i.e. without later having to change the markup. XML then plays the role of an enabling tool, making it possible, for instance, to find information that is of interest on a

specific occasion. This is an indication of how important a preparatory *document analysis* is.

A *schema* can be generally described as a specification or formal definition of the constraints on the content of an XML document, aiming at both structure and functionality. One way to specify a schema is to use a DTD, but XML schemas can model other kinds of structured data as well and are in principle more expressive. An important feature of an XML schema is the possibility of integrating database functionality and communication between applications. A major purpose of an XML schema is indeed to make it support data typing (integer, date, etc.) and thereby facilitate XML data interchange with conventional database systems. XML schemas are written in XML and have been developed for use on the Internet and are therefore co-ordinated with other W3C specifications.

A *document instance* is the encoded document itself containing data (e.g. legal text), *markup* (document element tags) and a DTD reference (if not present in the document). The markup elements surrounding the text are called *tags*. In the simple example below the tags are displayed in bold characters. The value of attribute type ID is shown in the 'article tag'. 'A3-95-46-EC' here stands for Article 3 in the EC Data Protection Directive.

<ARTICLE ID='A3-95-46-EC'>
<ARTTITLE>Scope **</ARTTITLE>**
<ARTNO>Article 3 **</ARTNO>**
<PARA> 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
> </PARA>
...
</ARTICLE>

In comparison with HTML, the dramatic difference is that while HTML aims at presentation of text on a (computer) screen, a major purpose of XML is to allow for semantic expressiveness. Furthermore, the HTML DTD consists of a predefined tag set whereas an application based on XML is open to any kind of customised vocabulary. Of utmost importance is the inherent validation component of an XML application governed by a DTD or schema. In practice this means that a marked-up document is validated against the predefined logical constraints (such as decided order of elements) and the predefined number of occurrences of particular elements.

So far so good, but is the XML approach secure and what makes it at all worth investigating in terms of legal implications? The purpose here is to convey a strategy for answering this question. The aim is thus not merely to satisfy curiosity but to make the approach serve more practical interests. A legally founded checklist of *XML related security-enhancing factors* would no doubt enhance the rule of law and thus promote trust in system design based on XML solutions (see further Section 5.3 below).

One starting point is that modern document management requires co-ordination in order to meet demands for efficient production, supply and use. Apart from general needs to improve recall and precision when retrieving information, there is also reason to consider, for instance, knowledge management attempts and exchange of business data in networks of various kinds.

XML has a potential to function as a lever and a sound basis for all of these developments in modern information society. In this context it should be mentioned that XML also has a profound impact on *substantive law* itself, in particular in the fields of contract law, intellectual property rights and privacy protection. For instance, XML-messaging quite often comprises personal data processing in a legal sense (see the EC Data Protection Directive, 95/46/EC). It concerns requirements of consent from data subjects to collect, store and disseminate personal data. Furthermore, modern e-business models make it necessary to consider information duties, e.g. that the identity of a service provider must be clarified according to the EC Directive on E-commerce (2000/31/EC). Liability issues are also relevant in terms of an analysis of who is responsible for damages emerging as a result of the abuse of a transferred authentication.

As indicated above, it all boils down to trust in global digital information and a need for *legal information security* in open as well as in closed computer-based networks. Every organisation, be it a private enterprise or a public authority, needs to reflect upon the handling of documents governing internal as well as external actions. One highly important question, for example, is how far XML may support message authentication and electronic measures to prevent distortion of (document) content. The concept of authority here covers a wide variety of actions, e.g. authorisations to enter into contract, and law enforcement.

Bearing in mind the initially mentioned checklist approach, *the group of addressees* or "*who will benefit*" may be described in the following way. To begin with, secure use of XML is relevant for commercial actors as well as for representatives of the

public sector. This can be instanced with *buyers* who, in a procurement situation, are dependent on clarification of legal conditions governing a particular situation. In a *vendor* perspective, the use of a checklist may be regarded as a business opportunity in terms of a legally founded security branding of offered solutions. Enhancing legal awareness among *politicians and public officials* for the purpose of efficiency, foreseeability, uniformity, openness, etc. is another obvious advantage.

3.3 XML as a tool

The expression "XML as a tool" connotes, to begin with, *markup languages in a broad sense,* not least including SGML (Standard Generalized Markup Language), considering the impact of this ISO standard, dating back to 1986, on applications which are still running today (ISO 8879:1986). A markup language may be utilised for representation of structures and contents, styling and communications. This implies that not only the core XML W3C Recommendation is of interest in this context, but also related standardisation initiatives such as XSL (Extensible Stylesheet language), SOAP (Simple Object Access Protocol), etc. Bearing this in mind, XML ought to be regarded as a symbol for a *system development approach* commonly including data management in terms of text.

At one stage of the relatively short historical development of this type of applied information technology, the SGML community was a pretty closed one, not particularly amenable to discussions, for instance, concerning the pros and cons of various database technologies. Today the situation has changed in that XML can be said to play a central role in more or less any technical solution involving web technologies, telecommunications as well as conventional electronic data processing and to some extent also techniques having their origin in artificial intelligence.

All of this may no doubt be elementary to the already experienced user of the above-mentioned family of standards. Practical experience has shown, however, that a common misunderstanding at the management level of an organisation, be it a private enterprise or a public agency, is that XML (in the broad sense) involves choosing a particular system design and possibly even software product. Representatives of the industry as well as other promoters of standardised markup languages thus have the educational task of explaining the underlying ideas of a non-proprietary approach to data management. Otherwise there is an

obvious *risk* that such a lack of understanding may turn out to be a major *obstacle* for widespread use of XML. In fact there may be legal advantages associated with awareness of the inherent capacities of XML. The choice of system development approach as such may have an impact on a court's assessment, for instance, of whether an organisation's archival system is to be regarded as accurate or negligent in terms of meeting legal requirements of evidence by keeping track of version-dependent legacy data. The pharmaceutical and vehicle industries are typical examples of branches heavily burdened by legal requirements of documentation. However, it may not be a trivial task in a litigation situation to explain to a court just how the use of XML manifests a party's legal awareness.

To summarise, although XML may be described as a tool, it is not just any kind of tool. It is not a physical object like a pen or a paper. Nor may XML be described as a mechanical mechanism resembling, for instance, the functions of a typewriter. XML is instead a tool with *strong infrastructural potentials* closely interlinked with IT-support for information retrieval, document management and knowledge management. From a legal point of view, this deserves particular attention.

4 Infrastructural changes

The term infrastructure is often used to describe the fundamental functions of society. It can refer to both 'hard infrastructures', such as the road system, or 'soft infrastructure', such as social systems and various types of information systems. The basic components of a legal infrastructure, which may be regarded as 'soft' according to the above-mentioned classification, include various forms of (a) data processing, (b) documentation, (c) communication, and (d) organisational forms.

The introduction of information technology into society has brought about dramatic changes to all these components. For example, *data processing*, which was a *manual* activity in the past, was transformed step by step during the 1970s and 1980s into automated data processing of cases. Today, automation of administrative activities, in the sense of legal decision-making based on wholly or partly *automated routines*, can be said to be a characteristic feature of administrative procedures. Another type of legal data processing takes place in connection with the development and conclusion of contracts. The technical possibilities of electronic conclusion of contracts with the whole world as a

market place warrants a discussion in this area concerning the fundamental legal principles underlying offers, acceptance, evaluation of evidence, etc. *XML* obviously has a role to play here as a *tool for improved legal system management* considering its potentials for handling version-dependent text units over time.

Earlier generations of lawyers would naturally associate the concept of '*documentation*' with physically demarcated paper documents, which could be geographically located. In the age of the Internet this view is not longer valid. It is no longer obvious that documentation consists of *paper documents*. In many cases it may come in different forms of *electronic documents*, which are carriers of declaratory acts, proprietary rights, criminal contents, etc. XML clearly mirrors this development. Mention should here be made of such initiatives as *XML Signatures* that explicitly address the need for incremental signatures, which, for instance, may be of relevance in a situation of successive drafting of contracts.

In a similar way (voice based) *analogical* communication services are used less frequently in legal work. Both civil servants' *communication* with the citizens, and lawyers' contacts with their clients are increasingly dependent instead on *digital* and mobile services. In Sweden, for instance, the comprehensive systems for the dissemination and collection of information by the authorities are based on a strategy that may be referred to as a kind of *XML-labelling*. The system for Dissemination and Collection (Sw. SHS) constitutes the public administration's investment in order to create a general communication link to secure information exchange through the open Internet. In contrast to electronic trading systems, which are usually designed with a focus on business transactions in a certain sector, SHS constitutes a general platform, which has not been especially programmed for a certain sphere of activity.

As regards *organisational forms* we have a strong tradition of working with nationally *well-demarcated larger and smaller entities*. This is especially clear as regards the information system of public administration which has developed in harmony with nationally defined government authorities which are divided into central and local organs, etc. Information technology as such and the Internet as a concept have provided leverage for loosening up boundaries between authorities as well as national demarcation lines. The private sector may be characterised by even more *all-embracing, network-based and global organisational forms* in recent years. It is evident that *XML supports or rather is an integrated part of this infrastructural shift*. Obviously this gives rise

to a whole series of substantive law issues, for instance, how to apply privacy legislations to transborder flows of personal data.

5 Interaction of law and IT

5.1 Regulatory management

In the era of IT-supported document management there is a growing need for version control in a long-term perspective. Document markup, including linking techniques of different kinds, is attractive as a general value-adding method. At the same time, the introduction and widespread use of more and more advanced digital document management systems is resulting in a very complex environment for text handling. Furthermore, *open systems* are a major development trend in today's communications networks. One important concern, therefore, is how best to secure trails of authorisations, alterations included. More precisely, this is a matter of information security policies mirroring the norms that govern an organisation, such as who has a right of access to what, without knowing beforehand who will be claiming this right of availability.

Considering that the *major characteristics* of normative documents are complex, interdependent text units, shifting in content over time, interpretable only in context, we can extract one key issue, and that is the question of a *methodological approach* to regulatory management. If the challenge in terms of a required *infrastructure* is overcome, we can indeed expect the added value so often promised by vendors. There is otherwise an obvious risk of turnback or perhaps even failure.

The cornerstones in a *system development approach* meeting the *fundamental requirements of modern regulatory management* are (a) document markup, (b) information security, and (c) legal awareness. XML naturally represents the core method as regards *document markup*. From the point of view of regulatory management, XML offers vital possibilities of transparent modularity in a structural context. The conventional understanding of *information security* is that it comprises availability, confidentiality (secrecy), integrity, accountability and non-repudiation. Ongoing work at IETF (The Internet Engineering Task Force) on securing web-based documents will of course serve as an important input. In this context the focus of attention is on the XML Signature and Encryption initiatives. The application of a cryptographic method of progressive (incremental) security enhancement may serve as supplement. Finally, *legal awareness* is re-

quired in terms both of methodological aspects of legal system development and of substantive law issues related to the use of electronic signatures, electronic evidence, etc. The last mentioned perspective might also be expressed in terms of *possible legal validity as proof of actions* of different kinds.

5.2 Electronic signatures as an illustration

There is no doubt that *electronic signatures* and other means of secure electronic messaging are becoming established in society. The main question of law is whether, how, and to what extent electronic signatures can be given the same *legal effect* as handwritten signatures. This will ultimately lead to the question of the *evidentiary value* of electronic signatures. This presentation does not aim to provide a detailed analysis of these questions in the light of different jurisdictions. Here it will be sufficient to say that in general civil law has a relatively limited number of formal requirements concerning handwritten signatures. Typical examples where such signatures are required include consumer credits and real-estate purchase. In family law, testamentary dispositions and marital property, agreements are often not valid without handwritten signatures. In administrative law it is more common to require signing, since processing of cases often presupposes submission of signed documents.

The implementation of the EC Directive on a Community framework for electronic signatures (1999/93/EC), which had to be enforced by the Member States by 19 July 2001 at the latest, clarifies certain legal situations. The overall objective of this Directive may be said to be to co-ordinate the legal and technical work of the Member States as regards electronic signatures, removing in this way the obstacles to the internal market, especially as regards e-commerce. The EC Signature Directive contains provisions relating to the legal effects of electronic signatures and the organs that may come to be able to offer electronic certificates verifying the genuineness of such signatures.

However, there is still a lot of work to be done before computer transactions can be performed on a daily basis with the help of modern information and communications technology in a *sufficiently secure way*. The latter expression refers to the need of minimising uncertainties as regards both different legal issues and practical (partly technical) circumstances surrounding electronic handling of documents. It may also be said that business models and administrative traditions have not yet been fully

adapted to the modern, more secure methods of information exchange.

Notwithstanding the above, the Directive can be said to be innovative from the European perspective in that electronic signatures under certain circumstances have been granted legal enforceability (see Article 5), which was not the case earlier in those countries which lack the principle of free examination and evaluation of evidence.

Applicable *Nordic law* shows in this respect that when the legislator uses the term 'written', electronic communication may be allowed to take place. The requirement of written procedure is posited here primarily as opposed to oral procedure. When a statute contains expressions such as 'signature' or 'that must be signed by the party in question', or the like, then this cannot be taken to mean that electronic documents or signatures may be allowed to replace traditional paper documents and manual signatures at the present stage of technical development. However, special rules or established practice may permit the use of electronic form after all.

As regards *evidentiary value*, the state of the law is a bit clearer in the sense that there is no doubt that the principle of *free examination of evidence* characterises Nordic law. In general terms, this means that there are no limitations on the sources of evidence that may be used at a trial, and also that a judge is not bound by any special regulations regarding the way in which different types of evidence shall be evaluated. Nor does the legislator seem inclined to introduce any general *rules on the burden of proof* which would be dependent on the medium used in a given case. The important factors are instead considered to be the parties' internal relations, the character of the legal document, etc. One can therefore conclude that Nordic courts encounter no formal obstacles to considering *system evidence* in the sense of electronic documents, electronic signatures and other components of information systems.

5.3 XML related security-enhancing factors

The discussion above boils down to a need for a strategy to handle legal uncertainty characterising the information society of today here illustrated by the EC Signature Directive. This manifest need for a legal strategy may in practical terms be transformed to a focus on *XML related security enhancing factors*. The table below presents an overview – not an exhaustive list – of what is

here referred to as *XML characteristics, means and legal incentives*.

1. XML characteristics	2. Means	3. Legal incentives
Non-proprietary format	Inherent in any XML application	*Public sector:* Accessibility in a long-term perspective *Private sector:* Legal requirements of keeping track of legacy data
Quality assurer in document production	Validated documents by means of DTD:s and schemas	*Public sector:* Public information supply (possible state responsibility) *Private sector:* Commercial products (avoiding liability)
Quality assurer in document distribution	One single repository as a basis for customising production on, e.g. CD-ROM, on-line, print	*Public sector:* See above *Private sector:* See above
Container of legal directives	Markup vocabularies	*Public and private sectors*: Availability differentiator (Official or secret data) - Authority indicator (Mirroring acting parties authorities) - Property rights administration (Labelling of rights and its owners)
Secure electronic messaging	For instance, XML signatures or mathematical approaches to incremental signatures of structures and marked-up documents	*Public and private sectors:* Normative as well as other legal requirements of authentication, validation and signed documents (text entities)

The approach described above serves as a basis for the so called SLIM Project – Secure Legal Information Management – carried out at the Swedish Law and Informatics Research Institute (IRI) at the Faculty of Law, Stockholm University. The project will run during the period 2002-2008.[1] The SLIM project is founded mainly on previous practical and theoretical experiences of using SGML in the legal domain – the Corpus Legis project together

[1] http://www.juridicum.su.se/slim.

with expertise from the Department of Information Theory at the University of Lund and the Swedish Institute of Computer Science (SICS).[2]

Because of the early stage of commercial tools that combine XML capability and digital security enhancing techniques, one aim of the SLIM Project is to have an impact on the development of future commercial XML tools for legal purposes.

6 Concluding remarks

This presentation is based on the standpoint that XML may be regarded as *a tool for legal validity in a security context*. A point is made of the fact that *XML* ought to be understood broadly and that the *tool* metaphor has implications beyond trivial physical and mechanical ones. The term "*docware*" may in this context be used as a label for XML-related technologies clarifying the chosen approach to document management in a given situation.

In terms of general development trends we have reflected upon how XML has become an integral part of *modern infrastructures* with obvious legal implications. More precisely, this has a bearing on modern means of data processing, documentation, communications and organisational forms.

The fact that there are still so many legal uncertainties in terms of lack of foreseeability concerning legal validity of actions of various kinds calls for special attention. A pragmatic approach is presented in terms of regarding various *XML characteristics as security enhancing factors*. The attraction of combining XML with conventional security-enhancing methods lies in the need for transparent, content-dependent and context-sensitive management of legally relevant text units over time. Legal awareness in this context may indeed enhance trust in the information society.

[2] http://www.juridicum.su.se/iri/corpus.

Peter Wahlgren*
The Quest for Law. Legal Sources via IT

1 Introduction

The Quest for Law was a research project conducted at the Swedish Law and Informatics Research Institute between 1993-1997.[1] The results of the study have subsequently been utilised in numerous evaluations of commercial IT-products developed for the legal market,[2] and the theoretical models developed in the project are also a basis for practical assignments and teaching activities in the Master's Programme in Law and IT,[3] offered by the Law Faculty at Stockholm University.

The aim has been for this work to contribute to the identification of the future requirements of the legal domain, with regard to legal information systems and other services traditionally related to law libraries. The intention has also been to discuss strategies and appropriate features that may be developed in order to meet such requirements.

At a somewhat more detailed level, one objective of the study has been to identify and analyse factors of relevance for the evaluation of legal IT products and in the following sections these aspects of the study are summarised.

---

* *Peter Wahlgren* is professor at the Faculty of law, Stockholm university. His doctoral thesis in 1992 treated fundamental issues of the application of artificial intelligence in the field of law. He has written studies on legal libraries and on legal risk analysis. He is presently involved in a research project on the methodology of law-making.

1 The full documentation of the project is available in Peter Wahlgren, *The Quest for Law*: *Law Libraries and Legal Information Management of the Future,* Stockholm: Jure 1999.

2 The evaluations have continuously been documented in Juridisk Tidskrift, one of the major Law Journals in Sweden. So far, some 20 products have been reviewed.

3 http://www.juridicum.su.se/iri/engindex.htm?studentinfo/master/master.

2 Evaluation of IT products for law

2.1 Background

The initial aim was to present a model that could be used in order to evaluate IT-related products and services and, more precisely, to formulate some criteria for the evaluation of phenomena of this kind. This approach was motivated by the fact that in the legal domain the knowledge of this development is rare and not very well documented. At the same time, there is little doubt that in many cases it is necessary to make choices regarding future IT investments in order to survive as a lawyer or a legal organisation. In this respect the potentialities with respect to rationalisation and quality enhancements are too important to be neglected. Consequently, the ability to evaluate various products and services is crucial.

With few exceptions, early studies of IT-based products for the legal domain have focused on technical aspects.[4] In Sweden, for instance, during the 1970s and 1980s several user surveys were completed, focusing on the first national legal information retrieval system, *Rättsdata.* These attempts were tentative and the questionnaires used in these studies basically reflected concrete technical issues, mingled with vague ideas about user friendliness. Simultaneously, an awareness of the need for legal standards was present. Any general considerations about such standards remained, however, inarticulate, and the relevant aspects to be investigated were by no means obvious. Technical aspects are, of course, still important, but as the development of IT continues, it is becoming more and more obvious that systematic evaluation must include a number of additional aspects. To accomplish this, several approaches are possible, and in this study a few of them were outlined. An attempt was also made to relate a number of such aspects to each other, in order to create a practical model for evaluation.

The starting point for this undertaking was the assumption that all legal information systems are to a large extent reflections of choices concerning i) information content, ii) technical aspects and iii) organisational arrangements (see figure 1 below).

---

[4] Jon Bing, *Legal Decisions and Computerized Systems*. In: P Seipel, From Data Protection to Knowledge Machines. Deventer: Kluwer Law and Taxation Publishers 1990 (Computer Law Series 5) at 224.

2.2 Information content

In this respect the study was devoted to the requirements connected with legal information, as these may be understood from an analysis of legal work processes and legal work situations of various kinds. Legal information was viewed in this context from the point of view of methodology. That is to say, the ambition was not to make an inventory of emerging legal problems and accompanying requests for regulations. Nor was this an attempt to try to predict legal issues of a substantial nature that can be expected to attract interest in the future. Instead, the focus was set on how legal information as such is employed and utilised in legal work processes, as they can be described at various levels. In other words, the aim was to provide a general description of the requirements that may be related to legal information – whatever legal domain they appear in. In this undertaking various functions of legal information and their relationship to legal work situations were investigated, the assumption being that an analysis of this kind should be useful for the development of future strategies of law libraries and other institutions and persons concerned with the administration of legal information.

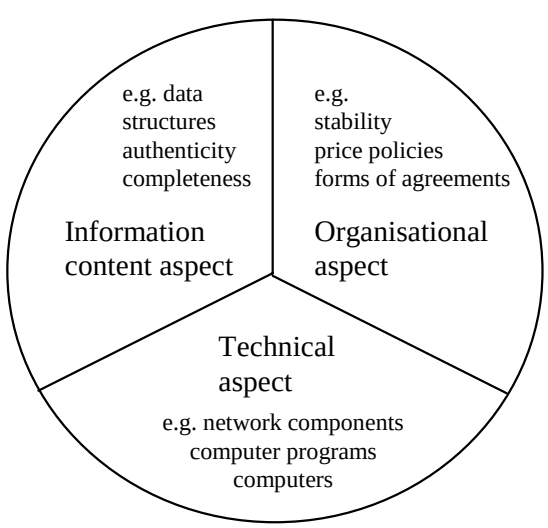


Figure 1: Basic components of legal IT applications and Legal IT systems

Thus, a somewhat more precise goal was that the study should enhance the understanding of the kind of legal products and services that may be useful to develop, and, furthermore, that the work should provide some indications of how legal information management resources ought to be allocated. In this undertaking three different levels at which various types of legal requirements can be defined were addressed – (a) the general, jurispru-

dential level where also the government's administration of public legal information has a decisive influence, (b) the organisational level, reflecting presuppositions of the organisations working with legal information, and (c) the situation of the individual lawyer.

(a) The analysis of *general requirements* clearly showed that the so-called *doctrine of legal source*s gives strong indications as to how legal information ought to be handled. Despite this, it became apparent that it is impossible to work out any universal code comprising an elaborate design strategy for legal IT-systems based on the existing descriptions of the content and hierarchical order of legal sources. In this respect the law is an all too complex phenomenon. It is also obvious that legal sources are ascribed various degrees of importance in different jurisdictions. An important drawback of a general design strategy based on an analysis of the doctrine of legal sources is furthermore the fact that conditions in different law areas vary, and that all development activities concerning legal IT systems must be adjusted to the domain in question.

The complications following from the domain-dependent nature of legal information must not, however, overshadow the fact that the doctrine of legal sources actually provides a number of standards which have to be taken into consideration in all undertakings dealing with legal information systems. It must also be observed that the analysis of the doctrine of legal sources clearly indicates a number of quality aspects which reflect the requirements of society at an aggregate level. Important illustrations in this respect are the principles of freedom of information, standards concerning free exchange of information, the importance of promulgation, etc.

It is also noticeable that the doctrine of legal sources makes explicit a number of factors that can be utilised in order to delimit and select materials in the process of legal information management. Examples of such factors are descriptions of subject-matter relevance, formal and hierarchical relevance, obsolescence, and so forth.

What this all adds up to is that the doctrine of legal sources will in most cases provide the necessary starting point for an analysis of the relevant legal material in a given area of law. Likewise, there is little doubt that the doctrine of legal sources constitutes the most reliable framework for legal information management.

(b) The investigation of the *organisational level* makes it apparent, in turn, that in all realistic enterprises involving IT in the legal sector organisational requirements must influence the ways

in which the legal material is selected. It is also obvious that organisational requirements may be of relevance for the ways in which the more subtle aspects of the material can be handled, relating, for example, to continuity, authenticity, and completeness.

The analysis further shows that requirements at the organisational level should determine the ways in which legal materials of various kinds ought to be combined and amended. It is likewise clear that the organisational framework will provide indications concerning the type of meta-information that must be included in a feasible legal information system. In this context it is also important to notice that different organisations within the same domain may exhibit quite different requirements, due to their having different objectives. Also worth mentioning is that various users within the same organisation may have different opinions about the ways in which the material ought to be best managed, and about prioritisation.

(c) The fact that users' opinions vary is even more apparent when the requirements of *individual lawyers* are studied. At this level it may be even correct to say that at some point all lawyers will have their own opinion concerning the ways in which the legal material ought to be managed. This is not only a reflection of the fact that all individuals working with legal material will have different needs, owing to differences in the tasks they have to face, but also a consequence of different lawyers having different background knowledge and different opinions on law.

Another conclusion from the analysis of individual lawyers' requirements is that law should be perceived as a network of component structures appearing at different levels of abstraction. This is a consequence of the fact that users will require various legal components in different situations. For instance, in the initial phase of the analysis of a legal problem a lawyer will seek for a legal concept describing the problem at a general level. The objective will then be to be able to delimit the issue from the legal point of view. In order to obtain a more distinct picture of the situation, in the following phase attention may have to be shifted towards legal rules and definitions of interrelated concepts (prerequisites). Thereafter, some methodological rule may have to be investigated, e.g. a rule concerning evidential value that may be ascribed to a certain fact which has been established. In the final stages of legal reasoning, search activities may aim at explicit references (documents) of a formal nature, etc.

In this perspective, documents and text units, concepts, legal rules, and rule systems are only a few examples of the components of the complex network that constitute legal knowledge. Some levels of the network (e.g. document structures with ex-

plicit references between associated documents) are clearly visible, while others (e.g. rule-structures) can only be perceived after a thorough investigation of legal texts. It may be also noticed that some of the relevant component structures necessarily generate secondary structures. Document categorisation, for instance, implies supplementary structures, specifying authors, publication series, and so forth.

The general conclusion drawn from the study of requirements of legal information was therefore not only that these requirements are domain dependent, but also that situations in which law is to be used, together with the identity of the users, must be accepted as the point of departure in the design of legal IT-systems.

2.3 Technical aspects

The exploration of technical aspects revealed, in turn, that demands concerning legal information systems vary to a considerable extent, depending on the user situation and the working tasks to be performed. Another important observation was that differences in expectations can be related to all aspects of technology, e.g. computers, communication facilities, software performance, etc. The analysis furthermore indicates that the IT maturity of the users (or the potential users) is an important aspect that must be included in any evaluation of system performance in this area.

Rapid development is a factor which complicates proper evaluation of technical methods. It is evident that, apart from more or less obvious conclusions concerning such things as access to high-speed communication facilities, graphical interfaces, cut and paste standards, hypertext and clickable buttons, etc., it is useless to be more specific about technical standards. In this respect the pace of change is simply too fast and unpredictable.

In an investigation of methods one must also take into consideration the fact that at present several different technical standards may provide satisfactory solutions. It is, for instance, obvious that CD-ROM products and on-line databases can both provide feasible storing and retrieval tools for professional lawyers, which is even more apparent when different software products are investigated. In the process of evaluation, however, it is not possible to foresee which standards will survive, and which will be replaced by new techniques and new technical solutions.

When technical aspects are scrutinised, it is nevertheless noticeable that a number of jurisprudential and practical presuppo-

sitions must be taken into consideration besides pure technical components. The complexity of legal information, for instance, may make it necessary to prioritise functions that may facilitate overviews. For similar reasons simplicity and focus on introduction facilities will always be crucial when a certain system is being evaluated. Likewise, for on-line applications 24-hour access, continuous assistance, e.g. in the form of a help desk, frequent updating of the content, print-out facilities and similar aspects are likely to be requested by a large majority of professional users in this area. These details suggest in turn that it is realistic to predict further development of computer-based legal networks, and that communication facilities and interoperability of systems are important components of investigation when various legal information systems are compared.

In a survey of technical aspects it is also relevant to remember that the analysis of legal requirements indicates that advanced legal information systems should be able to handle not only legal documents and legal texts, but also smaller components, such as legal rules, rule systems, and legal concepts of various kinds. This also makes it obvious that legal information applications will develop from pure IR-systems and simple administrative systems towards applications with much more integrated functions.

An additional factor to be considered is the fact that all lawyers will differ to some extent in their opinions about the law. This in turn makes it possible to predict that most users will be likely to appreciate customised systems rather than general-purpose systems, which is why in an evaluation of various suggested solutions priority should be given to applications that are open to such solutions.

2.4 Organisation

The third aspect of legal information systems included in the model of evaluation – *the organisational component* – focuses attention on several fundamental, but perhaps less frequently observed, aspects that may be relevant to look into when a legal information system is to be investigated.

The factors that can be related to organisational components are numerous, but in the completed analysis two aspects appeared to be more important than others, *viz.* stability and competence. Stability is necessary, since all professional use of a legal information system is likely to presuppose investments in terms of time, money, and education. From this it obviously also fol-

lows that it is desirable for the service to be of a permanent character.

The stability of a certain organisation, e.g. a publisher or a database provider, is, nevertheless, difficult to measure and predict, especially in a long-term perspective, but it can be estimated to some extent by means of studying components such as the future plans, the size, and the economy of the organisation.

Competence, in turn, is a generic concept covering a number of aspects ranging from legal proficiency, technical competence, and combined skills concerning all aspects of legal information systems. Competence thus perceived is not only of the utmost importance when legal information systems are to be designed, but is also a crucial element when a legal information system is to be integrated into the work process and, of course, when a system is to be managed over a longer period of time.

Competence being such a broad concept, its evaluation may sometimes be quite difficult and time-consuming. Then again, various aspects are of such a kind that their evaluation is only possible over a certain period of time. When this aspect is investigated, it may, nevertheless, be relevant to try to investigate components such as flexibility, service, etc.

Finally, the analysis of factors relevant to legal information systems shows that the investigation combining information content, technical aspects and organisational issues illustrates how a feasible model for the evaluation of legal information systems, IT products and services can be developed. It should also be noticed that the model of evaluation outlined in this study can be used not only when various legal information services are to be scrutinised and compared from the user's point of view, but that it can also be used by the legal information system designer, as well as the legal information manager.

3 Conclusions and future work

In this study some approaches have been described that may be utilised in order to evaluate legal IT-systems. The focus of attention has been on system components (content, technical aspects, organisation), user requirements and various external factors. The objective has been to provide the means for the critical and consistent scrutiny of the products and services that are being developed.

In this respect the model of evaluation based on information content, technical aspects and organisational aspects can be char-

acterised as exhibiting an *overall structure* facilitating more systematic investigations. It is also noticeable that the model is *general* in the sense that it can be used for evaluation of legal information systems of various kinds, and that it reflects components that can be accepted by scholars of different traditions.

In addition, it may be suggested that the model is *transparent* in the sense that the components can be described in a non-technical way, and that all legal and technical terms can be explained as they appear. It may furthermore be claimed that the model is *explicit* and *particular* by means of providing a basis for the elaboration of more or less stepwise specifications. It is also apparent that the model is *flexible* since it can be modularised in such a way that one or more components can be changed, elaborated upon, omitted, etc. without disturbing the overall structure of the model.

For the future, however, it is important to take into consideration the fact that the rapid development of IT and telecommunications, as well as the increasing internationalisation of law, necessitate revision and adjustment of many of the more detailed aspects of the employed method. Likewise, it may be concluded that this must be done more or less continuously. Additional factors to be considered in this context are the growing competitiveness and increased commercialisation of the legal information market.

Another, obvious, conclusion from the above is that enhanced and up-to-date knowledge of IT-components and various types of user requirements will continue to be important when various products and services are to be evaluated .

In the long-term perspective, however, it may be argued that one should be even more ambitious, trying to utilise the results of the analyses and evaluations in a broader sense. Most important in this respect appears to be that it is desirable that the analyses include *development methods* for legal IT-systems, as well as *long term effects*.

The need to include development methods in the discussion is motivated by the obvious fact that there exists a close relationship between the characteristics of legal IT-systems and the various strategies and methods that are employed in order to design and develop them. This is just another way of saying that it should be important to scrutinise, among other things, the ways in which preliminary studies are completed, organisational analyses carried out, and legal sources selected, adjusted and transformed. Likewise implementation strategies and educational activities are relevant to scrutinise in order to minimise problems with user acceptance.

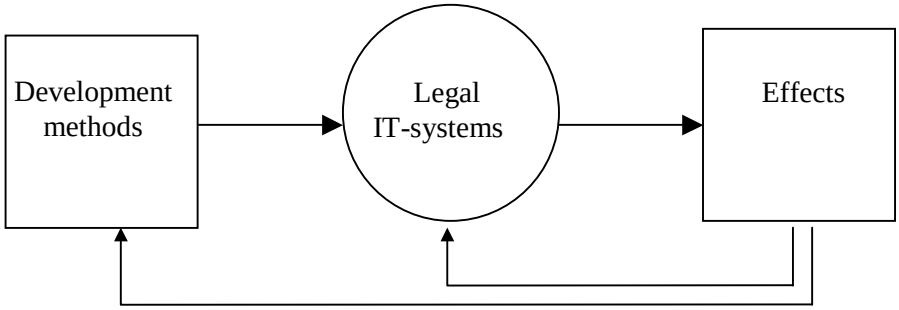


Figure 2: An evaluation of legal IT systems with any practical ambitions should include not only system components of a tangible nature but also system development methods and effects.

Similarly, the necessity of aggregating and systematising knowledge about the effects of legal information systems follows from the fact that it is important to understand the ways in which various legal IT-systems affect the legal community. In many situations it is quite clear that legal IT-systems are likely to have a considerable impact on the way legal work is carried out. Likewise, the ways in which the systems are designed and utilised may affect the substantial aspects of law, and for obvious reasons it is also interesting to understand and try to manage these consequences. In this wider perspective, the nature of investigations that have to be completed differs depending on the situation. When a legal IT-system is implemented in a teaching organisation, for instance, it is natural to investigate whether the system has had a positive effect on the actual learning, how the course administration and the teachers' resources have been affected, and so forth. Likewise, it is relevant to scrutinise the economic consequences, the emerging legal problems, the effect of IT investments on the future plans and flexibility of the organisations.

Another reason why the study of effects appears to be a crucial issue is the obvious fact that in many situations it may be necessary to regulate the consequences of legal IT-systems in order to vindicate various kinds of legal quality aspects.

A final insight from this study is that legal sources via IT constitute very complex phenomena with far reaching consequences. It is thus obvious that IT is having, and will continue to have a profound impact on the legal profession, revolutionising the quest for law. It should be underlined, however, that this development will not result automatically in enhanced quality and better efficiency in the legal sector. An increased complexity, which the subject matters addressed in this study doubtlessly represent, is also something that is likely to be reflected in the number of things that may create problems. From this in turn follows

that all lawyers must be prepared to elaborate their critical attitude, and be able to actively evaluate legal information in a very cautious way as the development continues

Ulf Maunsbach*
Alternative Dispute Resolution – The Features and the Future

1 Introductory remarks

During the past few years there has been a growing interest in different alternative dispute resolution models capable of working through the Internet (for a definition of the term ADR-online, see section 2.1). The discussions are not confined to Internet enthusiasts: interest is growing among decision-makers as well. One example of this is the Directive on electronic commerce, Article 17 of which addresses alternative dispute resolution.[1] Another is the Swedish government, which in its plan of action for consumer policy between 2001 and 2005 highlighted alternative dispute resolution as a possible solution to upcoming problems on the consumer market due to new technology.[2] Similar questions are discussed by WIPO, which already has operational alternative dispute resolution services functional through the Internet. On example is the WIPO Internet Domain Name Processes.

The question of alternative dispute resolution and its prerequisite was furthermore discussed during WIPO's conference "Forum on Private International Law and Intellectual Property" in Geneva, January 30th 2001. Among the reports from the conference, which can be found on-line at http://www.wipo.org/pil-forum/en/, I would like to mention the one performed by H. H. Perritt, "*Electronic Commerce: Issues in Private International Law and the Role of Alternative Dispute Resolution*".

In Geneva there is also an ongoing research project, the Geneva E-law project (http://www.online-adr.org/), conducted by the Private International Law Department of the Geneva Univer-

---

* *Ulf Maunsbach*. L.L.M., is a doctoral student at the Faculty of Law, Lund University. His research is focused on the interaction between intellectual property rights and private international law and will result in a dissertation regarding, in particular, issues arising from trademark infringements on the Internet.

1 See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, OJ L 178, 17/07/2000.

2 See Government bill 2000/01:135, *Handlingsplan för konsumentpolitiken 2001-2005*.

sity Law School with the aim of evaluating existing ADR-online systems and formulating recommendations for the improvement of upcoming dispute settlement mechanisms using information technology.

When glancing through the sources mentioned above, it is easy to conclude that the Internet society demands alternative dispute resolution. It is easy to promote the development of different resolution services, but it is also quite easy to forget the question of whether or not an average Internet user really demands all these different alternatives. Is it conceivable that a private-based dispute resolution might prevent individuals from getting their rights judged before a competent court? Is it possible to think that the development of private-based dispute resolution might lead to a veritable jungle of different dispute resolution systems impossible for the average Internet user to comprehend? Just as I believe alternative dispute resolution in many cases to be *necessary* for the development of the Internet marketplace, so I believe it to be *possible*, not least because of the development of a wide range of different dispute resolution services reaching out to consumers. However, there are problems in the consumer sphere. They are highlighted by Consumers International in a report about alternative dispute resolutions available online to consumers in cross-border disputes. In part this report supports the conclusion that consumers are not likely to be able to count on ADR-online systems offering adequate redress.[3]

As a consequence of the problems mentioned above I think that the development of new dispute resolution systems must be demand-based. The question whether or not there is a demand for an alternative (to traditional administrative and judicial procedures) is, in my opinion, sometimes forgotten or omitted in the on-going discussion about alternative dispute resolution. This short essay is an attempt to highlight this potential problem. I will not be particularly consumer-oriented in my presentation though. Instead I'm going to use a present Swedish example, the suggested introduction of an ADR-online system for the Swedish top-level domain .se. My hopes are however that the findings will be applicable on a more general level, for instance to the problems on the consumer area mentioned above.

[3] The report can be found on-line at www.consumersinternational.org.

2 The features and the future

2.1 What is ADR-online?

Before going into any further detail about my thoughts on this subject, it might be appropriate to mention something about what ADR-online is, or more correctly how I define the term for the purpose of this paper. I have no intention of presenting a new "wall-to-wall" definition, but still there has to be some kind of common starting point. To begin with, alternative dispute resolution can be considered to be something other than traditional administrative and judicial procedures. Furthermore, resolution has to be based on electronic communication to be regarded as ADR-online. This adds up to the following definition:

> Alternative dispute resolution online is a procedure different from traditional administrative and judicial procedure, in which disputes can be solved through the Internet or any other similar network.

This definition embraces numerous variations of proceedings. For instance, systems related to arbitration, mediation and various forms of evaluations or negotiations with the intention of binding the disputing parties on a voluntary basis. I will neither have the time nor the space to evaluate the differences in this paper though. Instead I refer, for further reading, to the comprehensive report from the Geneva E-law project *"Online Dispute Resolution: The state of the Art and the Issues"* conducted by T. Schultz, G Kaufmann-Kohler, D. Langer and V. Bonnet.

2.2 What is a successful ADR-online?

Even though the proceedings differ, I think that they have certain points in common.

The parties who are expected to use the ADR-online system must have confidence in the system. There are various ways of building confidence into an ADR system. One can talk about due process and openness, one can talk about the competence and independence of the mediators/arbitrators but nothing, in my opinion, is as crucial as the preceding discussion about demand. If there is no demand for a planned or newly launched ADR-online system, I can guarantee that success will fail to appear.

Demand can be a lot of things, and therefore the way of extracting it may differ. To simplify matters I have chosen to ex-

tract the most impending demand to a discussion about sanctions. In line with that I think quite a good demand-estimate would be accomplished by answering the following questions:

- Are the dispute resolution demands as regards sanctions fulfilled in the traditional judicial and administrative proceedings?
- If not – what is missing – what are the sanctions demanded?
- Is it possible for the ADR-online system to cure this unsatisfactory state of affairs; i.e. is it possible for the ADR-online system to decide upon those sanctions?

2.2.1 Are the dispute resolution demands as regards sanctions fulfilled in the traditional judicial and administrative proceedings?

The starting point in a discussion about ADR-online must, as mentioned above, be what kind of demands this alternative is supposed to fulfil. This demand ought to be derived from a shortage in the existing systems of judicial and administrative proceedings.

In the area of domain name registration there has been a history of name-napping and trademark infringement. This is an activity mainly concentrated to top-level domains with the characteristics of openness, that is top-level domains where domain names can be registered without any preceding control of intellectual property rights.

In January 2000 a dispute resolution service aimed, among other things, to solve problems with name-napping was introduced. The procedure was named “the Uniform Domain Name Dispute Resolution Policy” (UDRP) and was meant to be used mainly for solving problems in the generic top level domains .com, .net and .org. By now the system has proven to be a great success. At the time of writing more than 4,000 cases have been decided, thanks to the UDRP.

In Sweden there is an on-going discussion as to whether or not a system like the UDRP shall be adopted for the Swedish top-level domain .se. In line with my observations stated above, the first question must be whether there is a demand for that kind of system for the Swedish top-level domain and whether the demand can be met within the frames of the traditional judicial proceedings. Ultimately the demands in a domain name dispute are the transfer of the domain name from the holder to the plaintiff. This kind of transfer is easily accomplished in a traditional judi-

cial procedure and therefore one can argue that there is no demand of an ADR-online system. The truth might be more nuanced, though.

In the introduction to the report mentioned above, Perritt points out a variety of demands, i.e. arguments promoting ADR-online. For the purpose of this paper I have chosen the three demands I conclude to be most imminent:

1. The transaction cost of a traditional administrative judicial procedure is high. In a world where the value of the underlying transaction is low, victims tend to be less likely to seek vindication. ADR-online can be inexpensive, at least by comparison with traditional judicial proceedings, and thereby satisfy the interests of the victims in getting a dispute resolved with transaction costs not outweighing the value of the underlying transaction.
2. The Internet is by nature global and an Internet user can easily be anonymous in a world without borders. Traditional judicial proceedings often depend on localisation to determine jurisdiction. This makes the questions of jurisdiction somewhat unpredictable. A more foreseeable situation might be created by the help of ADR-online.
3. Another problem with the traditional judicial proceedings is that the decisions are difficult to enforce outside the jurisdiction of the deciding court. Enforcement between nations requires some kind of agreement, agreements which are quite uncommon. If private parties mutually agree to abide by the decision of the ADR-online system there might definitely be a demand to satisfy.

As regards the development of an UDRP for the Swedish top-level domain I am not certain whether or not such circumstances are at hand. If one suspects a lot of upcoming problems with name-napping in the .se domain it is likely that there will be disputes. In that sense there might be a demand for alternative dispute resolution services. Considering the low price of domain names and the following low cost of the transaction there might at least be arguments in favour of the first condition stated above.

2.2.2 What are the sanctions demanded?

As mentioned above, the parties are likely to demand an enforceable decision. The question of whether or not a decision is enforceable is influenced by which sanction the parties are demand-

ing. The sanctions relevant here are of course private-law-based, but even when this is the case there are a variety of possibilities. The problems could be illustrated with a consumer buying an object that leads to product liability. If the essence of the dispute is whether or not the consumer should be given replacement goods, it might very well be solved by an ADR-online system, but the question of product liability lies, in my opinion, outside the possible range of an ADR-online system. This last question must be solved in a traditional judicial procedure because of the far-reaching nature of the sanction and, consequently, an increased requirement of due process.

When it comes to domain name disputes the plaintiffs are, as mentioned above, mainly interested in a transfer of the domain name. The "sanction" in this case would in other words be a domain name transfer.

2.2.3 Is it possible for the ADR-online system to decide upon those sanctions?

In general the main problem for ADR-online systems is that the sanctions demanded are not at the disposal of the dispute resolution service. In such a situation you are dependent on the good intentions of the losing party. There are various ways to bind the losing party to the decision of an ADR-online system, but in a situation where you are dependent on the voluntary compliance of the parties you always risk defectors. Defectors tend for their part to undermine the confidence of the dispute resolution service and thereby threaten the future success of the ADR-online system.

This is not the case, however, with the "sanction" demanded in our example. A transfer of a domain name is enforceable within the framework of the ADR-online system. It is easy to accomplish as long as the actors in control of the domain name servers comply with the decisions. A transfer of a domain name means, putting it simply, that the stated domain name holder in the domain name server alters and you do not need the consent of the prior holder to do so. In other words it is perfectly possible to create an ADR-online system which really can satisfy the demand of an enforceable decision in this field.

I think that the reason why the UDRP has proven to be so successful is the fact that it is possible to get what you want within the frames of the system even if the losing party does not respect the outcome of the dispute. Conversely, this is the biggest

threat to the development of functional ADR-online – the difficulties of meeting the demand for enforceable decisions.

3 Final remarks

As you have probably already concluded, this paper is not a comprehensive documentation over ADR online. Nor is it a thorough investigation of the judicial risks at stake, but rather a few thoughts on the road to a more balanced discussion about ADR-online, which no doubt is a important part of the future dispute resolution regime.

In general I agree with most of the findings in the reports from the WIPO conference in Geneva and the Geneva E-law project. We cannot only discuss details about how to build functional ADR-online systems though. In my opinion, which is in no way contrary to the reports, there must be a preceding discussion about whether or not the alternative dispute resolution is demanded in the first place. Demand in this sense is a prerequisite for a functional ADR-online system. The demand ensures that the ADR-online system will be used and a frequent use builds confidence.

When it comes to my example, the introduction of an ADR-online system for the Swedish top-level domain, I do not think that the demand is high enough to motivate a new dispute resolution system. For the purpose of this paper that is of minor interest, however. The important thing is that the questions of demand should be raised and examined before an ADR-system is introduced.

Björn Larsson*
Courts of the Future

1 Introduction

In this presentation I will deal with various aspects of the use of IT in the courts. By way of introduction I will give a very brief description of the existing IT support system. Thereafter I will present some important premises for the work which is in progress on the further development of IT support in the courts. In conclusion I will outline some opportunities for the development of working methods and forms of organisation in the courts with the support of an improved IT-based operational support system.

2 Current IT-support in Swedish courts of law

Swedish law courts today present a great diversity of IT support. There are general systems which have been developed jointly for various types of court, and solutions which have been developed specifically for a certain type of court.

The lower courts, rent and tenancy tribunals, district courts and county administrative courts have had the support of the MÅHS system since the beginning or middle of the 1990s. This is a case management system which primarily supports the more administrative elements of case management. It is logically and physically located at the individual court and there is no real integration between the different courts' systems. There is no possibility of information pooling between different courts or lower courts. MÅHS was developed to support the working methods and forms of organisation that were normal at the time when the systems were developed. This, for example, has made it difficult to change operations that have used MÅHS as the tool. Thus, MÅHS provides good support to the courts in respect of case management but restricts the scope for adapting the system to new working methods and organisational forms.

---

* *Björn Larsson* is an associate judge of appeal. Since 1999 he has been engaged by the National Courts Administration to work on the development of IT-support in Swedish courts. He has also taken part in work by Government committees on organisational matters in the courts and in other state and municipality organs.

Since the 1970s, the administrative courts of appeal and the Supreme Administrative Court have had a uniform system which is completely different from MÅHS. The system, Imdoc/Find-IT, actually lacks any support for case management (MÅHS's strong point). The emphasis is instead on information-searching for the judges. The system is integrated between the courts and it is possible to search for information not only in the individual court, but in the other courts too. The city and district courts can also access the information in the system. Information about cases is stored in a common database which is managed by an external company. The system is a great aid to the judges when they are searching for similar decisions in their own court and in other courts. Searching for similar cases is likely to benefit the uniform application of the law.

Other courts of law, courts of appeal and the Supreme Court have different solutions with varying support systems for case management.

In addition to the system described, the employees of the courts also have extensive personal IT support available. This consists of support for word processing, calculation, e-mail and information searching via the Internet and in own information databases, for example the library system.

3 Some premises for the further development of IT support in the courts

Work has been in progress since 1999 to develop a new IT-based operational support system for the courts of law. The new system (VERA) is being developed on three levels. The platform or bottom level of the system is a database from Oracle. The intermediate level, business logic, is programmed in Java and the user interface is based on JavaScript and html format. Each court has its logically demarcated part of the database which is physically located in one place. The Swedish courts access the information via the judiciary's Intranet. I will not go into further detail with regard to the technology of the system design or the content of the operational support. I will just point out some significant aspects which are central for the development of the new operational support system.

3.1 When will things return to normal?

Society, of which the courts are a part, is undergoing constant change and development. With society constantly changing, the courts of law must understand and adapt to this change in order to be able to fulfil their tasks in the judicial process. Changes in the surrounding world will lead to changes in the courts. What form these changes will take and what impact they will have on the work of the courts is almost impossible to predict. What is important is to be aware that changes will come and to be prepared to constantly re-evaluate how the work of the courts should be carried out. The answer to the question in the title of this section is therefore that "Things will never return to normal". The normal is the state of constant change. This must be a cornerstone in the development work. The result should be flexible IT solutions which do not make the necessary operational development more difficult.

3.2 The goals of the court system

The courts of law are independent authorities and the Swedish Government, the National Courts Administration or others should not involve themselves in how courts rule in individual cases. Therefore, the IT support system must not be designed in such a way that the independence of the courts in their judicial process is affected.

Each year, the Swedish Government sets targets for the judicial sector in terms of throughput time (time taken to deal with a legal case). The courts' operations are also analysed on an annual basis in order to provide input data for the allocation of financial resources between them. A well-developed IT support system can be used to help the courts to achieve the goals which have been formulated for their operations and can also be used in the analysis of the operations themselves.

The overall goal of the judicial system can be described and measured in a variety of ways. In simple terms one can say that the goal of the judicial system is to determine cases quickly and with high quality. The goal of the system is thus concerned with the result as the parties, legal representatives, witnesses, aggrieved parties, media, citizens etc. experience it. The work of developing the new operational support system is based on the task of the courts being to satisfy the demands of these external groups, demands which can be formulated on the basis of legislation. For the sake of simplicity, I will hereafter refer to these ex-

ternal interests as the court's clients. The word "client" can appear somewhat misleading, but it works well when analysing the operations in order to develop an IT support system. The "client" concept also works well when using the IT support system as a tool for change. The word "client" does not fit so well in respect to managing individual cases and is wholly inappropriate as a term in respect to judgements and court decisions. The external parties concerned are therefore not called clients in the IT-based operational support system.

IT support shall be designed in such a way that it provides the greatest possible value to the courts' clients. By focusing on developing an IT support system which creates the greatest possible client value, the courts will at the same time obtain an efficient support system. Issues in respect to the courts' internal organisation and working methods can never be put first when designing IT support. Organisation and working methods are means to the ends which have been defined. Furthermore, they are always changing.

What is easy to quantify and describe is the part of the goal which consists of time, i.e. the time that it takes to arrive at the court's decision. Another aspect is the quality of the decisions. This is more difficult to quantify but some guidance can be obtained by looking at factors such as the frequency of appeals submitted and the frequency of successful appeals.

3.3 Business process re-engineering as a method

In order to be able to meet the clients' demands on the judicial system and provide the courts with opportunities to create as great a client value as possible, we use a process-orientated working method in order to further develop the courts' IT support system. The method has been originally taken from industry and has been adapted to public organisations. The operational method comprises identifying processes based on the type of clients, analysing the processes and making conclusions. It is only thereafter that one can address the consequences. One of the consequences is developing the new IT support. Another consequence is adapting working methods and organisation so that the greatest possible client value can be created. This work, however, has to be done by the individual courts. A basic prerequisite for the work on the new IT support system is that it shall facilitate efforts to change working methods and organisation, but the support cannot be designed in such a way that it forces a change in methods of operation.

3.4 Existing technology – Is it possible to create a judgment with the aid of a mobile phone?

The rapid rate of IT development in recent years has given us good opportunities to utilise existing technology, and more or less developed solutions. Before starting to design a modern IT support system a number of questions must be asked about the operations. We have utilised the process-orientated work method to do this.

The questions that should be asked are why a certain operation is being carried out, what is being done and what should be done, and finally how it should be done. It is really only with the last question that the new technology and its possibilities come into the equation. Thus it is not possible to begin by looking at the opportunities offered by the technology, otherwise one could imagine that a judgement could be written with the aid of a mobile phone. This is actually possible, but the idea of designing an IT support system to act in this way will not arise if its has been asked why the operation is carried out and what should be done, at the same time as the value to the client has been kept in focus. (Mobile phones can be used, for example, to distribute court judgements in real time to parties if they so desire, but that is another matter.) It has been a common mistake, though, in many development projects to focus on the opportunities presented by new technology, while paying less attention to the requirements of the clients and the operation in question. The work of designing a new IT support system must therefore be undertaken by people who are knowledgeable about operations in co-operation with people possessed of IT expertise.

4 Possible development

In this section I will discuss some possibilities for developing the court system with the aid of an improved IT support system. I will first deal with issues concerning the organisation and working methods of the courts and then issues concerning information management.

4.1 The internal organisation – The court's prioritisation of its work

In the above section I have pointed out the significance of the client's perspective in the development of the new IT-based operational support system. This perspective can also be used in the individual court and be the factor that guides planning and allocation of priority. With the help of the new IT support system the courts will be able to analyse the work facing them and to forecast case flow etc. on the basis of historical data. Such analyses and forecasts can then be used to plan and organise operations in order to achieve the greatest possible client value. I believe that the courts which utilise these opportunities will be organised and will work in a completely different way from that which has been normal in recent years. I will only raise a couple of aspects here in respect to organisation which may be handled differently if a client perspective is employed at the same time as a powerful IT support system is in place.

4.1.1 Division of the work within the court

The allocation of cases, and thereby the division of work, is normally carried out when a case arrives at the court. The allocation is thus made when it is known at least how much work will be required to deal with the case. This is often done primarily among the judges as the courts strive to achieve an equal distribution of work, and as this shall also lead to fairness for the clients. A well-developed IT support system can also provide more scope for taking the clients' requirements into consideration when allocating the work within the court. The allocation of the work can be done at several different times and can relate to other factors than the complete case management. An initial allocation of the work should be complemented by the opportunity for re-allocation and redistribution of goals and work assignments. This can be done with the aid of planning tools which can be used successively as it becomes known to the court how much work the case actually involves. The basis for allocating work within the court system can be done better than is usually done at present.

4.1.2 The organisation

A case is often allocated to an organisational unit, usually a department, which handles the case from beginning to end. The norm is that the case remains with the same department all the time it is being dealt with in the courts. This can almost be compared to actually dividing a court up into a number of smaller courts with a more or less well-developed degree of co-operation. The development in other areas of society is heading in the direction of larger units with more flexible organisations. I believe that the courts will follow in this direction and go from acting as individual proprietor enterprises to becoming large-scale enterprises. This development can be seen in respect to the external organisation where courts are merged to form larger units, but this must be followed by a corresponding change in the internal organisation in order to be able to achieve an increase in client value. With the aid of a modern IT support system, it will be possible for new organisational forms to be created without entailing any loss of control over the organisation. One possible development is that not all incoming cases are dealt with in the same way and in one joint organisation, different organisations instead being created within a court, depending on the amount of work required for the various cases.

4.1.3 The meeting with the client

In the operational analysis which was carried out as part of the development work on a new IT-based operational support system, the courts often returned to the issue of various elements which interrupt the planned operation. One such element which the court staff found annoying was all the telephone calls from parties etc. We discussed various solutions to this and suggestions were advanced, including limiting telephone time so that the work in court could flow better during working hours. Such a solution, however, is not exactly client-oriented. One should think instead in terms of a very important part of the work consisting in having contact with clients and informing them about what is happening in the case. This should be taken into account when considering how the work should be organised with the aid of an IT-based operational support system. The meeting with the client is important, and in this respect there are major opportunities for creating client value.

Existing organisations and work forms are often based on the client finding the right person in the court in order to obtain

answers to his/her questions. When the whole organisation has the opportunity to access information about all cases, opportunities are opened up for organising the meeting with the client differently. In other organisations various types of Call Centres are often used to deal with telephone enquiries. Such solutions require good access to information, which the IT support system can provide, and knowledge about the operation and authority within certain frameworks to act and provide information. I believe that there can be good opportunities to work with such solutions, even across court areas of responsibility. Many questions about case management can probably be answered and documentation provided by persons who work in several courts. This leads on to issues about the external organisation of the judiciary, and issues concerning the boundaries of responsibility between courts. I am convinced that the existing way of demarcating boundaries of responsibility between the courts can be improved if one means here improvements from the clients' perspective.

4.2 The new external organisation – The court district

IT support can be used in order to create a more flexible and client-oriented internal organisation. It must also be asked how the IT support may affect the external organisation or the country's division into court districts. The place where a case is to be dealt with is determined in accordance with the regulations in the Swedish Code of Judicial Procedure and other legislation. These regulations date from a time when today's opportunities for information management were not available.

For the client, the jurisdictional regulations are less important than other factors, for example the time it takes to bring a case to trial. The physical distance to the court does not have any significance in many cases. The majority of cases in the general administrative courts can be determined by written proceedings; the same applies to many cases in the appellate courts. I believe that the work of a certain court in the future will not be decided by where the disputes arise, but according to the capacity the court has to decide the case. I can imagine that a developed IT support system will enable more flexible jurisdiction regulations which will give the parties a greater say in respect to where the case shall be dealt with. Such a development will also be facilitated by new video technology which will enable witnesses and others to be in a physical location other than the premises in which the proceedings are being held. The opposite situation may also be possible in which the court's officials are located in an-

other place to that of the court room where the parties are located.

If, in this way, the clients obtain greater influence over where the case shall be dealt with, the work can be directed to where there is the production capacity. Elements of this can already be seen today when parties to agreements agree the legal venue where any future disputes shall be resolved. This could also be done in order to obtain rapid processing of a case or processing by a court where specialist knowledge is available.

The opportunities of directing the work to where there is production capacity are being opened up with the aid of the IT support system which will be implemented over the next few years. It will be possible, as I mentioned earlier, to allow the parties an increased say, but it will also be possible to manage the work in order to achieve the greatest possible client value otherwise. One example of such management may be that courts are given different profiles and will specialise in different areas of the law. The demarcations of the court's actual work content can thus be determined by other factors than the jurisdiction regulations. If work is determined according to production capacity, this will affect the way in which resources are allocated to courts. The current method of resource allocation is based on measuring the workload in different ways and allocating resources according to how much the courts have to do. The purpose of such an allocation model is not primarily to create client value but rather to create a more equitable allocation between independent authorities, in much the same way as efforts are made within a court to create an equitable distribution of cases among judges. The allocation of resources can instead be based on the client value that a certain court creates. This is close to a form of competitive situation between courts, and in other areas of society competition is said to create increased client value. This could be the case for courts and their clients too. There are even external competitors to the courts; legitimate in the form of arbitration tribunals, and illegitimate in the form of "enforcer" gangs and suchlike. Encouraging increased competition, both internal and external, with the aim of increasing client value could perhaps be tried and in that case with a new IT support system as a tool. Naturally, in such cases there are also other aspects to consider, such as the preservation of independence in the judicial process etc.

In the future, the demarcation between courts may become less rigid and the situation may approach that of a virtual court organisation where the work is not so rigidly linked to the physical unit which currently constitutes a court. From the client's perspective it could for example be possible to have a court of ap-

peal for the whole country where the work is directed to various local organisations according to where production capacity is available.

4.3 Access to information about the court's activities

Traditionally all information relating to a certain case has been managed in a physical file which is kept in the court. The parties have had access to certain parts of this information in the form of various documents. When the MÅHS system was introduced, this meant that certain information in respect of the case became available via the system internally within the court. The next stage is to open up the system and thereby to make the information concerning the case accessible outside the court as well. This also touches upon issues regarding the way in which the court meets the client. I would like to indicate some possibilities in this respect.

4.3.1 The parties' access to relevant information

The parties in a case should have direct access to such information concerning the case as is to be found in the operational support system. This could be compared with the access a bank customer can gain via an Internet bank. It is thus a question of being able to obtain information in real time about what is happening and about being able to provide information to the court. The parties should thus be able to go directly into their case and see the relevant information via an Internet service or other method. It may be difficult to give a party access to all information that the court has about a case. An example of such a situation could be direct access to documents which have been submitted to the courts. These documents may contain information which is confidential, and it is not reasonable that all such confidentiality issues shall be solved in advance and that all documents be checked by the court before they are made available to the parties. It is probable that the party can be given the information that the document exists, when it was received and who submitted it, and thereafter have the chance to order the document. Only at that stage will the court make an assessment of the confidentiality issue, and normally it should be possible for a document to be distributed, for example via e-mail, relatively promptly (provided that the court is organised to meet these client demands). The parties should also be able to provide information to the court di-

rectly via an Internet service or suchlike, and thereby to co-defendants or opposing parties. There may also be opportunities to allow the parties to submit a large part of the information which is required in order to register the case, for example the prosecution in a criminal case can submit practically everything that is required in order to initiate case proceedings in the court.

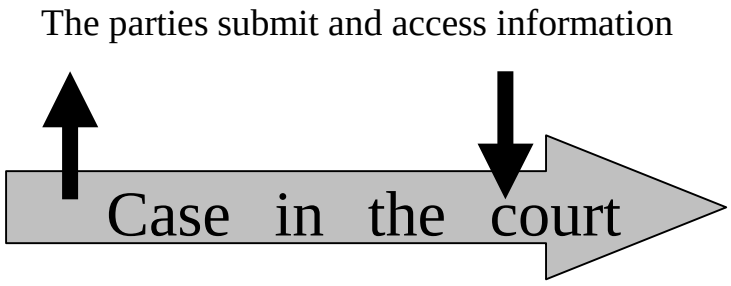


Figure 1: The information flow in a case

4.3.2 The information flow between courts – cases on appeal

When a case is appealed, the physical file is sent to the higher court. At present the file is the completely dominating information carrier for the higher court. With a new IT support system the information flow can be integrated between the courts so that one can look up and down in the court chain in order to find out what is happening to the case on appeal. This provides opportunities to recycle information about basic case details.

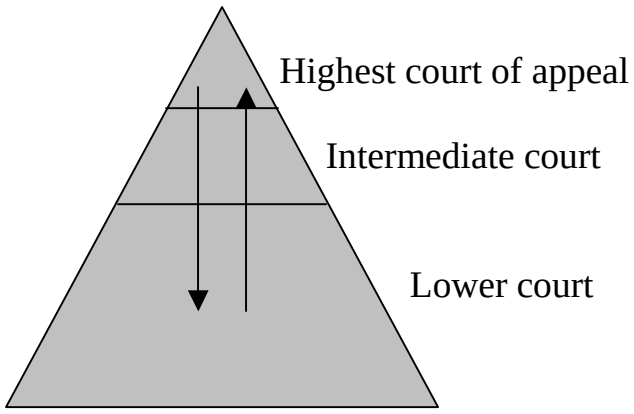


Figure 2: The information flow between courts

If the information is integrated in this way between the courts, completely new opportunities of making court rulings public will

be created. It is easiest to see this in respect to criminal cases. In order find out what the result has been of a criminal case in the appellate court, at present a party may need to obtain the following elements of the court of appeal's ruling:

- The prosecution's statement of the crime as an appendix to the judgement of the court of first instance.
- The judgement of the court of first instance.
- The findings of the court of first instance.
- The appeal as it has been noted in the appellate court.
- The judgement of the appellate court.
- The findings of the appellate court .

Except for the findings of the court, this is a question of structured information which can be handled together with the aid of a developed IT support system. The result of the verdict of the appellate court could be a summary of the structured information where it is stated how this has been altered from the prosecution's statement of the crime right up to the appellate court's judgement. I believe there are major opportunities here to create greater client value with the aid of the IT support system without actually affecting the content of the courts' work: it is just a better presentation of the result compared with the present set-up.

4.3.3 Other flows of information between courts

There is a need for direct access to information about other courts' cases even in other circumstances than when a case is being appealed. The administrative courts of appeal and the Supreme Administrative Court have had a well-developed system of this kind for a long time now. It is used above all by the judges in order to search for similar decisions, a situation which must be deemed of benefit in attaining a uniform judicial application. There are also elements of this in the general courts but there the methods are not so developed as in the administrative courts of appeal and the Supreme Administrative Court. For example there is a certain exchange of this type in that certain reports of proceedings with reviews of decisions are sent to other courts. There are good opportunities in this respect to allow courts to have access in real time to at least meta data concerning the decisions of other courts. It is possible to solve this from a technical perspective, what it is important to focus on is obtaining good quality

levels in respect to the information that is to be made available to others.

4.3.4 Division of work between the court and the parties

When the court and the parties have access to common information in respect to the case in real time, opportunities are created to work in other ways than the traditional ones. The boundaries of the responsibility of the court and the parties respectively can be called into question and new solutions sought. It is difficult to see the direction in which this development can go, but with shared information and transparent systems it should be possible to find more expedient solutions that the ones in use at present and which are largely based on paper-bound information or on attending court in person. I can imagine that development may go in the direction of the parties assuming a greater responsibility for progressing the case, for example through greater involvement in the planning. This could take the form for example of the prosecution, which provides the court system with the greater part of the information required for the management of the case, also planning and summoning the defendant to pleadings/proceedings in the court. In such a situation the court should provide the resources to adjudicate upon the case – premises, equipment etc. – and the prosecution will have the responsibility of booking these resources within given limits.

Another possibility could be to use the court's system and the common information in the system as a platform in order to try to resolve disputes prior to initiating proceedings. The parties should be able to use the court's system for example for conciliation discussions, with or without the active participation of the court.

5 Concluding viewpoints

Now that a modern and transparent information management system is being introduced in the courts over the next few years, we will have opportunities to change and improve operations for the benefit of the courts' clients. The new IT support system, however, will not automatically lead to anything other than marginal effects. We are now facing a greater task than just the development of IT support. It is a question of utilising the opportunities which are created. In this respect the courts need to be prepared to analyse and re-evaluate their working methods and also to im-

plement major changes. Only then will we really benefit from the investments which are now being made in an IT-based operational support system. If the present court organisation and working methods are retained, the benefits will be marginal.

Annex 1
The IT Law Observatory

Peter Seipel
has chaired the IT Law Observatory since its creation in 1996. He has also been a member of the Swedish ICT Commission since 1994 and its vice chairman since 1998. He obtained his doctor's degree in 1977 at the Faculty of Law, Stockholm University. His thesis, "Computing Law. Perspectives on a New Legal Discipline", argued for the advantages of a broad, systematic, and interdisciplinary study of the interaction of law and information technology. In 1982 he was invited to a chair in "legal informatics" at the Stockholm law faculty with national responsibility for the development of study and research programmes in the field. He has been engaged as an expert by both government and industry. Among other things, he has served on various study groups and committees of the World Intellectual Property Organisation, the Organisation for Economic Co-operation and Development, the Council of Europe, and the European Union. His published works include "EDP and Law. An Inventory of Issues" (in Swedish, 1975), "From Data Protection to Knowledge Machines" (1990, editor) and "Law and IT" (in Swedish, 7th edition, 2001).

Kjell Skoglund
has worked as Senior Project Manager with the Swedish ICT Commission since 1995. His main responsibility has been the IT Law Observatory. He obtained his law degree at the Faculty of Law, University of Uppsala in 1981. He has served as secretary with several Swedish Governmental Committees, among them the Committee on Health Care Data. He is also a judge at the Administrative County Court of Västernorrland.

Joachim Benno
Director of Regulatory Affairs at Telenor Plus, has been a member of the IT Law Observatory since 1996. He has been working with ICT-related legal issues since the end of the 1980s and functioned as Principal Secretary to the Swedish Committee on Media Convergence (1997-1999). He is the author of "Consumer Purchases through Telecommunications in Europe - Application of Private International Law to Cross-Border Contractual Disputes", CompLex 4/93 (Oslo: Tano, 1993), "Ytringsfrihet - en konstitusjonell utfordring?" (Fredrikstad: Institutt for Journalistikk, 1994) and the IT Law Observatory report 6/98, "The "anonymisation" of the transaction and its impact on legal problems - A theory as to why the use of ICT engenders legal problems". Areas of interest: Convergence, E-commerce, freedom of expression and information, telecoms, media etc.

Viveca Bergstedt Sten
has been a member of the IT Law Observatory since 1996. She has recently been appointed General Counsel and Corporate Secretary at the Swedish Post, and has previously served as General Counsel at LetsBuyIt.com and as

Corporate Legal Counsel at Scandinavian Airlines. Viveca Bergstedt Sten graduated from the Faculty of Law, Stockholm University, in 1986 and also holds a Master of Science from the Stockholm School of Economics, where she graduated the same year. She is a frequent lecturer in the area of "IT-law" and international business, and co-authored the book "Outsourcing of IT-services" in 1999 (with Magdalena Augustsson Öhd). Her next work will be published in 2003, under the title "Business Negotiations" and she will also be a contributor to a book tentatively titled "International Agreements", also to be published in 2003.

Peter Danovsky
obtained his law degree from the Faculty of Law, Uppsala university. His continued academic legal work includes studies at the Collège d'Europe in Brügge and at Columbia University, New York, where he obtained a LL.M degree. In 1981 he became a member of the Swedish Bar Association. 1988-1993 he was associated with the law firm Philip Lemans Advokatbyrå. Since 1993 he is a partner with the Danowsky & Partners law firm. Much of his work has involved media-related issues, in particular copyright and privacy protection. He has also been active in contract formation regarding structural matters in the media sector. In addition to numerous articles, his published works include books on, among other things, rights in pictures and a commentary to Swedish intellectual property rights legislation. Peter Danowsky joined the Observatory in 1996.

Malin Forsman
joined the Observatory in 1998. She has worked as a legal expert for the "Cultural Network Sweden", a project aimed at establishing an Internet portal for Swedish cultural endeavours. Later she has been employed by the Delphi & Co law firm where she has specialised in legal issues related to Internet publication, a subject on which she has also written a book, "Internetpublicering. En juridisk vägledning" (Internet Publication. A Legal Guide, 3rd ed. 2001).

Per Furberg
Having worked within different Governmental committees from 1988 to 1997 with the task to consider IT-related legal issues in different areas, e.g., civil law, procedural law, criminal law, and administrative law, Per Furberg was appointed District Court Judge in Gothenburg in November 1997. Today, he works at the law firm Setterwalls with IT related issues. Per Furberg has been a member of various international working groups. e.g., the OECD Group of Experts on Guidelines for the Security of Information Systems, the Council of Europe Committee of Experts on Problems of Criminal Procedural Law Connected with Information Technology, and the Council Of Europe Committee of Experts on Crime in Cyberspace. He has further been Consulting Expert regarding IT related issues in various projects sponsored by the European Commission. Per Furberg joined the Observatory in 1996.

Johan Hirschfeldt
is President of Svea hovrätt (Svea Court of Appeal), Stockholm, Sweden. He has earlier worked in the Office of the Parliamentary Ombudsman and in the Cabinet Office and served as Chancellor of Justice. He is a member of the IT Law Observatory since 1999. His main interest in the work of the

Observatory has been IT and its impact on judicial procedure, on the administration of justice, and on court administration.

Håkan Hydén
has been a member of the IT Law Observatory since 1996. He is educated both as a lawyer and a social scientist. He obtained his doctor´s degree in 1978 in Sociology of Law at the Faculty of Social sciences, Lund University. His thesis, ”The Societal Functions of Law”, entailed a comprehensive overview of the legal system. He has worked as a senior lecturer in Business law at Lund University where in 1984 he became docent (reader) in civil law at the Faculty of Law. Later on, in 1988, he returned to the Department of Sociology of Law, now as appointed professor (chair). Hydén has served as an expert in several public committees and has undertaken many missions especially in the field of human rights and development of the legal system. He is a member of several editorial committees, among them the Nordic Journal of Justice, Retfaerd, and the Italian Journal in Sociology of Law. During the first half of the 1990s he was a member of the Board of Trustees of Sida (the Swedish International Development Co-operation Agency). Hydén has written numerous articles and books on different subjects, such as environmental law and human rights. During the last ten years he has been interested in future studies, for instance in relation to self-regulation, information technology, and biotechnology. Hydén argues for Sociology of Law as a science about norms, for instance in his book, ”Norm science” (first published in 2002).

Katarina Högbom
works as Regional Counsel for IBM in the Nordic region. She obtained her law degree from the Faculty of Law, Uppsala University in 1980 and an LLM degree from Harvard Law School in 1982. Among other things, she is the chairperson of the legal council of the IT-företagen, a business organisation for the Swedish IT industry. She joined the Observatory in 1996.

Agne Lindberg
is a partner with the Delphi & Co law firm, where he heads the firm’s IT and Intellectual property group. His practice includes E-commerce, digital copyright, IT contracting and data protection issues. He is a member of the Swedish Bar Association since 1992. Agne Lindberg has been involved in Swedish and international organisations. One of the engagements was serving as a co-chair of the sub-committee on international transactions in the American Bar Association, whose main work resulted in a report on jurisdictional issues on Internet transactions. His experience also covers serving as a national expert in UN/ECE working group on E-commerce and OECD. In Sweden, he has been a member of the IT Law Observatory since its creation in 1996. He has also been a member of the legal council of the Swedish IT Trade organization. His published works include “Electronic Documents and Electronic Signatures” (1987), “IT Contracts” (in Swedish, 1991, “EDI, the law and the accountant” (in Swedish, 1992) and “Practical IT Law” (in Swedish, 3rd edition, 2001).

Christina Ramberg
(formerly Hultmark) is professor of Commercial Law at Göteborg University and holder of the Wiarda-professorship at the University of Utrecht. She

has been a member of the IT Law Observatory since 1999. She is chairman of the drafting group in the Study Group on a European Civil Code, Expert to the International Chamber of Commerce on e-commerce and to the EU Commission on B2B Internet platforms. She was head of the Swedish delegation in the UNCITRAL Working Group on Electronic Commerce during 1996-2001 and has been engaged as an expert on e-commerce to governments. She has written extensively within the fields of contract law and electronic commerce. Her latest book is "Internet Marketplaces – The Law of Auctions and Exchanges Online" (Oxford University Press 2002).

Nicklas Skår
joined the Observatory in 2002. He works for the Confederation of Swedish Enterprise with matters of IT law, company law, and environmental law. He has earlier professional experience from the publishing sector and the banking sector.

Hans Sundström
is Chief Legal Adviser of the Swedish Agency for Public Management since 1989. After obtaining his law degree at the Stockholm University in 1983, he worked as a Legal Adviser at DAFA, the Swedish data-processing centre during 1984-1989. In 1991 he served as Legal Adviser to the Swedish Telecommunications Administration. He is often engaged as an expert in the field of IT law in general, as well as in the area of administrative law, including e.g. legal automation. At present (2002) he is engaged by the Ministry of Justice as Secretary in the Working Group for removing legal obstacles to electronic communication and electronic processing. Previous commissions concern various working groups and projects, such as being Secretary in the Open Sweden Campaign (2000-2002). The campaign was run by the Ministry of Justice in order to improve knowledge of the Right to Access to Official Documents among civil servants and the public. Another task implied being Project Secretary of LEXIT in 1995; a Pre-Study on legal amendments necessary to accomplish an effective use of IT in public administration. Hans Sundström joined the Observatory in 1996.

Monique Wadsted
joined the Observatory in 1996. She is a business lawyer specialising in matters of IT and media law. Among other things, she is a member of the board of BitoS, a Swedish business organisation for players such as portals, on-line newspapers, service providers and other new media enterprises. She is a partner with the Magnusson Wahlin law firm.

B G Wennersten
joined the Observatory in 1997. He is a journalist and writer with a long experience in legal and economic matters of the IT society.

Kerstin Wiss Holmdahl
joined the Observatory in 2002. She works as legal advisor for the private law section of the Swedish Association of Local Authorities. She specialises in, among other things, electronic commerce, IT contracts, and intellectual property law.

Annex 2
References to documentary materials of the IT Law Observatory

Reports (in Swedish unless otherwise indicated):

1/97 ***Transaktionens anonymisering och dess påverkan på rättsliga problemställningar.*** (also in English, see below 6/98.) Joachim Benno.

2/97 ***Konsumentskyddet i informationssamhäll*****et.**
(Consumer protection in the information society. Documentation from a hearing.)

3/98 ***Cyberrymdens juridik – Lagstiftning och självreglering.***
(Cyberspace law – legal regulation and self regulation. Documentation of a seminar.)

4/98 ***Mobila agenter.***
(Mobile agents. A discussion of legal aspects of agent technology.) Erik Woodcock.

5/98 ***SPAM!?***
(SPAM!? Documenation of two seminars on a new phenomenon and its legal consequences.)

6/98 ***The "anonymisation" of the transaction and its impact on legal problems***.
A theory as to why the use of ICT engenders legal problems.
Joachim Benno

7/98 ***Fri aktör, egenanställd, ny daglönare!? (I)***
(Free agent, self employed, new day-labourers!? Documentation from a seminar.)

8/98 ***En missbruksmodell***.
(An abuse model. A discussion of new strategies for personal data protection.)
Per Hammarstedt

9/98 ***Rättspolitik på IT-området – ett diskussionsunderlag***
(Politics of law in the IT area. A report.)
Daniel Westman

10/99 ***Teknikoberoende yttrandefrihetsreglering?***
(Technology independent regulation of freedom of speech. An analysis of recent developments in Swedish law.)
Martin Brinnen

11/99 ***Fri aktör, egenanställd, ny daglönare!? (II)***
(Free agent, self employed, new day-labourers II. The present situation and needs for action.)

12/2000 ***Ledningsrätten i IT-tider***
(The law of conduits in the IT era. An inventory of issues.)
Anders Victorin and Barbro Julstad

14/2000 ***Elektronisk handel och indirekt skatt.***
(Electronic commerce and indirect tax. A report.)
Philip Hallenborg

15/2000 ***Behov av nya associassionsformer?***
(Needs for new kinds of legal entities. A report.)
Christina Helgesson

16/2000 ***Insynens gränser – Allt eller intet?***
Limits to access – All or nothing? Report and summary of a seminar.)
Peter Seipel

17/2000 ***Datavirus - Hur skall en reglering utformas?***
(Data viruses. Seminar documentation.)

18/2000 ***e-skatt? i-skatt? o-skatt?***
(e tax? i tax? o tax?. Report on tax law issues in a new environment.)
Gustaf Johnssén

30/2001 ***Ledningsrätt i IT-tider.***
(The law of conduits in the IT era. How to use the existing infrastructure for new purposes.)
Anders Victorin and Barbro Julstad

31/2001 ***Fri aktör, egenanställd, ny daglönare? (IV) – Fri, ensam, trygg?***
(Free agents, self employed, new day-labourers IV. Documentation of a seminar on one-person enterprises and social insurance.)

43/2001 ***Gratiserbjudanden & IT.***
(Free offers and IT. Report and seminar materials.)
Lena Olsén

52/2002 ***IT i domstolsprocessen.***
(IT in the courts. Seminar documentation.)

55/2002 ***Företagshemligheter i digital miljö.***
(Trade secrets in a digital environment. Seminar documentation.)
Fredrik Jonason (AWA-patent)

56/2002 ***Behandling av personuppgifter och rättsinformationen.***
(Processing of personal data and legal information retrieval systems. Workshop documentation.)

SOU 1998:109 ***Rättsinformation och IT.***
(Legal information and IT. Reports from two conferences 1996 and 1998)

SOU 2001:71 ***Rättsinformation under 2000-talet.***
(Legal information in the 3rd millennium. Report from a conference 2000)

SOU 2002:102 ***Legal Information and the Internet.***
Report from a conference 2001. In English.

Memos

1:1998	***Missbruksmodell – Alternativ reglering av skyddet för person-uppgifter.*** (An abuse model – alternative regulation of the protection of personal data. Also available in English) Per Hammarstedt
1:1999	***Fri aktör, egenanställd, ny daglönare – Hur ser det ut idag? Vad behöver göras? En första karta och sammanställningar av utmaningar.*** (Free agents, self employed, new day-labourers. The situation today.) Mats Utbult
3:1999	***Observatoriets syn på vissa straff- och processrättsliga lagstift-ningsfrågor.*** (The views of the Observatory regarding certain matters of legis-lation in criminal an procedural law.)
4:1999	***Nätets genomskinlighet – En sammanfattning av ett samtal.*** (The transparency of the net. Seminar documentation.)
5:1999	***E-post på arbetsplatsen – En redovisning av ett samtal***. (E-mail at the work place. Seminar documentation.)
6:2000	***Fri agent, egenanställd, ny daglönare III. En workshop och ett förslag till ”Lag om självanställning”.*** (Free agent, self employed, new day-labourers. Workshop docu–mentation and a proposal for a new act on self employment.)
7:2000	***Rättsliga och andra samhällsaspekter på agentteknik. Rapport från ett seminarium.*** (Legal and other social aspects on agent technology. Seminar documentation.)
8:2000	***Auktioner på Internet – Rapport från ett seminarium.*** (Auctions on the Internet. Seminar documentation.)
9:2000	***Överlever upphovsrätten upphovsrätten? Rapport från ett se-minarium.*** (Will copyright survive copyright? Seminar report.)
10:2000	***Bolagsstämma online – Rapport från ett seminarium.*** (Shareholder meetings on-line. Seminar documentation.)
11:2001	***Digitala dokuments bevisvärde – Rapport från ett seminarium.*** (Digital documents as proof. Seminar documentation.)
12:2001	***Deponering av källkod.*** (Deposition of source code.)
14:2001	***Fri agent, egenanställd, ny daglönare!? - En summering.*** (Free agent, self employed, new day-labourers!? A summary.)
15:2001	***Alternativ tvistelösning (ADR) online.*** (Alternative dispute resolution online.)