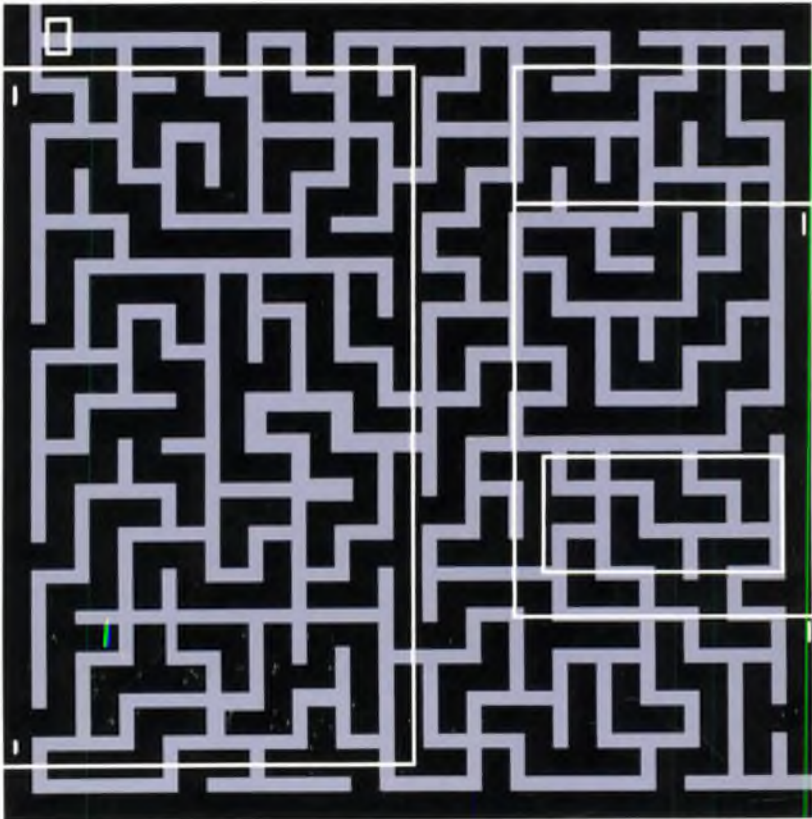


MORTEN S HAGEDAL

FOUR ESSAYS ON:

COMPUTERS AND INFORMATION
TECHNOLOGY LAW



COMPLEX 5/93
INSTITUTT FOR RETTTSINFORMATIKK

TANO



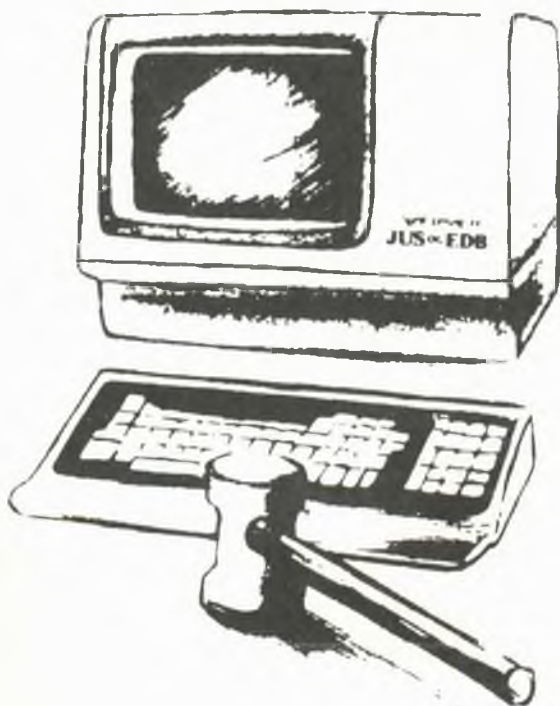
Hovedkontor: Rosenholmvn. 25, 1410 Kolbotn, tlf. (66) 99 80 00
Bergen: Øvre Kråkenes 17, tlf. (05) 12 08 00
Stavanger: Professor Olav Hanssens vei 13, tlf. (04) 87 70 00
Trondheim: Vestre Rosten 81, tlf. (07) 88 00 00

Norsk forening for **JUS og EDB**

Postboks 7557, Skillebekk, OSLO 2

Postgiro 5 13 96 54 Bankgiro 8200.42.49727

Postgiro CompLex 2 12 16 63



Foreningen står bl.a. for
salget av CompLex-heftene
og vedlikeholder abonnements-
ordningene for serien.



***Enkel og hurtig tilgang til
offentlige informasjonsdata***

***- en forutsetning for
effektiv saksbehandling og
riktige beslutninger***

Statens Datasentral er Norges ledende databasevert for offentlig informasjon.

Vi formidler opplysninger fra Løsøreregisteret, Det sentrale personregister, Motorvognregisteret, Tinglysingsdata og Lovdata, for å nevne de viktigste.

I tillegg til alle tjenester for online bruk av basene, bistår vi selvsagt også med satsvise datauttak.

Ta kontakt for nærmere opplysninger!



***- sikker vei til
sikker informasjon***

Statens Datasentral a.s
Ulvenveien 89 B, 0581 Oslo
telefon 22 95 63 00



FØYEN

**Informasjons- og telekommunikasjonsrett
teknologi- og EDB-rett**

Kontrakter - Forhandlinger - Prosedyrer

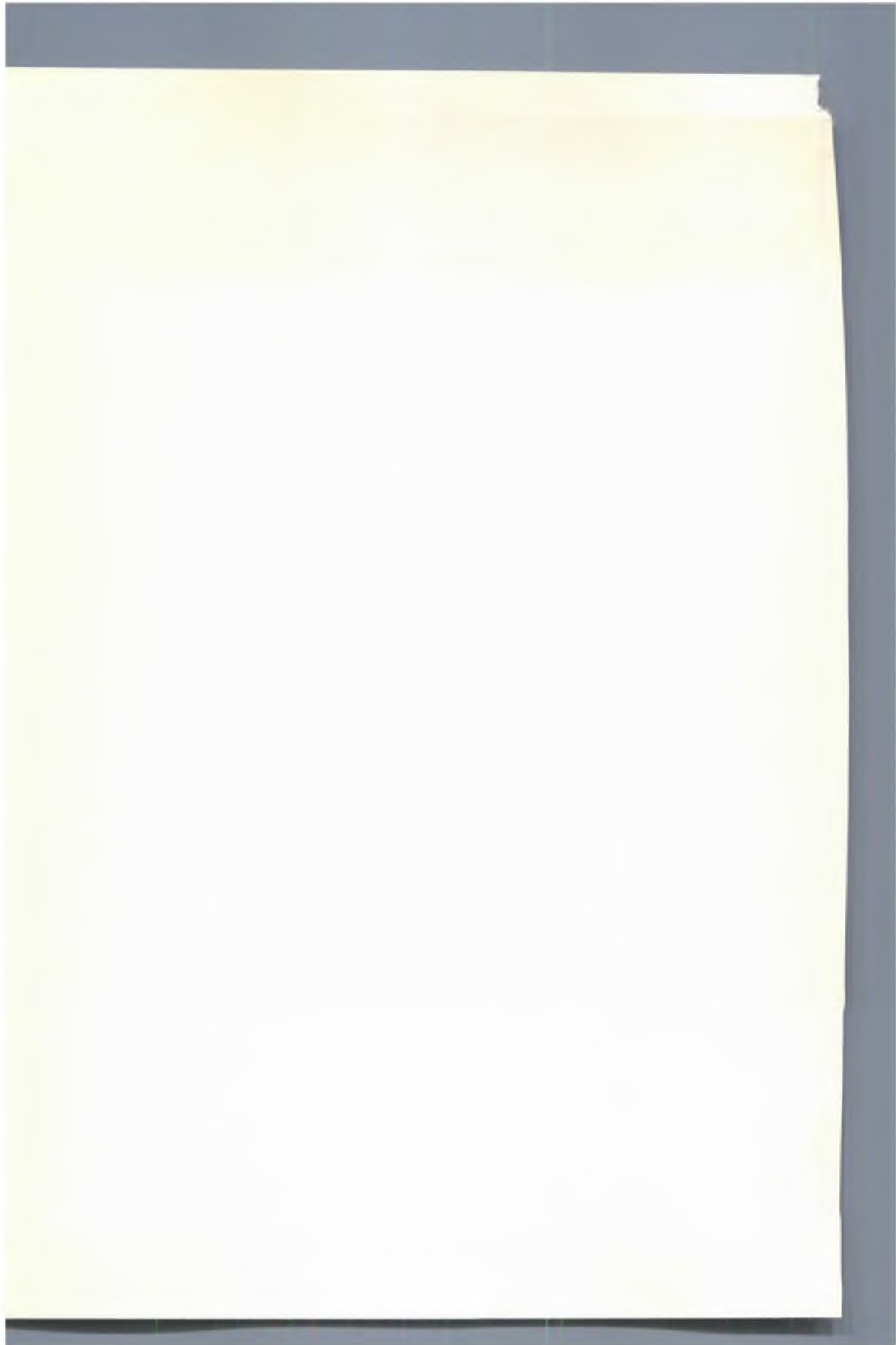
Advokatfirmaet Føyen & Co Ans

Oslo - Asker

Oscarsgate 52, 0258 Oslo

Tel. 22 44 46 40, Fax. 22 44 89 27

STOCKHOLM - LONDON - NEW YORK



W I K B O R G, R E I N & C O.

ADVOKATFIRMA. M.N.A.

Advokatfirmaet Wikborg, Rein & Co beskjeftiger ca 50 advokater fordelt på kontorer i Oslo, Bergen, London og Kobe. Firmaet har spisskompetanse innenfor selskapsrett, skatterett, sjørett, shipping, petroleumsrett, forsikringsrett, finansiering, verdipapir- og børsrett og konkurs- og insolvensbehandling.

WR

Sigurd Wælgaard
Erling C. Hjort
Lars A. Christensen
Helge Myhre
Haakon Stang Lund
Einar L. Koefoed
Olav E. Klingenberg
Haakon Blaauw
Tom B. Knudsen
Øystein Meland
John A. Rein
Arne Didrik Kjørnæs

Dag Steinfeld
Stein Pettersen
Knud Lorentzen
Jon Heimset
Christian Friis
Marius M. Gisvold
Trond Eilertsen
Finn Bjørnstad
Lars Olav Askheim
Jan L. Backer
Leif Petter Madsen
Bernhard Haukali
Geir Ove Røberg

Oslo

Kronprinsesse Märthas pl. 1
Postboks 1513 Vika
0117 Oslo
Telefon.: 22 33 55 10
Telex: 76131 WRCO N
Telefax: 22 41 88 22

London

1 Knightbridge Court
4th floor
London EC4V 5JP
Telefon: (44-71) 236 4598
Telex: 915952 WRCOUK G
Telefax: (44-71) 236 4599

Bergen

Handelens og Sjøfartens Hus
Olav Kyrres gate 11
5014 Bergen
Telefon: (05) 31 81 16
Telex: 42516 WRCO N
Telefax: (05) 31 00 15

Kobe

1-1, 5-Chome Minatojima
Nakamachi Chuo-Ku,
Kobe 650, Japan
Telefon: (81-78) 303 1772
Telex: 5622404
Telefax: (81-78) 303 1781



Advokatfirmaet Selmer & Co. ANS har 31 medarbeidere, hvorav 19 advokater og advokatfullmektiger. Firmaet yter advokattjenester hovedsakelig innen de forretningsjuridiske disipliner, omfattende bl.a. kontraktsrett, selskapsrett, skatterett, aksje- og børsrett, arbeidsrett, petroleumsrett, gjeldsforhandlinger og konkurs, jus og EDB. Våre oppdragsgivere er i det vesentlige innenfor bank, finans, revisjon, forsikring, shipping, energi, handel, entreprise og fast eiendom, forskning- og utviklingsarbeid. Firmaet yter dessuten advokattjenester ved generasjonsskifte i familiebedrifter og bistand generelt innen arverett, familierett og skifterett.

ADVOKATFIRMAET
SELMER & CO
ANSVARLIG SELSKAP

MEDLEMMER AV DEN NORSKE ADVOKATFORENING

CHRISTIAN SELMER
EILIF TORMA
SVERRE S. TYSLAND
BJØRN KLEIVEN

MORTEN STANG
ASBJØRN BERG
ROY M. SLETTEVOLD
TRYGVE ØYDNE

ANNE-BLANCA DAHL
LARS WEYER-LARSEN
JON SKJØRSHAMMER
ODD-EINAR CHRISTOPHERSEN

Fullmektiger

Synnøve Smedal, Susan Halvorsen
Ingebjørg Harto, Anne Helene Osberg
Kirkegt. 15, Tlf. 22 42 64 90
Postboks 478 Sentrum, 0105 Oslo





DEN NORSKE BANKFORENING
BANKFORENINGENS SERVICEKONTOR

Småskriftserie og Bankjuristen

Bankforeningen har siden 1988 utgitt en serie med småskrifter som inneholder dels lov- og regeltekster, kommentarer og utredninger. Bankforeningen utgir også gjennom tidskriftet Økonomisk Revy den bankjuridiske nyhetsrapporten Bankjuristen. Både småskriftene og Bankjuristen er nyttige verktøy for jurister og andre i bank og finansnæringen.

Småskrifter

Lovtekster på norsk og engelsk

* Forretningsbankloven, Finansieringsvirksomhetsloven og Kredittsinsloven

- første utgave, desember 1988

- annen utgave, oktober 1990

- tredje utgave, mars 1992 (inneholder også lovene om Statens Banksikringsfond og Statens Bankinvesteringsfond)

* Tekstene til de samme lover i engelsk oversettelse

- første utgave, 1988

- annen utgave, 1990

- tredje utgave, ventes i løpet av 1992

* Bankers kapitaldekning/Banks' Capital Adequacy, juli 1992

* Den nye tvangsfullbyrdsesloven og bankene, november 1992

Bankinterne avtaler, betalingsformidling,

Ansvarsregulerende utvalg

* Mønsteravtale mellom bank og kortholder om bruk av elektroniske utfak- og betalingskort - med kommentarer, februar 1989

* Avtale- og regelverksamling for Innenlands betalingsformidling, annen utgave oktober 1990

* Avgjørelser av Ansvarsregulerende utvalg
- for perioden 1986-89, november 1990
- for perioden 1986-91, juli 1992

Kommentarutgaver og utredninger

* Ansvarsforholdet mellom Kredittilsynet og Sikringsfondet når det oppstår krise i en bank, januar 1989

* Finansinstitusjonslovens bestemmelser om eierforhold m.v., lovkommentarer, februar 1991

* "Kjenn din kunde". Identitets- og legitimasjonskontroll, problemer - anbefalinger, oktober 1991

* Rapport om organiseringen av bankenes kontrollsystemer, oktober 1991

* Regelverk for vurdering av tap på utfån m.v. Kommentarrapport fra en arbeidsgruppe nedsatt av Den norske Bankforening, mars 1992

* Store engasjementer - grense for kreditt til en enkelt kunde, september 1992

EF-rettslige emner

* EF-bankdirektiver, mars 1990

* Oversikt over EF's regelverk på bankområdet, desember 1991

Kommentarer til Bankklagenemndas uttalelser

(utgis i samarbeid med Sparebankforeningen)

* Bankklagenemndas uttalelser om umyndlige, oktober 1990

* Bankklagenemndas uttalelser om utfån, desember 1990

* Bankklagenemndas uttalelser om innskudd, januar 1992

Jeg ønsker å kjøpe småskriftet _____

Jeg ønsker å tegne meg som abonnent på Bankforeningens småskriftserie, og mottar dermed disse raskt etter utgivelse

Prisene vil variere, fra ca. kr. 100,- (Eks. forsendelse)

(Sett kryss)

Jeg ønsker å abonnere på Bankjuristen gjennom Økonomisk Revy

Årsabonnement kr. 315,- for seks utgaver, fritt tilsendt i Norden

Bestillingen returneres til Bankforeningens Servicekontor, Postboks 1489 Vika, 0116 OSLO

Bestillingen kan også sendes pr. telefax: 22 83 07 43 eller telefon 22 83 31 60

Navn på bedriften: _____

Bestillerens navn: _____

Postadresse: _____

Postnummer/sted: _____

Dato..... Signatur.....



ADVOKATFIRMAET
BLOMSETH, KRISTIANSEN & SOLBERG ANS
M.N.A.

- | | |
|-----------------------------------|---------------------------|
| ♦ Telekommunikasjonsrett | ♦ Bygg- og entrepriserett |
| kabel-TV, kringkasting m.m. | ♦ Eiendomsrett |
| ♦ Opphavsrett | ♦ Boligrett |
| ♦ Transportrett - Luftrett | ♦ Selskapsrett |
| ♦ Skjønns- og ekspropriasjonsrett | ♦ Foreningsrett |
| ♦ Anglo-amerikansk kontraktsrett | ♦ Arbeidsrett |

Tlf. 22 60 85 85 - Fax 22 60 85 20
Pilestredet 57, 0350 Oslo



CompLex nr 5/93

Institutt for rettsinformatikk
Niels Juels gt. 16
0272 Oslo

Morten S Hagedal

Four essays on:

COMPUTER AND INFORMATION
TECHNOLOGY LAW

TANO

© Tano A.S. 1993
ISBN 82-518-3198-9

Institutt for rettsinformatikks utgivelser i skriftserien CompLex er støttet av:

Den norske Advokatforening
Den norske Bankforening
Digital Equipment Corporation A/S
Lovdata
Kopinor

Fotografisk opptrykk ved
Engers Boktrykkeri A/S. Otta

Preface:

These four essays are all written as a part of my LLM in Computer and Information Technology Law at the University of Strathclyde. I have kept the structure in the essays and have only made some minor corrections and additions.

The reader is apt to find that it is primarily written for an English or Scottish examiner, hence my emphasis on continental law, and the jurisprudence of the European Court of Justice and the differences from English or Scottish literal interpretation.

This LLM has four compulsory subjects, in each of these an essay is written, with a tentative limitation of 5 000 words. In addition to this there is written a dissertation.

In publishing these four essays I must admit that each of them are in fields that opened new perspectives for me - and I would like to continue working on some of them. This implies that much more could have been written on each topic, and probably should have been done. This would take a considerable amount of time. I am therefor left with the choices of publishing them as they are, or not publishing them at all. Hopefully the reader finds some ideas that might be of use for him.

My year in Glasgow gave me a rather broadened horizon in the field of IT-law, and I would like to thank the lecturers at the University for their support and guidance in the field - dr Ian Lloyd and Moira Simpson.

Unfortunately being a citizen of a non-EC country a year at a British University is a rather expensive experience, and without the financial help of the British Council, Marie Bachkes reiselegat for ungdom and Norwegian Business Foundation for Education Abroad this would not have been possible.

Trondheim, October 1993

Morten S Hagedal

Table of Contents:

Preface:	iii
Table of authorities	xiii
Bibliography	xiii
Norwegian Cases	xviii
English Cases	xviii
American Cases	xviii
Cases from the European Court of Justice	xix
Dutch Cases	xix
Canadian Cases	xix
German Cases	xix
Cases from the European Court of Human Rights	xx
Abbreviations	xxi
The relation between EC Competition Law and Intellectual Property Rights.	1
1 Introduction	2
1.1 Is there an antagonism between intellectual property rights and competition?	3
1.2 The concept of intellectual property rights	5
1.3 The balancing of interests as a ground for intellectual property rights	6
1.3.1 Different levels of protection - depending on the criteria to obtain protection	7
1.3.2 International cooperation	9
1.3.3 Copyright	10
1.3.4 Patent	11

	1.3.5	Some terminological problems arising from the differences between the different jurisdictions	12
	1.4	The aim of the essay	13
2	A European dimension		13
	2.1	The interaction between competition and free movement of goods	13
	2.2	Europe 1992 - Intellectual property rights	15
	2.3	The problem with national treatment and the European Community - the exhaustion of rights or the rights granted the public over a copyrighted work	15
	2.4	Different criteria for achieving protection in different member states and different protection in the member states	18
	2.5	Actions in the field of competition and intellectual property rights within the EC	20
	2.6	The interpretation of EC-directives	20
3	Competition and Intellectual Property Rights		21
	3.1	Two different ways to change the balance	21
	3.2	Copyright	22
	3.2.1	Computer programs	23
	3.2.1.1	The right to reverse engineering under	

	the Software Directive	25
3.2.2	Databases	26
3.3	Examples where the intellectual property rights and the competition rules differ - and the competition rules are used to change the balance	28
3.3.1	Intellectual property rights conflicts with competition rules . . .	28
3.3.1.1	Article 86	29
3.3.1.2	Article 85	31
3.3.2	Competition rules gives protection to extend the right under an intellectual property right	31
4	Conclusions	32
	Data protection - where next?	35
1	Introduction	36
1.1	The use of computers - is the problem new?	37
1.2	The problems	38
1.2.1	The vast amount of information available to the decision-maker . . .	38
1.2.2	The assessment for the decision maker	40
1.2.3	Some information may - wrongly- be regarded as prima facie	42
1.2.4	The struggles to make decisions by computer	43

1.3	The solutions or the challenges to the legal system	44
1.3.1	The concept of privacy	44
1.3.2	The continental european approach in conflict with the concept of privacy	45
1.4	The problems dealt with in this essay . . .	46
2	Communication theory and some of the problems with communication	47
2.1	Basics of communication theory	47
2.2	The vagueness of the language - the jargon used in some parts	49
2.3	The problems with the lack of awareness of the communication process and the different meaning of words	49
2.4	The problems of the group interests	51
3	The collection, storage, use and abuse of data in an automated process	52
3.1	A database	52
3.2	A model	52
3.2.1	The reason for the gathering of the information	54
3.2.2	The accuracy of the information . . .	55
3.2.3	Questions of security	55
4	The European dimension	58
4.1	Free movement of data as one of the basics of the Community?	58
4.2	The data-flows generated due to the internal market	59
4.3	Technical trade barriers or favouring one member state	60

5	Is the proposal from the Commission sufficient to cope with these problems	60
	The problems with information crime	65
1	Introduction	66
2	Information law and information crime - general considerations	70
2.1	Information	71
2.1.1	The concept of information	71
2.1.2	Ways of communicating information	72
2.1.3	Information and the media	74
2.1.4	Information - concluding remarks	76
2.2	Communication processes	77
2.3	Information and secrecy	78
2.4	Economics of information	79
2.4.1	The value of information	80
2.4.2	Protection of the investments in information	81
2.5	Aspects of information law - why "ownership"-structure is not applicable . .	82
2.5.1	Controlling data - due to its content	83
2.5.2	Privacy	83
2.5.3	Security of the state	84
2.5.4	Professional secrecy	84
2.5.5	Freedom: right to information? . . .	85
2.6	Models for "information law"	87
2.7	A temporary summary of this part	89
2.8	Intellectual property rights	90
2.9	Some special problem with regulation of information law	91

3	Theft of information - a <i>de lege lata</i>	
	overview	93
3.1	The general starting point	94
3.2	Different jurisdictions - overview	95
4	Some general considerations as to	
	information crime	98
5	Theft of information - a <i>de lege ferenda</i>	
	discussion	100
5.1	Legal and other measures	101
5.2	To extend the present criminal offenses or create new offenses	103
5.3	A starting point for the discussion whether to make new criminal offenses or not	104
5.4	The need for international legal harmonization	104
5.5	The balancing of interests. Whether to regulate or not	105
5.6	Whether to make a criminal offence or not	108
	Software and product liability	111
1	Introduction	112
2	The relation between the Consumer	
	Protection Act and the Product Liability	
	Directive	113
3	Approaching the problem	115
3.1	The problem of description in computer tort law	115

3.2	The jurisprudence of the European Court of Justice	116
4	The factual side of the description - what is software	118
4.1	Communication theory	118
4.2	Programming	119
4.3	The software and the media	121
	4.3.1 General considerations	121
	4.3.2 The problem of software and media in our context	123
4.4	The connection between software and a database - an attempt to illustrate that there is more than one element in some software	124
5	Liability - general considerations	126
5.1	Where does Product liability fit into the general liability scheme	127
5.2	Why the Product Liability legislation ...	128
6	Can software be regarded as <i>products</i> as defined in the directive?	131
6.1	The media carrying the software	133
6.2	Software, <i>per se</i> a product?	133
6.3	The consequences of defining software as a subject matter for product liability .	134
	6.3.1 Damage - as defined in the Directive	134
	6.3.2 Different kinds of software	135
	6.3.3 Casuistical approach	136
	6.3.4 Defect - as defined in the Directive	139

6.3.5	When is software to be regarded as defect in the meaning of the directive?	140
6.3.6	The development risk defence . . .	142
6.4	The position of the Commission	144
6.5	Conclusion	145

Table of authorities

Bibliography

- Altes, William F, Donimering, Egbert J, Hugenholtz, P Bernt and Kabel, Jan J C (ed) (1992); *Information law towards the 21th Century*, Deventer 67
- Arnesen, Finn (1992); *Introduksjon til rettskildelæren i EF*, 2 edition, IUSEF nr 2, Oslo 117
- Barendt, Eric M (1992); *Fundamental freedoms*, in Altes et al; *Information Law Towards the 21th Century*, Deventer 85
- Bellis, Jean-Francois and L'Ecluse, Peter (1991); *The Meaning of Competition Law for Information Technology In Europe*, in Meijboom and Prins; *The Law of Information Technology in Europe 1992* 13
- Bender, David (1991); *Computer Software Product Liability. The United States Perspective*, in Meijboom and Prins (ed); *The Law of Information Technology in Europe 1992 (A Comparison with the USA)*, Deventer 137
- Bing, Jon (1981); *Information Law?*, *Journal of Media Law and Practice* 1981 p 219-239 66, 67, 71, 75, 112
- Bing, Jon (1991a); *Personvern i faresonen*, Oslo 45
- Bing, Jon (1991b); *Reflections on a Data Protection Policy for 1992*; *Yearbook of Law Computer and Technology*, Volume 5 1991 p 164 53, 59
- Bing, Jon (1992); *Rettslige aspekter ved etablering og distribusjon av offentlige tjenester*, Oslo 52
- Bing, Jon (1993); *AXION Information Technology and Law*, Oslo . . . 72, 73
- Bing, Jon; Madsen, Kristine M; Myrland, Kjell (1987); *Strafferettslig vern av immaterielle goder*, *CompLex* 12/87, Oslo 87

- Blume, Peter (1992); *Nyt udkast til EF-direktiv om databeskyttelse*, Lov & Data nr 33 Desember 1992 61
- Bown, Christopher M (1986); *Liability for the Supply of Defective Software*, CL&P, September/October 1986 p 2 132
- Brannigan, Vincent M and Dayhoff, Ruth E (1981); *Liability for Personal Injuries Caused by Defective Medical Computer Programs*, American Journal of Law & Medicine 125
- Bryde Andersen, Mads (1988); *edb og ansvar*, Copenhagen 115, 118
- Bryde Andersen, Mads (1991a); *Lærebog i edb-ret*, Copenhagen .. 47, 68, 74, 77, 78, 118, 120, 122, 130
- Bryde Andersen, Mads (1991b); "Problems of description" in *Computer Tort Law*, in Blume (ed) Scandinavian Studies in Information Technology and Law, Deventer 68, 75, 115, 118, 122, 123, 127, 137
- Bull, H P (1985); *De fundamentele problemen van het informatierech. Die Grundprobleme des Informationsrecht*, Tjeenk Willik - Zwolle 67, 80
- Coleman, Allison (1993); *Protecting confidential information*, in Reed (ed); Computer Law, London 67, 80, 83, 86, 108
- COM (85) 310 FINAL; *White Paper Completing the Internal Market* .. 20
- COM (88) 172 FINAL; Green Paper on "Copyright and the Challenge of Technology" 20
- COM (92) 24 FINAL - SYN 393; *Proposal for a council directive on the legal protection of databases*, presented by the Commission. 26
- COM (92) 422 - SYN 287, *Amended proposal for a Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Presented by the Commission 61
- Council of Europe Recommendation No R (89) 9, adopted by the Council of ministers on 13. September 1989. 108

- Dommering, Egbert J (1991); *An Introduction to Information Law. Works of Fact at the Crossroad of Freedom and Protection*, in Dommering and Hugenholtz (ed); *Protecting Works of Fact*, Deventer . . . 66-68, 81, 88, 90
- Dommering, Egbert J (1992); *Information Law and the Themes of this Book*, in Altes et al (ed); *Information Law towards the 21th Century*, Deventer 67
- Dyckjær-Hansen, Karen (1993) *Immaterialrettigheder indenfor EF - en statusrapport*, NIR 1993 p 176 17
- Forester, Tom and Morrison, Perry (1990); *Computer Ethics*, Oxford . 40, 51, 53
- Franken, Hans (1990); *Computing and security*, in Kaspersen and Oskamp (ed) *Amongst Friends in Computers and Law*, Deventer 75, 94, 97, 100, 101, 122
- Galtung, Andreas (1992); *Rettslige sider ved teletorg*, CompLex 10/92, Oslo 92
- Groves, Peter; Martino, Anthony; Miskin, Claire and Richards, John (1993) *Intellectual Property and the Internal Market of the European Community*, London, Norwell 13
- Hagedal, Morten S (1994) *Legal Protection of Databases; Norwegian and English law, also compared with the Present Proposal from the Commission*, CompLex, Oslo NYP 2, 6
- Hagstrøm, Viggo (1989); *Informasjonsansvar (om villedning av annen enn kontraktspart)*, TfR 1989 p 196-220 128
- Hirschbäck, Jakob (1989); *Is software a product?* 5 CL&P 154 . . 75, 122, 132, 142
- Karnell, Gunnar GW (1991) *The Nordic Catalogue Rule*, in Dommering and Hugenholtz (ed); *Protecting Works of Facts*, Deventer/Boston . . . 27
- Kirk, Gordon (1988); *Software and the Consumer Protection Act 1987* 6 CL&P 2 124
- Knoph, Ragnar (1936) *Åndsretten*, Oslo 5

- Koktvedtgaard, Mogens (1991); *Lærebog i immaterialret*, Copenhagen 17, 19, 29
- Law Commission (England and Wales); *Computer Misuse*, LAW.COM No 186 69
- Lloyd, Ian (1993); *Computer Crime*, in Reed (ed) *Computer Law*, London 69
- Mackaay, Ejan (1992); *The Public's Right to Information*, in Altes et al; *Information Law Towards the 21th Century*, Deventer 85, 86
- McFarlane, S M and Davis, R H (1984); *Personell administration: privacy issues*, Information age, vol 6 No 4 october 1984 p 223 44
- Millard, Christopher J (1993) *Copyright* in Reed (ed) *Computer Law*, London 10
- NOU 1992:23; *Ny straffelov - alminnelige bestemmelser*, Straffelovkomisjonens delutredning V, Oslo 89, 133
- Ploman, Edward W. and Hamilton, L. Clark (1980); *Copyright*, London. 3
- Pounder, Chris (1985); *Police computers and the Metropolitan Police part II: command and control and criminal information systems*, Information age volume 7 no 4 october 1985 p 189 50
- Reed, Chris (1993); *Liability*, in Reed (ed) *Computer Law*, London . 119, 131, 145
- Saxby, Stephen (1990); *The Role of Law in the Development of the Information Society*, in Kaspersen and Oskamp (ed) *Amongst Friends in Computers and Law*, Deventer 67, 76, 90, 105, 128, 129, 136
- Schjølberg, Stein (1991); *Datakriminalitet og straffelovgivning - en internasjonal utvikling*, in Galtung (ed); *Internationella aspekter på rättsinformatiken*, Nordisk Årbok i rättsinformatikk 1991, Stockholm 102
- Scottish Law Commission; *Report on Computer Crime*, Scot Law Com No 106 69

- Seipel, Peter (1992); *Contracts for Databases*, in Erik Moseson (ed)
Software Procurement, Stockholm 125
- Selmer, Knut S (1992); *Hvem er du? Om systemer for registrering og
identifikasjon av personer*, LoR 1992 p 311 ff, Oslo. 56
- Sieber, Ulrich (1990); *The Emergence of Criminal Information Law*, in
Kaspersen and Oskamp (ed); *Amongst Friends in Computers and Law*,
Deventer, p 117-129. 67, 84, 96, 98, 100-102, 104, 106
- Sieber, Ulrich (1992); *The International Emergence of Criminal
Information Law*, Cologne, Berlin, Bonn, Munich 67, 69, 82, 95, 99, 100,
103, 105, 108
- Sieber, Ulrich (ed) (1991); *Liability for On-line Data Bank Services*,
Cologne, Berlin, Bonn, Munich 127
- Steiner, Josephine (1992); *Textbook on EEC Law*, London 17, 28, 114, 117
- Sterling, JAL (1989) *Harmonisation of Usage of the Terms "Copyright",
"Author's Right" and "Neighbouring Rights"* [1989] 1 EIPR 14 12
- Stuurman, Kees (1991); *The EC Directive on Product Liability and its
Application to information technologie [sic]*, in Meijboom and Prins (ed);
*The Law of Information Technology in Europe 1992 (A comparison with
the USA)*, Deventer 75, 122, 130
- Tapper, Colin (1987); *"Computer Crime": Scotch Mist?*, [1987] Crim.L.R. 4
..... 69
- Triaille, Jean-Paul (1991); *The EEC Directive (25 July 1985) on product
liability and its application to databases and information*, CL&P May-
June 1991 p 217 126, 133
- Vivant, Michel (1991); *Copyrightability of Computer Programs in Europe*,
in Meijboom and Prins; *The Law of Information Technology in Europe
1992*, Deventer. 11, 23, 25
- Vyrje, Magnus Stray (1987); *Opphavsrettens ABC*, Oslo 3

XVIII FOUR ESSAYS ON COMPUTER AND IT LAW

- Wiebe, Andreas (1992) *Know-how-Schutz von Computersoftware (Eine rechtsvergleichende Untersuchung der wettbewerbsrechtlichen Schutzmöglichkeiten in Deutschland und den USA)*, Munich 19

Norwegian Cases

- Inter-Media Graphic Systems Inc v Aladdin Software A/S, Strømmen District Court, 20. June 1989 32
- Rt 1992 p 1629 67, 76

English Cases

- Cox v Riley, (1986) 83 Cr App R 54 99
- Oxford v Moss (1978) 68 Cr App R 183 97, 102, 104
- R v Absolom, (1983) The Times 14 September 1983 97
- R v Henn [1981] AC 850 20, 117
- Sayre v Moore 1 East 361 (1785) 4
- University of London v University Tutorial Press [1916] 2 Ch. 601 . . 26

American Cases

- Feist Publications Inc v. Rural Telephone Service Co. Inc., U.S. Sup. Ct., No 89-1909 7, 8, 10, 27
- Hancock v Decker, (1967) 379 F.2nd 552 96
- Hancock v Texas, (1966) 402 SW 2d 906 96, 97

Cases from the European Court of Justice

British Broadcasting Corporation v Commission of the European Communities (Intervener Magill TV Guide) [1991] 4 CMLR 669 ..	3, 30
Deutsche Grammophon Gesellschaft v Metro-S.B.-Grossmärkte, 1971 E. Comm Ct. J. Rep. 487, 10 CMLR 631 (1971)	16, 17
Independent Television Publishers v Commission of the European Communities (intervener Magill TV Guide) [1991] 4 CMLR 745 ..	3, 30
Radio Telefis Eirann v Commission of the European Communities (Intervener Magill TV Guide) [1991] 4 CMLR 586	3, 30
Warner Brothers Inc and Metronomone Video ApS v Erik Viuff Christiansen, Case 158/86	18

Dutch Cases

Dutch Courts of Appeal, October 1983	97
Electricity Judgement; Supreme Court, 1921	97

Canadian Cases

R v Stewart, 50 D.L.R. (4th) 1	86, 91, 97, 102, 106
--------------------------------------	----------------------

German Cases

[1985] 94 BGHZ 276 (Inkasso-case)	19, 95, 97
---	------------

Cases from the European Court of Human Rights

Gaskin v U.K, (1990) 12 EHRR 36	85
Leander v Sweden, (1987) 9 EHRR 433	85

Abbreviations

AC	Appeal Cases
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
Ch	Changery
CL&P	Computer Law and Practice
CMLR	Common Market Law Review
Cr App R	Criminal Appeal Reports
Crim L R	Criminal Law Review
D.L.R.	Dominion Law Review
EHRR	European Human Right Reports
EIPR	European Intellectual Property Review
F. 2nd	Federal Reporter (Second Series)
LoR	Lov og Rett
NIR	Nordiskt Immaterialt Rättskydd
NOU	Norges Offentlige Utredninger
Rt	Norsk Retstidende
SW	Southwestern Reporter (First Series)
TfR	Tidsskrift for rettsvitenskap



The relation between EC Competition Law and Intellectual Property Rights.

Article 36 of the Treaty of Rome provides that the provisions of intellectual property law may be used in a manner which conflicts with the Treaty provisions relating to free movement of goods. Considering recent developments, indicate how satisfactory you consider the relationship between the provisions of competition and of intellectual property law.

1 Introduction

Intellectual property law involves in most jurisdictions the law of copyright, the law of patent, the law of trademarks, the law of design etc. The similarity between these rights are basically that they involve immaterial objects, hence intellectual property and that they give the holder of the right some exclusive rights concerning the intellectual property.

Traditionally the first problem is the fact that there is no physical substance for the right. Whereas the right of property, real property and movables, has some physical substance this may be the basis for the rights concerning it. This is not the case with the intellectual property rights. The intellectual property is intangible, hence the substance may not be used as a basis for the rights. The object of the right must be based on something else.

The rights given the intellectual property owner must be found outside the substance of the property. In all jurisdictions this is based upon statutory provisions, that under some circumstances give the owner some exclusive rights concerning the property, which is intangible.

The different intellectual property right differs - partly the requirements for protection are different - between different jurisdictions. Also the rights given under the intellectual property scheme differs between the jurisdictions.¹

¹ For an comparison of copyright with the emphasis on databases between Norwegian and English law, see the forthcoming Hagedal 1994

1.1 Is there an antagonism between intellectual property rights and competition?

It is claimed that in some circumstances there is an antagonism between Intellectual Property Rights and Competition Law. Whether this is true is partly based on the way the problem is approached. If one considers examples of monopolistic behaviour or conduct that may be traced back to a strong Intellectual Property Right owned by the part - it may be claimed that this is due to the Intellectual Property Right². On the other hand the intellectual property rights may be seen as examples of competition law, set up for one or more specific fields.

Partly one might argue that the intellectual property rights are the result of a balancing of interest, where these considerations also are the basis of some continental unfair competition laws.

From a historical point of view it is easy to find examples of this. The first known copyright law is The statute of Queen Anne from 1709³. Ploman/Hamilton 1980 p 13 writes about this statute⁴;

The basic provisions of the Statute were directed towards resolving the problems and abuses of the book trade. To accomplish this, the framers

² As an example of this see the Magill cases; RTE v Commission, BBC v Commission and ITP v Commission

³ Vyrje 1987 p 39

⁴ Quoted from Vyrje 1987

of the Statute codified not only the Stationers' copyright but also the author's right to copy.

It seems clear that one of the basis of the statute was to set up rules of trading and competition among the publishers of books. The aim is to give the copyright owner some exclusive rights concerning the copyrighted work.

In defining the limitations and scope of copyright protection Lord Mansfield has put forward in *Sayre v Moore*;

We must take care to guard against two extremes, equally prejudicial, the one, that men of ability, who have employed their time for the service of the community, may not be deprived of their just merit, and the reward of their ingenuity and labour; the other that the world may not be deprived of improvements, nor the progress of the arts be retarded.

Already at this stage it seems clear that copyright was set up to give rules that are similar to many unfair competition rules we have in some European jurisdictions today.

Regarding patent it has through the history of patent been recognized that the monopoly a patent gives may be too strong, therefore there is an opening to be granted compulsory licences in some circumstances, cfr the Paris convention article 5 A.-(2):

Each country of the Union shall have the right to take legislative measures providing for the grant of compulsory licences to prevent the abuses which might result from the exercise of the exclusive rights conferred by the patent, for example, failure to work.

For the case that a patent becomes too strong there is a possibility that a compulsory license may be granted, it seems naturally to consider this an effect of a competition rule, but as it is built into the patent system it is likewise easy to consider it as a part of the patent system.

Trade marks, which in most jurisdictions are considered to be a part of the intellectual property system is basically set up to make rules for the competition. In most circumstances there is no need for originality or ingeniousness to obtain a trade mark right. The main criterion is that it is distinctive. Normally the name or expression used in trade mark is not given protection due to the creativity of the "writer", but so competitors shall not abuse it in an unfair way. Normally trade marks would not process any creativity needed under most (continental) copyright laws.

This has also been stated by the Commission, that the "era of protection in itself and the definition of the acts exclusively reserved to the copyright owner directly affect the conditions of competition." (Nineteenth Report on Competition Policy (1990) No 34.)

1.2 The concept of intellectual property rights

The concept of intellectual property rights differs between the rights in question. The similarities may be said to be that if a certain work or idea is produced or invented the producer or inventor gets some rights concerning the work or idea.

Traditionally there has been a strong division between copyright and patent, in such a way that patent governs the industrial products and copyright is for the arts⁵.

Of course from the beginning copyright has covered also more industrial products.

⁵ See Knoph 1936 p 52

There is also a difference in the approach to at least copyright between the common-law jurisdictions and the continental approach⁶.

These differences implies that it is rather difficult to make a general discussion. The problem has to be assessed on each intellectual property right, in each jurisdiction in order to give a full overview of the implications of intellectual property rights.

1.3 The balancing of interests as a ground for intellectual property rights

The law of property, real property and movables, goes back to the Roman Law. The Roman Law did not have any intellectual property law, and when at some stage in the development of the legal system would create this it had to be made as a result of a balance between the different interest.

One interest lies with the inventor, writer or whatever creator that made the work. He has a legitimate interest which is twofold; the one and obvious is to get a financial outcome of his work, the other lies in his moral rights, *la droits morale*. The economic interest would be to create a monopoly that is so strong as possible, so any use of the work, idea or whatever - would depend on him and he could therefore claim money for the use of it. The moral rights becomes apparent with authors right, more than any of the other intellectual property rights.

⁶

In relation to databases, see the forthcoming Hagedal 1994

Another interest lies with each and every one of us. That there should be a possible to use the ideas, inventions or whatever made by other as freely as possible. That no obstacle should be made for the free use of ideas and work.

Also the society has an interest in this field; the society must move forward, there is from an economical point of view necessary to uphold production and competition - this includes the simple fact that in order to move forward some inventions must be made and used, there has to be a development in the economic life. In order to achieve this it is necessary to give some rights to the inventors and the copyright owners.

At the same time this should balance the interest of competition between different parties in the financial live. If you give a right that is too strong this is not good for the competition, and if you give a right that is not strong enough, this would counter competition. These aspects are also discussed by the US Supreme court in *Feist*.

Trade marks falls outside this balancing of interests, since it only is concerned with the trade and distinction between different trade marks.

1.3.1 Different levels of protection - depending on the criteria to obtain protection

Generally it may be said that the stronger protection you should get by an intellectual property right, the more may be demanded to achieve it. While copyright is given to any banal expression, patent is given only where there is an invention. The protection given by copyright is not as strong as the protection given by a patent. This is shown in figure 1.

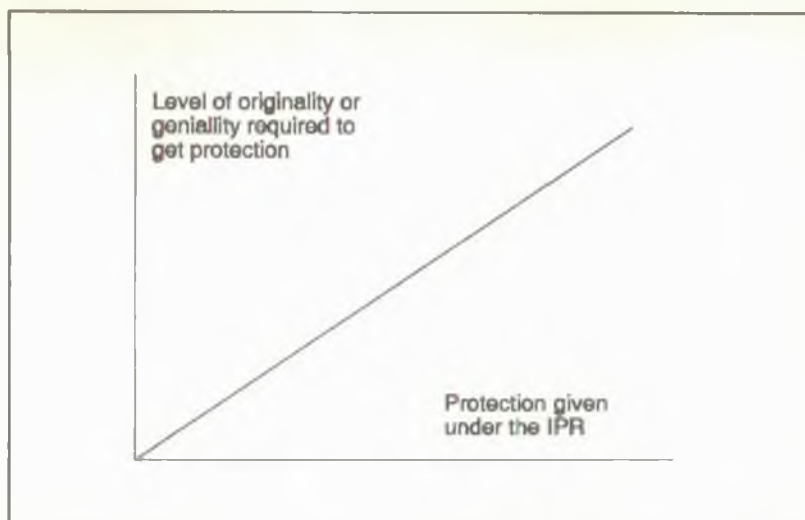


figure 1 The relation between the level of originality or ingeniousness needed and the protection given

It seems as if this is one of the basics of any intellectual property right. There is to be a relation between the requirements and the protection given⁷.

Alas this is not necessarily the situation in all circumstances. There is a demand from the advocates of the copyright holders that there should be a stronger protection than what follows from this model. In some cases this is upheld.

For the case of patent this would give a monopoly of the idea - or the practical use of it. For copyright this will give a "monopoly" on the expression, but not the underlying idea.

⁷

However this might not necessarily be the case with copyright protection based on the skill and labour doctrine under English law., cfr also *Feist*, supra.

Since there may be different criteria in the different member states, and the exclusive rights may differ or be the same the correlation is not as stringent as it may seem from this part.

1.3.2 International cooperation

Since ideas and expressions does not respect borders between different states, there is a demand for some kind of international cooperation in this field - so any intellectual property right might be respected also abroad. In the field of intellectual property rights there has from the early days been a cooperation between the states.

To a large extent intellectual property rights are based upon treaties. These treaties sets out the *minimal* protection that is to be given for the works and is based upon national treatment of the intellectual property rights.

The main treaties are: For copyright the Berne-convention and the World Convention on Copyright; for patent the Paris convention the European Patent convention, and the plant varieties convention; trade marks are governed by the Madrid convention in addition to the Paris convention.

For copyright this means, under the Berne-convention, that a work is given copyright protection in one state of the Berne Union, if produced by a citizen of that country, or if it first is published in the country. For other works there will be given copyright if the country where the work was published is a part of the Berner-convention, on the same basis as the citizens of the country.

A result of this is that each state may set up the rules for granting copyright in work *and also* the rights granted. In the European dimension, *infra* 2.3, this distinction is of importance.

This also means that a work that is protected by copyright in the United Kingdom, not necessarily is copyrighted in the Federal Republic of Germany, or in Norway. This simply due to the differences in requirements for copyright protection.

1.3.3 Copyright

Copyright is given to the expression of an idea. There is a dichotomy between an idea and the way it is expressed. Most things may be expressed in different ways, and the choice of expression is what gains protection under copyright, if the necessary criteria applies.

The reason for this is that if not the expression, but the idea was to be given protection it would statute a monopoly for the ideas*.

It might however be argued that the skill and labour doctrine under English law would protect ideas, or rather facts, see the discussion by the US Supreme court in *Feist* at this point. Arguing that this is not the case, see however Millard 1993 p 94.

At the same time the requirements for copyright are low, as long as the same idea may be expressed in other ways and the expression is original (and creative) - copyright is given. There are differences in the level required in the different jurisdictions.

* This is basically what patent does, but the criteria for gaining a patent are different from the criteria for getting protection by copyright.

Traditionally this is based upon a balance between the interests of the copyright owner and the interest of the society as such.

Traditionally there has been two different views of copyright, the Common-law approach and the continental European approach. Where the European has had a stronger aim towards the moral rights, cfr Vivant 1991 p 103;

Today, the question of the protection of computer programs in Europe by author's right or copyright appears a delicate one. ... First, conflicts among the national laws, as the solutions opted for vary from country to country, if we only consider the almost philosophical differences between systems of author's rights and of copyright.

1.3.4 Patent

The concept of patent is that a strong protection is given for an invention in the industrial field. Though the criteria may differ between the jurisdictions, the Patens Act (UK) of 1977 (which may be used as an example) art 1 (1) gives the following conditions:

- (a) the invention is new;
- (b) it involves an inventive step
- (c) it is capable of industrial application;

Normally there are some specific elements that are excepted from patentability, art 1 (2);

- (a) a discovery, scientific theory or mathematical method;
- (b) a literary, dramatic, musical or artistic work or any other aesthetic creation whatsoever;

- (c) a scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer;
- (d) the presentation of information

These exceptions from the patent sphere can easily be regarded as set up due to a competition policy, since a monopoly in most of these fields would give a monopoly that is regarded to be too strong.

1.3.5 Some terminological problems arising from the differences between the different jurisdictions

Especially in the field of copyright, or authors right, there is a terminological confusion. Looking at continental jurisdictions you are apt to find the distinction between authors right and neighbouring rights. Such a distinction is not found under English law, where everything is protected by copyright.

There has been brought forward suggestions to solve this problem terminologically⁹. However there has not been any agreement between different commentators as how to solve this problem. Terminologically I will speak of Copyright protection of computer programs and databases, primarily because this is in compliance with the terminology found in the directives and proposals from the EC.

1.4 The aim of the essay

The aim of this essay is to discuss some of the problems arising from intellectual property rights and competition in the EC. To a large extent I will discuss copyright. Patents will be mentioned, but mainly to illustrate some aspects. The same will be the situation with trade marks.

Due to the limits in length, it is only possible to give a broad overview of the questions¹⁰.

2 A European dimension

2.1 The interaction between competition and free movement of goods

There is a connection between the competition rules and the provision of free movement of goods. This may be seen from two different standing points. One is that the competition rules are essential to obtain the free movement of goods¹¹, the other is that the free movement of goods (art 30) is a competition rule in a trans-european perspective.

Cfr *Bellis and L'Ecluse* 1991 p 29; First and foremost, EC competition law serves as a policy instrument to shape and consolidate a Community-wide internal market. This emphasis on market integration has been

¹⁰ For a general discussion of Intellectual Property Rights and the Community, see Groves et al 1993

¹¹ and services, persons, and capital

reflected in particular fields of law, such as ... the exercise of intellectual property rights.

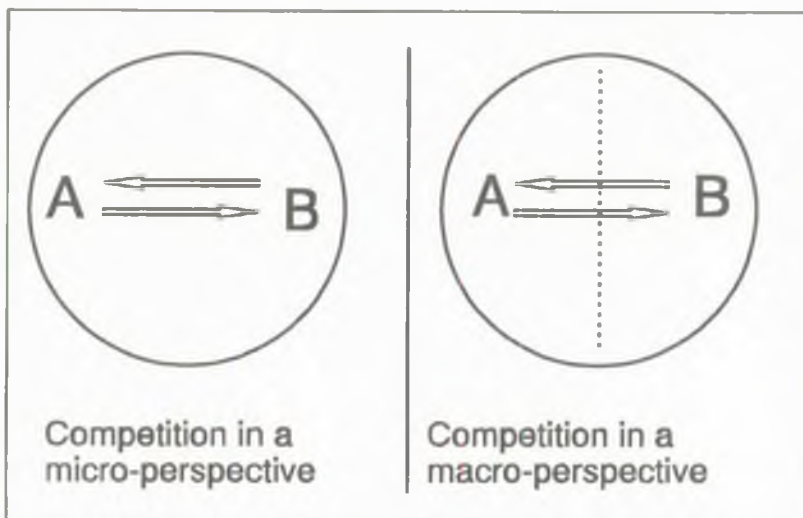


figure 2 Competition in a micro perspective and in a macro perspective

In a micro perspective there is the question of rules to set up competition in *a market*, between the different participants. As long as the market is functioning this will not constitute any problems. The macro perspective, which will apply to the European market, includes the problem that there is not one market, but twelve *different markets*. The aim is to combine these together as one *internal market*. Regarding intellectual property rights this may constitute problems, it is a possibility that the intellectual property rights may be used in a way that conflicts with the idea or concept of *an internal market*.

2.2 Europe 1992 - Intellectual property rights

The conflicts between the idea of the internal market - Europe 1992 and the existence and exercise of the intellectual property rights may occur in many field. One of the main problems is the national treatment of the intellectual property rights.

At this stage it might be useful to keep in mind that intellectual property rights might be divided into two different groups. The first is where the intellectual property right *per se* is the relevant aspect of protection, this would regard copyright, patent and chip protection. The other group is where the intellectual property right actually is used as a description of a producer or a product, typically this is trade-marks. With trade marks it is not the trade mark *per se* that is the real and underlying aim when it comes to protection, but the product the trade marks is connected with.

The problems I will deal with in this part of the essay are the national treatment of intellectual property rights, and the problems arising from the different criteria for obtaining protection in the different jurisdictions.

2.3 The problem with national treatment and the European Community - the exhaustion of rights or the rights granted the public over a copyrighted work

The first obstacle to competition in a macro perspective is the traditional national treatment of intellectual property rights.

Concerning copyright this problem is mainly with the exhaustion of rights, with trade marks the problem is that it may be used to hinder the

import of any product that has a trade mark from one member state to another.

Concerning copyright the exhaustion of rights - or the rights given the public over a work, of importance, are the right to sell and to rent the product. If a product is brought to the market in Denmark the right to resell it or hire it within the Danish market is permitted, since according to the Danish copyright act the right to sell the copy is exhausted within the Danish jurisdiction.

The problem is then how this should be dealt with to obtain a competition in a macro-perspective. Art 36 states that Intellectual Property rights *may be used* in a manner that conflict with the free movement of goods. Art 222 states that the Treaty of Rome shall "in no way prejudice the rules in member states governing the system of property ownership.

Hence there might be an antagonism between the free movement of goods and intellectual property rights. The conflict is obviously how this conflict is supposed to be solved. At this point there is some case-law from the European Court of Justice. In *Deutsche Grammophon*¹² the Court stated that:

it would be in conflict with the provisions prescribing the free movement of products within the common market for a manufacturer ... to exercise the exclusive right to distribute ... conferred upon him by the legislation of a Member State ... solely because [first] distribution did not occur within the territory of [that] Member State.

¹² Deutsche Grammophon Gesellschaft v Metro-S.B.-Grossmarkte

Furthermore, the court decided that article 36 of the EEC Treaty - which allows national prohibitions or restrictions on imports, export, and goods in transit insofar as the prohibition relate to protecting industrial and commercial property- deals only with the existence of such rights and not necessarily with their exercise¹³. According to Steiner¹⁴, the Court concluded that "Article 36 permitted prohibitions or restrictions on the free movement of goods only to the extent that they were justified for the protection of the rights that form the *specific-subject-matter of the property*"

A result from this is that the national treatment of copyright must be abolished in a way that the exhaustion rights should be based on a trans - European market; the exhaustion would occur for the whole internal market once brought to the market anywhere in the Community.¹⁵

Eg English does not have any general scheme of exhaustion of rights, since the same acts seems to be permitted over unpublished works as well as published works. The implication in this respect would therefore be that the rights granted members in the jurisdiction would be extended to cover the Community.

The next question is obviously if a product is brought to the market in one member state, hence the exhaustion occurs, and brought to another member state, should the exhaustion rights from the first or the second jurisdiction govern this? This was also among the questions in *Deutsche Grammophon*, where the court drew the

¹³ However this distinction seems hard to fit into some copyright systems, like the Nordic, see Dyekjær-Hansen 1993.

¹⁴ Steiner 1992 p 98

¹⁵ See Køktvedtguard 1991 p 43

distinction between the existence of an intellectual property right and the exercise of the same.

This was also among the problems in *Warner Brothers Inc and Metronomone Video ApS v Erik Viuff Christiansen*. Mr Christiansen had imported a video cassette from England to Denmark and offered this cassette in his video rental shop. Under the Danish exhaustion rights this would not be permitted, whilst it would be permitted under the UK Act. The Court held that the Danish rules should be applied.

With trade marks it is obvious that trade marks may be used to hinder import and sale in different member states. The problem normally occurs with the registration of a trade mark in different countries, which with a national treatment should imply that a product may not be imported from another member state and sold. This is a obstacle to the free movement of goods and the Court has in several cases not approved that the trade marks may be used in this manner, normally under proceedings concerning art 85.

2.4 Different criteria for achieving protection in different member states and different protection in the member states

The intellectual property right has no physical substance and is only protected to the extend provided by the law of the member state. This protection may differ between the member states, and does so. This may have impact on the trade or the competition in the community.

There are two relevant aspects; the level of originality or ingeniousness required to achieve protection; and the protection given. To some extent there is a connection between these two - in the question of infringement.

Already when it comes to the copyrightability of novels there are differences. An example may be Regine Deforges "La Bicyclette Bleue", which was charged of infringement of the copyright vested in Margaret Mitchell's "Gone with the wind". In France Ms Deforges lost in the city court but this was overruled by the court of appeal, whereas according to Danish law it was obvious that it was not an infringement¹⁶.

Also in the field of information technology there has been some serious differences. The most famous was probably the German requirement for originality to achieve copyright for a computer program, which is stated in the Inkasso-case¹⁷.

The main problem with the different levels of protection in the different member states is the free movement of goods. If any "work" is not protected in one member state, for example Germany, it is clear that it is permitted to make copies of the "work" in that jurisdiction. With the free movement of goods it should be possible to import these copies to a jurisdiction where they are protected by any intellectual property right, for example copyright. It is possible that art 36 could be used to stop such imports, but the extent is unclear. Even if it could be prohibited, it would be an obstacle to the internal market. Hence there is a demand for a joint protection scheme in the Community.

¹⁶ Koktvedtgaard 1991

¹⁷ For a general discussion of the requirements for obtaining copyright protection for computer program under German law, see Wiebe 1992 p 94-115

2.5 Actions in the field of competition and intellectual property rights within the EC

Traditionally, at least prior to the Single European Act, there was little action taken from the Commission. In the same time the Court decided upon several cases with competition, in a micro and a macro perspective, and intellectual property rights. This is mainly concerned with the infringement of art 85 and 86 - the general competition rules of the treaty.

With the Single European Act the Commission has passed several proposals for equalization of intellectual property rights within the community, of them some has already passed the Council.

In the *White Paper Completing the Internal Market*, the Commission proposed to create harmonization in the field of trade mark legislation, software, patent and chips-protection. See also the Green Paper on Copyright.

2.6 The interpretation of EC-directives

As all other legal instruments EC directives needs interpretation, there is a difference between the English way of interpretation and the one that is used by the European Court of Justice.

As Lord Diplock pointed out in *R v Henn*;

The European Court, in contrast to English courts, applies teleological rather than historical methods to the interpretation of the Treaties and other Community legislation. It seeks to give effect to what it conceives to be the spirit rather than the letter of the Treaties; sometimes, indeed,

to an English judge, it may seem to exclusion of the letter. It views the Communities as living and expanding organisms and the interpretation of the provisions of the Treaties as changing to match their growth.

3 Competition and Intellectual Property Rights

It may be argued that all the intellectual property rights are basically competition rules. But at some stage there may be unbalance between the intellectual property right and the competition rules.

This may be both the rules of monopoly and other aspects of unfair trading - depending on the jurisdiction in question.

The aim in this part of the essay is to look at the intellectual property rights as they are today and evaluate whether this is within the concept of fair trading or monopoly.

3.1 Two different ways to change the balance

From what I already have said there are two ways to change the balance between the rights of the IPR-owner and the competitor.

- Either you may use the competition rules, both nationally and art 85 and 86 in the treaty of Rome,
- or you may change the intellectual property law, to achieve the same result.

The difference seems to be that if you change or make new competition rules they may be more elastic in some respects. The reason for this is that you may use unfair competition as a *condition* to use the rules. Under the intellectual property rights this has been difficult up till now, but at least theoretically the same should be possible.

However there is a difference in the nature and scope of the different rules. A continental approach to unfair competition would partly be based on the fairness of the result. Under an intellectual property right scheme this would be of less interest. These differences should not be overlooked.

In the subsequent parts of this essay the aim is to give some indications as to, and examples of the way this problem is handled, especially in the EC.

3.2 Copyright

Copyright is normally based upon some simple exclusive rights for the copyright owner, normally the right to make copies, and the right to offer the work to the public.

The Berner-convention states in article 9 (1);

Authors of literary and artistic works protected by this Convention shall have the exclusive right of authorising the reproduction of these works, in any manner or form.

and in article 11 (1);

Authors of literary works shall enjoy the exclusive right of authorising:

- (i) the public recitation of their works, including such recitation by any means or process;
- (ii) any communication to the public of the recitation of their works.

From article 9 follows that not the copying of the whole work but also copying of parts thereof is an exclusive right. The same concerns the adaptation of the works.¹⁸

The Berner-convention opens for the member states to in certain circumstances might give exemptions from these rights, as the right to reverse engineering, at least in some cases, is¹⁹.

3.2.1 Computer programs

Computer programs are protected as literal works in most jurisdiction, in the EC this is stated in article 1 (1) of the Software Directive.

In one aspect is there a serious difference between computer programs and other literal works.

Traditionally the author produced a literal work and published it in some form. At the same time you shared with other members of the society the underlying ideas²⁰.

When an article was published in a scientific journal the article would obviously be protected by copyright, but the ideas stated in the article would be free for everyone to use.

When it comes to computer programs this is not the situation. A computer program is normally published or brought to the market as object-code. For a human it is not

¹⁸ See also Copyright, designs and patents Act (UK) 1988 s 17 cfr s 16, and the Norwegian Copyright Act s 2

¹⁹ The Software Directive art 6

²⁰ This argument is also put forward by Vivant 1991

possible to read the object-code and understand it. In order to understand it and the underlying ideas you will need either access to the source-code or undertake a reverse engineering.

To obtain a copy of the source-code you need an agreement with the person in whose possession the source-code is. This is normally the copyright owner or somebody acting on his behalf. Normally his interest in giving the source-code to any third party is limited- simply because he at the same time would give away the expressions and the ideas vested in the program.

The other way to get access to the underlying ideas in the program is to undertake a reverse engineering. Unfortunately this would normally mean that a copy would be made of the program, and this is, presumably, an exclusive right for the copyright owner.

Therefore in this respect there is a difference between computer programs and other copyrighted works.

There may be several reasons for wanting to undertake a reverse engineering; one is to get the knowledge that lies in the program, another is because one would like to make a program that in some respects shall interact with the present.

An example may be that somebody would like to make a telefax-program, which aim is to send and receive faxes on a PC. This may be made as a stand-alone program, but it is desirable to let it work within several word processors, so that the user simple writes the fax in his ordinary word-processor pushed a sequence of keys to invoke the fax-program, or simple define the fax-program as a printer that works with the word-processor. In these circumstances you would need to know several parameters to get this program working.

In the software directive there is given a right to reverse engineering - insofar as it is necessary to obtain interoperability with another program (the latter category above).

3.2.1.1 The right to reverse engineering under the Software Directive

Article 6 of the Software Directive gives under certain circumstances the right to reverse engineering. To the extend it is necessary to obtain interoperability with another program. Article 6 sets out a set of criteria that need to be fulfilled in order to fall within the scope of art 6.

The problem is that other aspects of reverse engineering is not dealt with by the directive. The question whether a decompilation, and output to the screen, is making a copy of the program is unclear in most jurisdictions, and may still constitute problems. This is criticised by Vivant²¹;

First a question which all the laws have in common: what is covered by the word reproduction, and representation?

Concretely, what does an individual when he puts software in a computer? Does he perform an action of reproduction which is *a priori* reserved for the holder, which makes him, unless authorized, an infringer? Does he only perform an action of use, *a priori* lawful, at least with regard to the general principles of the matter? ... The importance of these questions is obvious. But insofar they have not really been decided on, at least not in a resolute manner. In particular in the perspective of the question of the lawfulness or the unlawfulness of reverse engineering, uncertainty remains.

²¹ Vivant 1991 p 111

So the right to reverse engineering is to some extent uncertain. The right given by article 6 may not be the only possibility to perform any reverse engineering.

Within the scope of article 6 is the prohibition of there is no possibility for the copyright owner to deny anybody within the scope of article 6 to perform a decompilation.

Article 6 states that: The authorization of the rightholder shall not be required where reproduction...., and article 9 states that; Any contractual provisions contrary to Article 6 ... shall be null and void. this is a rather odd way to make this a prohibition, but it seems obvious that it is the meaning of the articles.

3.2.2 Databases

In most european jurisdictions databases are protected by copyright, even though there are no clear references to it in the copyright statutes in the jurisdictions²². The problem seems to some extent to be that some jurisdictions are giving a powerful protection for databases, namely the United Kingdom, which follows the skill and labour doctrine.

Traditionally the criteria for copyright protection for databases are "the Act does not require that the expression must be in an original or novel form, but that the work must not be copied from another work - that it should originate from the author." (University of London v University Tutorial Press).

There is a paradox inherent in the continental approach; if you have a exhaustive compilation, for instance a database of all cases decided by the Bundesgerichtshof this collection

²² COM (92) 24 p 19 ff

is not based upon any creativity by the organizer, hence should not be protected by copyright. Whereas a database that not is complete, for instance a database of the more interesting cases from the Bundesgerichtshof is based upon the creativity of the organizer, hence should be protected by copyright.

But there is a vast amount of work put into the production of such a complete database, in gathering the information, entering it into a database system, defining the extent of the material that should be entered into the database. It might seem as if it needs some protection. It seems desirable to extend copyright protection also to this collections or to offer a *sui generis* protection²³.

The essence of the skill and labour doctrine is to give protection on basis of the labour not on the originality. As such there is a risk that the copyright will be too strong and thereby create a monopoly on something that not is an intellectual effort.

It seemed as skill and labour doctrine also was in force in the United States, but this was denied by the Supreme Court in the case of Feist Publications Inc v. Rural Telephone Service Co. Inc.

The aim of the Commission was also here to bring the criteria for achieving protection to a common level in the community, this would deny the use of the skill and labour doctrine.

²³ As today is the situation in the Nordic countries. For a discussion in English of the "catalogue" protection see Karnell 1991

In addition to this; the Commission has proposed a *sui generis* protection for unfair extraction from data bases, which presumably is a better way to stop the unfair use of the work of other parties, without creating a monopoly for the specific type of compilation.

3.3 Examples where the intellectual property rights and the competition rules differ - and the competition rules are used to change the balance

As stated above it is possible to modify the contents of the intellectual property rights in order to achieve competition in some fields.

The interaction between intellectual property rights and competition law might work in two different ways. Firstly where intellectual property rights conflicts with competition rules, *supra* 3.3.1, secondly the competition rules works as an extension of the intellectual property rights, *supra* 3.3.2.

3.3.1 Intellectual property rights conflicts with competition rules

It is stated that whilst the Treaty of Rome does not interfere with the existence of intellectual property rights, *cfr* art 36 and 222, but the exercise of them may be in breach of articles 85 and 86.²⁴ Hence intellectual property

²⁴ Steiner 1992 p 174

rights must not be exercised in a matter that does not conform with the competition rules of the treaty of Rome²⁵.

3.3.1.1 Article 86

The problem in this context is where a intellectual property right gives a monopoly or a strong position that may be abused. If and to what extent this applies is depending on the framing of the intellectual property rights in the member state. If its gets to strong it seems obvious that it may conflict with article 86;

Any abuse by one or more undertakings of a dominant position within the common market or in substantial part of it shall be prohibited as incompatible with the common market in so far as it may affect trade between Member States.

Such abuse may, in particular, consist in:

- (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;
- (b) limiting production, markets or technical development to the prejudice of consumers;
- (c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;
- (d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

The enumeration in a-d are only examples on what may be deemed an abuse of a dominant position. The conditions under which article 86 applies are basically that there must

²⁵ Cfr Koktvedtgaard 1991 p 43

be a "dominant position", in "substantial parts of the common market" and that one uses such a position for "abuse". In terms of intellectual property this prohibition may apply if the intellectual property rights puts the owner in a dominant position.

It is obvious that it may be used even if the intellectual property is the reason for a dominant position that is abused. It is not necessarily because of the intellectual property rights that for instance Microsoft is in a dominant position. This is probably due to a good business strategy.

In one case the Commission has brought a case on the unfair trading and abuse of an intellectual property right, three of the four television companies in Great Britain and Ireland²⁶ used the intellectual property rights in the television and radio listing to prohibit the publication of independent television magazines. The commission found this in breach with article 86, by their Decision of 21 December 1988. The three TV-companies commenced proceeding for the European Court to get an annulment of this decision. Due to technicalities this was commenced as three cases²⁷, since they are all in principle the same I discuss one of them.

In *Radio Television Eirann v Commission* the Court concluded that the use of a copyright in the listing of television programs, that where protected by copyright was in breach of article 86, since the copyright in the listing gave a dominant position in the market of weekly TV-magazines.

²⁶ BBC, ITV and RTE

²⁷ BBC v Commission, ITP v Commission and RTE v Commission

It may seem obvious, but one of the problems was whether it was the publishing of the weekly listing or the television *per se* that was the market to be considered. Since the court found that the relevant market was the weekly listings, it seems as if this principle is to be used in other cases - a small part of a business that involves any intellectual property may be considered to be one market - in the meaning of art 86 - hence a potential breach of the competition rules.

The Television companies has launched an appeal against the decision. The written preparation finished in September 1992, but no date has yet been set for the oral hearing²⁸.

3.3.1.2 Article 85

The use of an intellectual property right may as well infringe with article 85. The criteria are not that different from the criteria in article 86.

Many of the trade mark cases has been based upon article 85.

3.3.2 Competition rules gives protection to extend the right under an intellectual property right

To the extent of my knowledge the Commission has not handled any cases where there has been any breach of the competition rules to areas where the intellectual property rights does not give protection.

²⁸ According to information from the information Service of the European Court of justice

It may be argued that the proposed *sui generis* protection for databases is such, but it seems more natural to regard this as a new intellectual property right, even though it is not based upon any intellectual effort.

One the other hand, it does seem to be to possible to use the competition rules of the treaty of Rome in such cases.

An example from outside the jurisdiction of the EEC is *Inter-Media Graphic Systems Inc v Aladdin Software A/S*, where the copying of a user interface was denied due to the Norwegian Unfair Competition Act. It seems to fall outside the scope of art 85 and 86 to give any protection against this type of unfair trading.

4 Conclusions

Since there is no antagonism between the concept of intellectual property rights and the concept of competition, the question is if the framing of the legal system in this field is balanced or not.

The main effort of the Commissions is to fulfil the internal market, and he competition rules. This has opened for rights not presently known in any member state, such as the right to reverse engineering - as an example of balancing interests.

At the same time the Court has changed the exhaustion rights from national treatment to a trans-european system. For the competition in a trans-european system the different legal protection seems still to be a problem.

The fact that the directives, such as the Software directive, has not dealt with some of the uncertainties that exists this may be an obstacle to the competition in the Community,

since when there is an uncertainty there is a change that peoples will be reluctant to use the rights they may be have.

As a total there seems to be an opening for more competition in the field of intellectual property rights, but there is not an unbalance between the predefined intellectual property rights and competition law.

The actions also differ among the different intellectual property rights. Patents has over the years developed with a system for granting of compulsory licenses, and the need for further actions seems smaller than with copyright and trade marks that due to the national treatment has made more severe problems.



Data protection - where next?

New dimensions to the life of Joseph K.

1 Introduction

Any decision has to be based on a certain amount of information, that is available to the person making the decision. This amount of information is in some respects limited. This simple principle applies both in the private and the public sector. Between these two sectors there are some differences - regarding public sector there might be some legislation stipulating that certain types of information shall be taken into account. In the private sector this is rarely the case.

Someone must have been telling lies about Joseph K., for without having done anything wrong he was arrested one fine morning.

Franz Kafka

The information must be brought to the person making the decision one way or the other. Normally someone is collecting the information or it might be given by the person affected by the decision. In some cases the information necessity might be transferred from another corporation or a public entity - it might be purchased. This might happen with or without the consent or knowledge of the person affected by the decision.

This information is necessary in the decision-process, and the result or outcome of the decision-process will depend on the information obtained. If the one party has an legal obligation to get one special outcome of the decision-process he will probably give all information to the other party, but this may check the information against other sources, to verify the information given by one party.

If this is an application for something and the result is negative and the applicant is only told the outcome of the application, but not the reasons for it, the situation is like that of Joseph K.

There are several different situations where the problem may arise; firstly the obvious the applicant is only given the negative result, secondly he is given the result and some "fact" on which the decision is based, but are wrong. In the first case he has no possibility to contest the outcome, in the latter he is in a position where he has to give evidence that the fact underlying the decision is wrong.

1.1 The use of computers - is the problem new?

The situation with decision making processes and the lack of relevance and relevant information has basically existed since the beginning of time, and has been discussed for about as long.

The introduction of computers has not made any new problems in this context, only stressed some old. Though the problems are more apparent and the situations in which information collected from different sources are used are becoming more apparent and happening more often. Namely the possibility of storing and communicating data, that prior to the information age, with the use of information technology, has earlier not been possible, is today possible. The problem seems to be that the society never has been perfect, but with the new methods of handling information, and making decisions this lack of perfectness constitutes a problem.

On the other hand, this problems exist and has existed for a long time also with manual information systems. But it seems in a smaller scale.

An other aspect is that today there is a greater need to obtain information, from other sources than was the situation some decades ago, this development has partly been together with the development of information technology, and partly beside this development.

The structures of society has changed, the need to make some inquiries before granting a permission or enter into an agreement, simple because you do not know the other party may be used as examples of this.

1.2 The problems

With the introduction of computers we have got new and improved ways of *storing* and *communicating* information. If something worked bad beforehand it probably works even worse this days, if thing worked good beforehand they should work even better with the use of computers. But this, is however, not necessarily the case.

1.2.1 The vast amount of information available to the decision-maker

There has been a development in two dimension, one is that there is more information regarding each and every one of us stored in different files, (manual or electronic) in different public bodies and in the private sector.

A foreigner entering the United Kingdom with the purpose of studying, is apt to be registered by the immigration authorities (which seems to keep a register of every time he crosses the border, his address, his reason for obtaining a residence permit etc), the University (which has some information on his previous studies, his present studies, his next of kind,

his progress in the study, his marks, his use of the email-system and other services in the international networks) and the poll-tax-register. In addition he would probably need a bank-account, and they may obtain some information from his bank at home, a students railcard, a coach card, etc, etc.

Some of these types of information has been collected for some decades. The new aspect, however, is the fact that the information technology opens for new ways of communicating this information from one register to another.

Therefore the decision-maker has access to a larger amount of information, on his fingertips. If the information in a manual file - stored away in a basement - is wrong this probably would never effect any decision at a later time. But when it is possible to access the information, by making a phonecall to an employee in the corporation or the public administrative body *or* by having on-line access to the information from the desk of the decision-maker *or* even having a subroutine in the computer-system verifying or collecting the information, the harm a small amount of wrong data may do is much larger. This problem arises in different circumstances: A term may describe different things in different situation. If an executive officer makes a note of something, in the context where he or she writes it *may* make sense, and have one particular meaning. But the moment it comes into another context the next decision-maker may probably not be able to make the right interpretation of it. Where something is wrong in the first place, it remains wrong also in other contexts.

There is a disbelief that the decision maker is capable of coping with this amount of data, cfr Forester and Morrison²⁹;

there is very little doubt that the technological capabilities to gather awesome amounts of personal information has increased exponentially in recent decades, there is even less doubt that the abilities of humans to judge the worth and validity of such *data* (as compared to information) has not improved at all.

1.2.2 The assessment for the decision maker

For the decision maker the assessment is based on a mathematical formula that is quite simple. If the expenditure to gather all relevant information is higher than the profit involved, the information will not be collected. There has to be drawn a balance between the expenditures involved and the profit (or other measures) involved. If we stick to a bank as an example; the bank needs to make money on their business. In doing so the bank must make sure that the accounts are not overdrawn, and that the mortgages offered are good enough for the loan, and of course that the loan will be repaid as agreed upon. There is not in the interest of the bank to make any judgement of all costumers - to collect all relevant information before any decision is made. The assessment by the bank will typically be based on some simple parameters. This will be to expensive, hence not remunerative. Benefits, typically from the government, has to be based on some parameters. The same is for payment for goods or services. In both these categories there has been a move away from the balancing of the duties of the

²⁹ Forester and Morrison 1990 p 92

parties into a system that is based on other parameters. An example in the latter category is the payment for water used, found in some jurisdictions³⁰. Earlier the water company would set up a meter in your flat, but today this is based on different parameters. In some municipality in Norway you pay according to the size of your flat or house, and in others all households pays the same. The reason behind the change is simply that the manpower of verifying the amounts used is too high. Social benefits should theoretically benefit those who need it most. If this was to be taken literally every aspect of the applicants would have to be considered carefully. Normally this is not done.

An example; the Norwegian housing benefits is not based on your actual house expenditures and your actual income. All you have to do to apply for housing benefits is to tell the authorities your personal identification number³¹, and they will check your latest reported income by the inland revenue (which until the end of 1993 will be for 1991), and with the national register to find your registered residence. This will be controlled with the GAD-system which tells the floorage of the residence. Of course it will also take into account any other persons registered at the same residence. Based upon these parameters they will decide whether you are entitled to benefits and how much. Nothing in this process is done by humans, every process is done automatically by computers. For the Norwegian government this is an extremely inexpensive way of handling

³⁰ However not in England, where after privatization the costumers pay per gallon used.

³¹ a eleven-digit number where the first six is the date of birth (dd-mm-yy), 3 digits identifying the person and the two last is control digits based on some mathematical algorithm and the first 9 digits.

this type of requests. From this economical point of view it seems of less interest that it may take up till two years from you loose your job till you are entitled to the benefits. So far this has been examples on the pressure towards automatic processing. In Italy there seems to be a regulation stating that all rules that are to be made shall be made in so a matter that they are possible to be handled automatically³².

1.2.3 Some information may -wrongly- be regarded as prima facie

In many corporations, institutions and public administrative bodies there exist security precautions; control of access to the building, a part of the building, etc; control of the access to documents or files on the computer system, etc. These obstacles are made so to stop anybody who has no right to access and let the ones who has the right to access pass trough. To pass these obstacles there has to be a control of something to find out that the person really has the right of access. Normally this is not the person as such or any part of him or her, but something a person is supposed to bring or remember. The access to a computer system is normally based on two things, the general known user-name and a secret password. To pass a physical obstacle this may be a key, a pin-code, a plastic card or a combination of the above mentioned. Security systems will often have the possibility of making a log of who (rather what) passed where, and who (rather what) tried to pass where. If a physical security system is based

³² Claimed by Prof Schnellen at a seminar held by NACAL, september 1991

only at a card, there will be a log on where this card has passed.

The normal assumption is that the "owner" of that card also passed. This however is not necessarily the case. One might borrow the card of a colleague or a card with a magnetic stripe (like an ATM-card) might with the correct hardware devices easily be copied.

In many cases this registration would be regarded as *prima facie* evidence. Hence place the right owner of the card in a uncomfortable situation, where counter-arguments hardly will be accepted. Take the example of theft from a hotel-room, the log indicated that the card of a certain room-maid has passed the door at the time of the theft. The hotel (and the police) would probably regard this as *prima facie* evidence that the room-maid entered the room. Her possibilities of raising counter-evidence are limited.³³

1.2.4 The struggles to makes decisions by computer

Traditionally, at least we like to believe, decisions where based on what was the best in the present case - as an overall. A banal example; some years ago - at least in Norway - you paid for the amount of water you used, but this is today based on the size of you home, in square-meters. The reason for this is obvious. It is much easier to base the prizing on some permanent factor than to employ controllers to walk around a checking to water-meters in everybody's houses. There is not necessarily any coherence

³³ The extent of this argumentation would obviously depend of the evidence law in the jurisdiction in questions, but one must however not only take regards for the criminal sanctions.

between the size of your home and the amount of water you are using, but this is sacrificed to reduce the work. This struggle to reduce work and let decision be made on information already present somewhere is growing. A few examples will - hopefully - clarify this: *The Norwegian housing benefit*, supra, and the *Italian aim*, supra.

1.3 The solutions or the challenges to the legal system

Some of this problems are normally regarded as *questions of privacy*, at least in the common-law jurisdictions. This constitutes two essential questions:

- Is there a connection between the concept of privacy and the problems described above? and
- Is it possible for the United Kingdom to rest upon the concept of privacy? Especially in a European context?

1.3.1 The concept of privacy

The concept of privacy originates partly from the amendments to the American Constitution and partly from American literature and case-law. It constitutes a sphere-theory that something is private, hence shall not be removed from the private sphere.

According to McFarlane and Davis (1984) p 224 there are two widely recognized definitions of privacy; "Westin proposed that privacy is 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about themselves should be

communicated to others', and Miller defined it to be 'the individual's ability to control the circulation of information relating to him'

The problems with the next generation of data protection laws lies to a large extent in the use of information. To some extent there is a interconnection in this, but some of the basics are different.

In setting up a rule or a set of rules for a new situation, it must be possible to base this on the present. The limitations in this is the problems that arise *if this not is able to give the relevant protection*

1.3.2 The continental european approach in conflict with the concept of privacy

Since none of the continental jurisdictions has the same concept of privacy as the US, neither in their constitutions or in doctrine, there has been a development in an other direction to cope with the same problems. This is to a large extent based upon a balancing of the interest of the parties involved³⁴.

From this it is easy to demonstrate that there is a conflict of methods within the european communities. Since the problem of data protection to a large extent has to find its solution within the European Communities, *infra* 4, this constitutes a conflict between the common-law approach to the problems and the continental approach in finding the European approach to the problems.

³⁴ For Norwegian law, cfr Bing 1991a

The outcome of this dispute is not easy to predict, some of it may be found in the proposal for a Directive, *infra*.

It is easy for anyone from a Continental jurisdiction to claim that the Continental system is the better, and that the UK should leave its connection to the US doctrine. But it is not this obvious that the commentators and the legislative authorities in the United Kingdom will except this.

1.4 The problems dealt with in this essay

The aim of this introduction is much broader than traditional concept of privacy, as found in the common-law jurisdictions, so is the aim of this essay.

Whilst privacy during the times has found its signification, the same is not the case with the concept of data protection. The term may be understood in a broad sense, or as a mere continuum from the traditional concept of privacy.

In this essay my aim is to take a broad approach to the problems and I will try to draw the attention to some aspects of the use of information technology in the society, and the impacts this has or most probably will have. This will constitute challenges to the legal system in a broader sense than what is normally dealt with under the label of privacy or data protection in some jurisdictions.

At the same time I will not deal with the present generation of data protection legislation, but try to look at the developments and challenges that exist today and are apt to come in the next few years.

This makes it necessary to look at the basic principles of communication theory, and the practical impacts thereof, as

well as to stress why the solution has to be found in an European context, and not within the different member states.

2 Communication theory and some of the problems with communication

2.1 Basics of communication theory

The theory of communication goes back to some articles by Claude Shannon, Warren Weaver and Norbert Wiener dated in the late 1940's³⁵. The theory of communication characterizes communication as a process, where one party wants to influence another by or with information.

The language used is governed by two sets of rules, the semantic and the syntactic. The medium is a matter for the ability to communicate or rather to hold information.

One aspect of communication theory that is interesting in our context is the communication of information or data between two or more persons. To make the model as easy as possible I will only use the communication between two persons.

The illustration in figure 3 shows the way information is handled in a communication process³⁶.

³⁵ Bryde Andersen 1991a p 97

³⁶ This drawing is fetched from Bryde Andersen 1991a p 102

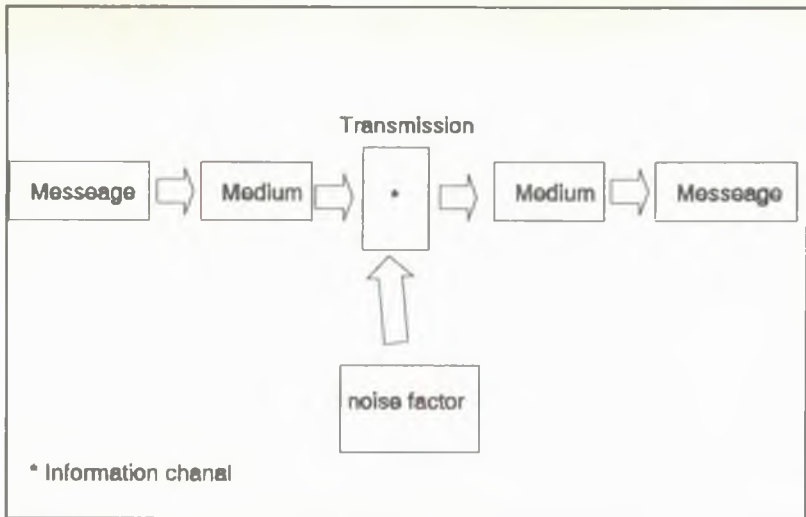


figure 3A model for communication

It is not possible to give the exact information from one person to another, it has to be communicated in one way or another, according to certain rules accepted by both parties. The first step is that the person who wishes to communicate forms a message, normally this will be written, but it may be graphical, in drawing or other ways. A combination is also possible. This message has to be connected to a medium; paper, a computer system or whatever. Then this message has to be communicated to the other party - there has to be a transmission.

At every stage in this process there is a change that the input or the original intended message is changes or modified. At this stage we may point at two basic problems in communication; the vagueness of the language and the other the awareness of the different meanings.

2.2 The vagueness of the language - the jargon used in some parts

Even though the person wanting to communicate knows exactly what the message is supposed to be - it must be brought out of the head of the person and - normally - into writing. Here lies the first problem; it is not always possible to describe exactly the meaning in the written language. The language is too vague. Traditionally we have used the word *forrest* as an example³⁷ - how many trees must there be present in order to be a *forrest*?

Even if the communicator uses an almost precise word for what he wants to communicate the next problem is the recipient - he may not be aware of the term means. This comes more obvious in the context of jargon used in different parts of the society.

The European dimension, *infra* section 4, this problem will be even stronger, because of the different languages involved. Either there has to be a translation, which causes disturbance to the message or one language must be used. The problems described here are obviously more prominent when persons have to use a foreign language.

2.3 The problems with the lack of awareness of the communication process and the different meaning of words

This is a problem that has been stressed in legal theory for some time, and has a connection to the problems with the

³⁷ At least in jurisprudence in Norway

vagueness of the language. The users of information technology are normally not aware of the possibilities that systems opens for, and the concrete use of it. It is natural to make the same statement as you would in a traditional paper based system.

The first generation of computerized systems normally just did the same job as the manual systems they replaced. Such that there was basically little new in a communication process. Typical examples of such systems is national registers, tax offices, etc. At the same time there has been a transition from the use of manual storage media (such as paper) to electronic storage media (typically a computer), by the use of for instance word processors.

Under such manual systems it is obviously difficult to obtain the information that lies in them; one would have to make a phonecall or even write a letter to the person or body who holds the file.

One of the concerns is with a transition to computerized files the lack of awareness that previously not constituted any practical problem will constitute some.

There are some examples of this problem given in legal theory, I will just mention some of the concerned that has been put forward.

Criminal intelligence at its worst is simple gossip, the following extracts are a transcription of a two-page police collator record from the Skelmersdale Division in Lancashire³⁸;

Robert Jones of 14 Crosby Road, Newton - known affectionately to his CB mates as 'Tiny Tot' - paid another return visit to our fair Division at 3.30 a.m. on 15.7.82 when he was stopped/checked in his nifty yellow Ford Galazy PXY838A. Gracefully reclining in the passenger seat was none

other than school breaker, a suspected druggie, James Richard Dack (30.3.62) (wounding, burglary, theft,damage) whose unforgettable features are pictured left [A photograph depicting a black person is included.] Dack, a state benefit subscriber, augments his hard-earned dole by working on the door at Talk of the Town, keeping out other undesirables. Jones and Dack are well acquainted with the finer point of our division and are worth every stop/check they can get.

The question arising is how other persons would be able to interpret this message, and use it in their own decision making.

2.4 The problems of the group interests

Connected to this is the group interest. One group of data controllers or data owners has a specific task in society, for instance the Police³⁹ "see their role as the prevention of crime and the apprehension of law-breakers. The maximization of this function is of supreme interest to them and the costs associated with invasion of privacy, wrongful arrest, forced confessions and even fabrication of evidence, can often be considered to be acceptable as long as the primary role of the police in the prevention and apprehension of criminal elements is achieved ."

Even if it is not done to the extent that is described as a possibility, it is easy to assume that this is an element that will be present to some extent.

³⁹ Forester and Morrison 1990 p 100

3 The collection, storage, use and abuse of data in an automated process

3.1 A database

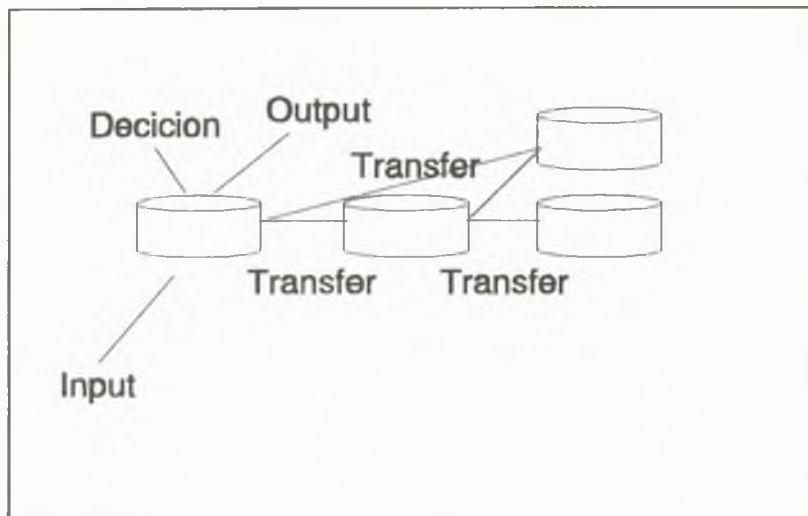
Data needs to be stored in some kind of a database. We may divide the types of databases into two different kinds of databases, cfr Bing 1992.

One is text retrieval systems, where the text is in ordinary language, and it is up to the user of the system to search for words that are present in the text. A typical example of this may be LEXIS - a legal information retrieval system..

The other group is may be called database services, there is information on a specific subject, and these information are dyadic, consisting of one definition and one variable. An example of this is the vehicle owner register. This may contain name, sex, date and place of birth, type of car, registration number of vehicle as well as other information.

3.2 A model

Data is gathered from several sources, this may be as easy as that the person on question voluntarily gives the information. If the information is necessary to get any benefits the person may be more than willing to give the information. The data may also come from other sources, such as the employer, the GP, the dentist, the Children's Officer, the bank, or theoretically any other source. Some of this data would fall within the definition of electronic



traces⁴⁰.

Once entered one information system it is easy to use the same information for other purposes than intended. As shown above, page 41, with the Norwegian housing benefit system.

This is by some commentators called the Mosaic effect⁴¹, and one of the aspects is that when information is gathered from different sources the result will be more than intended.

Not only is it possible to use it as input for a decision-making, but it may be used to verify information given in other circumstances. It seems clear that one person cannot

⁴⁰ Cfr Bing 1991b

⁴¹ Cfr Forester and Morrison 1990

at the same time unemployed, hence receive unemployment benefit, and be employed by a company; a person cannot at the same time be blind and drive a car; a person cannot at the same time be a student and unemployed (in most jurisdictions).

It seems desirable to use information from one source to verify the information in other systems. For example if you match the persons receiving unemployment benefit with the persons employed (if there is such a register) one person should not be in both. Also you may match the persons receiving unemployment benefits with the persons receiving student loan or similar benefits.

From an economical point of view this is efficient. You will not have to use the same amount of labour to gather the information, and the decision may also be automatically.

If you are using a free text retrieval system this will have to be done manually, but if you are using a information system which has predefined data-fields, *this may be done automatically*.

There are several problems involved in this;

3.2.1 The reason for the gathering of the information

The reason for gathering the information may not be the most obvious problem, but it gives limitation to the usefulness of the information. In a system where you cannot give precisely the information you want, but have to adapt to the information system it is easy to make the interpretations according to your own use of the information. Also; the person who types the information

may have his or her own interpretation of the information that is entered into the system.

Even if the data is entered according to the "label", the same "label" may mean different thing in different circumstances.

Such an easy term as income, may (depending on the jurisdiction) mean gross income, gross taxable income, or net income (after tax).

3.2.2 The accuracy of the information

The question of the accuracy of information may be two different elements.

The first is that the information - at the time it is entered into the system - is false or not as precise as it should be.

The second is that the information may be outdated. Either the database-owner does not update the information and the information may be used by somebody else at a later time, or somebody has an obligation to update the information, but is not doing so.

3.2.3 Questions of security

There is also a question on the security for the stored data. Normally this is view as a problem of unauthorized access to the data, but another aspect is also present.

Access control systems may be based on one or more different things; either that the person knows something (a

password), or that the person is in the possession of something (a key, a card) or some distinctive characteristic with the person (his fingerprints, his DNA structure)⁴², or combinations of the above. It is also possible to restrict access control so access only is permitted from certain places (a certain computer, computers in a certain building).

Access to a computer is normally dependent on a username and a password (something the person knows), but it is also often restricted to access only from within a certain network. Access to ATM-services⁴³ are normally dependent on an ATM-card (something in the account-owners possession) and a PIN-code (something he knows), though it is possible to set up systems that are based in fingerprints or DNA-structures. Instead of entering a card and a PIN-code, you may set up a terminal where you only need to press your thumb towards an optical reader that checks your fingerprint against the registered fingerprint in the central database; or press you thumb against a needle that takes a blood-sample and controls the DNA-structure against the central database. A variant may be that you carry a card with the structure, this way it is not necessary to use a central database.

Towards an open electronic society, with access from different places this security problems comes more apparent than ever. As long as systems are to be open the risk of unlawful entries are increasing. This indicates that there should be a possibility to verify who has got access from where, and what did the person do. Concerning the latter; if data is changed it should be shown who entered the data, when the data was entered. This makes it possible to verify the data at a later stage.

If I as a data-subject would deny the data that is registered about me it should not be possible to spurn this by saying

⁴² Selmer 1992

⁴³ Automatic Teller Machines

that "this is all in our computer, that never makes any mistakes". On the other hand, if I alone am trying to deny the accuracy of the data it would be my word against somebody-who-at-one-time-entered-this into-the database. And if it is not possible to trace that person or verify that the data has been entered according to some procedures, this is difficult.

This constitutes a dispute, which it may be difficult to solve. In addition to this, the data that has been manipulated may be transferred and used as a basis for decisions made by the owner of the database in question or other institutions.

When it comes to ATMs in most of Europe there has been disputes on whether the money that has been withdrawn by the account owner or not. This is a question of evidence, and it seems as is the banks in most jurisdictions are claiming that it is not possible to fool the system, whereas the consumers claims that they have not used their cards.

But in addition to the problems that may arise in the dispute comes the problems this may give the account-owner because of the wrong data. Firstly he may run into financial problems, because the bank probably will refuse him to use his money, he may also get difficulties paying his other debts and may be blacklisted as a "bad payer".

The problem of unauthorized access has two aspects; the first is the possibility to see and obtain the information that is stored; the second is the possibility that information may be changed.

This may be in two different ways, one is by hacking into a database. The other by getting access by a wrong indicator.

If the database of the local social security office has been intruded I may find my privacy violated because they found information about me, but I may also become furious when I discover that the data has been modified so I do not get the benefits I am entitled to.

Inside one system the problem is the possibilities for data being misrepresented in one way or another. There must be routines to make sure that the data not is being altered, into misrepresentation. If a system contains of sub-systems there is also the problem with communicating and converting data correctly. It is possible to make some routines to verify the information that is transferred.

4 The European dimension

The European dimension in this problem has several aspects;

The first is that there must be a free movement of data within the Community, this is actually a prerequisite for the four basic freedoms.

The second is that the Internal Market, without borders, creates a vast amount of dataflows between the member states - the Schengen agreement entered into by some of the member states hopes to achieve this.

The third is that different levels of data protection regulations in the member states may constitute technical trade barriers or favour one or more member states.

4.1 Free movement of data as one of the basics of the Community?

The 4 basic freedoms of the Community are: free movement of goods, services, persons and capital. It seems obvious that in order to achieve this there must be a free movement of data corresponding to the movement of goods etc.. It is

not possible to create any free movement of goods, services, persons, and capital without the data that is connected with it. With the export of goods from one member state to another there has to pass some information regarding the same goods. So is the situation with the other three basic freedoms.

4.2 The data-flows generated due to the internal market

One of the impacts of 1992 is that there shall be no borders, no physical borders between the member states, no customs control, no immigration control. This is not yet the case, but the struggle is still on.

Some member states has some problems in this respect. Foremost this is the case with Denmark, that due to the conventions on reduced border control between the Nordic countries will have difficulties in opening the border to Germany. This is also a problem for the Community as such. The united Kingdom is also having a more relaxed attitude in this matter, but this is due to internal considerations.

Immigration control, custom control etc had several aims. The main aim of these control-systems was a control of what passed the borders. This is interesting in several aspects; for tax-purposes, for investigating criminal offence etc.

There is still a need for some of these control functions, this is one of the reasons for the Schengen-agreement of 14 June 1985⁴⁴, entered into by some member states.

⁴⁴ Bing 1991b p 167

4.3 Technical trade barriers or favouring one member state

One of the traditional problems with trans-border dataflows has been that you could export data to "data-heavens", or jurisdictions where the level of data-protection was lower than in your own jurisdiction. This is still a problem in the Community, since the levels of data-protection is not the same.

The problem with refusing export of data is minimized by the Council of Europe treaty and the OECD-guidelines, in the respect that no member state can refuse the export of data to another member state so long as the latter is fulfilling the qualifications set out in these instruments.

This indicates that if this is upheld, there may be more favourable to have a data-base and data-processing⁴⁵ in one member state than in another.

5 Is the proposal from the Commission sufficient to cope with these problems

So far I have pointed out some of the challenges to data protection in the year to come, and also given some indications as to how they may be solved.

⁴⁵ The aspect of data-processing might be due to a lack of adequate protection in one member state, or merely due to lower costs for the service.

In the last part of this essay I will briefly discuss the what extent the proposal from the Commission is coping with the problems highlighted above.

The Commission has on 15. October 1992 released an amended proposal for a directive on data protection, COM (92) 422. The aim in this part is to evaluate whether this proposal is giving manageable solutions to this questions.

The time perspective on this is that the directive, if enacted, shall be implemented in national law within 1. July 1994, and that all data processing shall be within the limits of the directive within 30. June 1997. (Blume 1992)

There are some interesting differences between the directive and the present legislation in most member states, among them that the regulation is not any longer concerned a register or "data files"⁴⁶ but "the rights and freedoms of natural persons with respect to the *processing of personal data*, and in particular their right of privacy"⁴⁷ (my italics), and that also manual processing to some extend is included⁴⁸.

Article 17 states that there shall be taken "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration or disclosure or any other unauthorized form of processing.", and that they shall ensure "a suitable level of security". But there is no further set of rules as to the impact of this, it would be desirable if this would be prescribed. Taken

⁴⁶ as used in the first proposal

⁴⁷ Article 1

⁴⁸ Article 2, b

into consideration that there is a working comity in data security in EEC this seems odd.

The task to ensure the data quality is basically left to the member states⁴⁹, and the proposal only gives some vague guidelines that are similar to the vague principles in today's Data Protection Act (UK). Since this, and the problems with system security has the possibility to create technical trade barriers there is a possibility that the principle of subsidiarity has been drawn to far.

The other problems dealt with in this essay is given little consideration in the Proposal, with the exception of some provisions regarding the transferring of data, where there is a main point that the data subject shall be notified in some circumstances⁵⁰.

At the same time it should be noted that due to the principle of subsidiarity, there are some possibilities for the member state to develop derogations from the directive, as with article 8 - concerning sensitive data.

The main reason for this is the fact that the problems dealt with in this essay falls without the scope of the Proposal. Since the Proposal deals with the rules for the processing of data, and this essay to a large extent dealt with the results of the use in a decision process. But the connection is that the possibilities for processing of data opens for the use of it in a decision process.

⁴⁹ Article 6

⁵⁰ Articles 10 and 12

The fields in the Proposal that is covered by this essay is to a large extent left to the member states to decide. Hence not solved in a international context



The problems with information crime

In the Canadian Case of *R v Stewart*, Mr Justice Krever stated:

Confidential information is not property for the purpose of the law of theft ... If this interpretation should be thought to be inadequate to meet the needs of modern society, particularly because of its implications for the computer age, the remedy must be a change in the law by Parliament.

The problems of applying existing criminal offenses in an information context
- and an attempt to solve it
-with the emphasis on the crime of theft

1 Introduction

*"Our society has reached a phase at which information has become a "commodity", which is replacing material goods to a considerable degree. As a product, information, has become an indispensable element in our everyday thoughts and acts which is worth a lot of money. It may take many forms, ranging from the news of far-slung calamities via satellites or the rapid exchange of financial data over immense distances essential for the functioning of world markets, to systematically-accessible information in medical data bases."*⁵¹

This increasing information flow has at the same time released a demand for a strong protection of the same information. It is argued that the traditional legal systems, made for the industrial society is not sufficient in the post-industrial society.

One of the aspects that makes regulating information difficult is that the liberation of information and media is a new concept, and a new challenge to the legal system - dealing with information, *per se*. Traditionally the focus has been at the media carrying the information - not the information itself - this due to the fact that the media is "closely associated with the information"⁵². Hence stealing

⁵¹ Dommering 1991 p 1

⁵² Bing 1981 p 219

a book would be subject matter for theft since the paper and ink are movables⁵³.

In this context Sieber⁵⁴ states that "that common ground for this problems originates from the fact that all criminal codes have, to the present, predominantly protected tangible and visible objects. The *protection of information and other intangibles* existed, but did not play a dominant role until the middle of the 20th century." (footnote omitted) By Saxby⁵⁵ it is argued that so "far as the criminal law was concerned, abuse of property rights within the laws of theft and criminal damage assumed that the medium and the thing of value were inextricably linked. Thus information itself could not be stolen, but a piece of paper containing confidential information could." See also Coleman 1993 p 174.

This has lead to the new concept of *information law*. This term is rather new, but it seems to be generally excepted to cover the general problems with law and information in a rather broad meaning.⁵⁶

It is argued that in order to understand the concept of *information law* it is necessary to start with "an analysis of the subject in *non-legal terms*"⁵⁷.

⁵³ However in relation to securities the Norwegian Supreme Court has not upheld this distinction, and states that in this respect there is of no relevance whether the information is stored electronically or in a more traditional file, cfr Rt 1992 p 1629.

⁵⁴ Sieber 1990 p 120

⁵⁵ Saxby 1990 p 219

⁵⁶ Cfr Bing 1981, Bull 1985 Dommering 1991, Dommering 1992, Sieber 1992 p 17. Saxby 1990 seems to be of the same opinion. For a total overview of the problems of information law, see Altes et al 1992

⁵⁷ Dommering 1991 p 11. See also Saxby 1990 p 220

In relation to computer law it is argued by Bryde Andersen⁵⁸ that "In ordinary "lawyers law" the necessary legal and factual knowledge is typically sufficient known by counsel. "Understanding" the case seldomly presents substantial problems. If it does, the remedies are usually at hand. In a case concerning liability for poisoning, counsel's own knowledge on the human organs etc. will suffice as a basis for additional knowledge to be obtained by expert testimonies etc. In computer cases this is different. An equally sound basis of knowledge on how computers work etc. is rarely at hand for the average lawyer. Notoriously lawyers - like computer users - have great difficulty in grasping what a computer is and how it works. This difficulty seems to be more profound than in other areas of law with complex matters." At the same time it is clear that this statement does concern computer law as such, and not only the liability aspects of it⁵⁹.

The area necessary to describe in respect of information law is not necessary the same as within computer law; it is argued by Dommering⁶⁰ that "such an analysis is made with the aid of knowledge gathered from communication science, informatics, media economics and telecommunications science. The emphasis is not, however, on the information technology, but on the communication process".

This essay will deal with information crime. Generally the theme of the new doctrine "of 'criminal information law' is founded on the still developing general concept of 'information law' and 'law on information technology'. In accordance with modern cybernetics and informatics, the *new concept of 'information law'* recognizes information as a third fundamental factor besides matter and energy. Based on empirical analysis, this concept evaluates information

⁵⁸ Bryde Andersen 1991b p 122

⁵⁹ Bryde Andersen 1991a p 67 et seq

⁶⁰ Dommering 1991 p 11

both as a new economic, cultural and political asset, and as a specific danger potential. The new theory of 'information law' realizes that modern information technology alters the characteristics of information, especially by strengthening its importance and by treating it as an active factor that works without human intervention in automatic processing systems"⁶¹.

Computer Crime has as its starting point computers and communication between computer (not communication as such). The distinction between "computer crime" and "information crime" lies in the fact that "computer crime" is concerned with the computer as a victim, as a means or constitute the environment of the crime, whilst "information crime" is concerned with the information - not the computer.

The Law Commission for England and Wales in their report on computer crime⁶² defined the nature of the subject as "the misuse of computers or computer systems by parties not entitled to use or control those computers, either by simply seeking access to the computers, or by going further and using the computers or amending the information held in them for what may be a wide range of ulterior motives" (footnote omitted). They also identified a number of misuses done by or with a computer - or with a computer as a target. The same approach of identify misuses are found in the Scottish Law commission⁶³. Lloyd⁶⁴, notices that "each agency or legislature involved in the topic has set out its own agenda for action. Although the particular categorisations adopted may vary, three common threads can be identified in their work. These encompass the topics of: (a) computer fraud, (b) damage to data or programs, (c) "theft" of information." The concept of computer crime is

⁶¹ Sieber 1992 p 17

⁶² Law Commission (England and Wales) p 1

⁶³ Scottish Law Commission p 3

⁶⁴ Lloyd 1993 p 205

also to some extent criticized, as being a collection of different questions just treated together due to the involvement of a computer - one way or the other⁶⁵.

"Theft of information" might appear within the context of a computer system, and also outside. In the *de lege lata* discussion, infra 3, it will be shown that there has been case law in both categories.

With this general introduction the theme of this essay is given, first it will be necessary to look at some of the underlying problems of "information law" - which also will illustrate the problems of applying existing criminal offenses to information. This will have to cover a large part of this essay. This seems to be necessary, in order to make some conclusions *de lege ferenda*, due to the approach chosen. Before this *de lege ferenda* discussion I will give a brief overview of the situation, *de lege lata*.

2 Information law and information crime - general considerations

In this part there are a number of aspects to be discussed. The first is an attempt to describe or define information, the second is to give some indications as to the economics of information, the third to be discussed are some aspects of the nature of information, which indicates that a more traditional "ownership" construction is not applicable.

⁶⁵ Tapper 1987 p 4

2.1 Information

A starting point would be briefly to look at the concept of information, and the connection between information and the media carrying the information. It seems as especially this connection, *de lege lata*, makes problems and causes confusion in many jurisdictions. But - it must be emphasised - that this connection will be relevant also in a *de lege ferenda* discussion.

2.1.1 The concept of information

In a legal context *information* is traditionally used loosely as a synonym for data, news or similar loosely given matters. There is no stringent definition found. In information science, on the other hand, two main definitions may be found.⁶⁶

The first is based on the *communication theory* formulated by Shannon in 1948. This theory defines information in terms of the probability of the occurrence of a certain event or the reception of a certain message. The less probability of the occurrence of a the event or the reception of the message, the higher information contained by that event or that message. This definition of information does not seem to be helpful in a legal context⁶⁷ for the discussion of information law.

In *information and computer science* information is usually taken as knowledge or new knowledge. At the same time it

⁶⁶ Cfr Bing 1981 p 221

⁶⁷ Cfr Bing 1981

is conventional to distinguish between information and data. Where data⁶⁸ has to be communicated (received) and understood in order to transform into information. This seems to be a more likeable starting point for a legal discussion, it should at the same time be stressed that this makes information a *relative* expression in that different people will receive different information from the same data.

For the purpose of this essay it is stressed that information to some extent is synonymous with knowledge or new knowledge. This stresses two factors. The first that information is *relative*, in the sense that it gives different knowledge to different persons (if you already have the information, there is no use in getting it again). Secondly that it is the use of the information that seems to be the relevant point, not the "possession" of the information itself. This becomes apparent, eg in the discussion of the economics of information, *infra* 2.4.

2.1.2 Ways of communicating information

Historically, information - or rather the commercial use of information may be divided in three categories. Contract of services or contract for services; the sale of the information embedded in a physical medium; the trade with information without the same physical embedding.⁶⁹ The same three categorizes are still in use, the historical impact lies in the development of the ways of communicating information.

⁶⁸ made up of sign, ie letters, pictures, movements etc.

⁶⁹ Cfr Bing 1993 p 105 ff

The *contract of services or contract for services*, is illustrated by the fact that someone is employed or contracted due to their knowledge - not due to their physical strength etc. This is a basic way of communication information, and has probably been around since time immemorial. Knowledge has a price and it is a way of communicating information, and a payment of some kind has always been involved. Bing⁷⁰ uses this example; If you give me a leg of a mammoth, I will tell you where there is good hunting.

The *sales contract* came into existence with the development of a written language, and the development of medium for carrying the same information. This is a convenient way of "mass-communication", since the information may be duplicated in a certain number (though there are limitations). Through the history of man there has also been development in the media⁷¹, and the production techniques⁷².

With the information age came the possibility of *separating information from its medium*. This opened for mass-communication of information in a new at yet unknown way. It should be stressed that logically this category includes both *digital* and *analogous* information, typically information stored on a computer and broadcasting. But today we see that this analogue information is moving into a digital environment (CD's instead of records, ISDN instead of analogue telephone, digital HDTV instead of analogue television).

⁷⁰ Bing 1993 p 105

⁷¹ from stone, via papyrus to paper

⁷² from writing, via printing to the rotary press.

2.1.3 Information and the media

Information is either secured - tied to - some media or just communicated from person to person. This reflects the ways of communicating information, *supra* 2.1.2. The problems lies in the ways information is connected to the media - if at all.

If information is not written to some media there is difficult to "take it away" from the person possessing it, unless one prefers to use blackmailing or torture. This is the case with traditional craftsman's knowledge. A special recipe for beer or whisky is given orally from one brewer to another, and will never find its ways into a filing cabinet. Technically one might argue that also the human brain is a media for storing information, but it does not seem likeable that this approach will be of much help in this context.

Bryde Andersen⁷³ point out three different ways information might be connected to its media. The first is where the information might easily be moved from one media to another or from one group of medias to another. This is the case with personal expertise, slogans, passwords, general ideas, etc. The second category is information that, according to its character or purpose, has to be connected to a certain *type* of medium - but it might easily be moved to another media within the same type. This is typically the situation with software. The third category is the information, that under normal use is inseparable from its media. This is the case for hardware component, chips, but also other physical objects, such as handicraft.

As mentioned above traditionally legal rules has been adjusted towards a moveable, not the information. There has for some time discussions - in several fields of

⁷³ Bryde Andersen 1991a p 282-283

information law (and computer law) as to whether especially computer programs are to be considered as movables or not.

Bing⁷⁴ observed, already in 1981, that the "similarity to a physical object on the one hand and to intellectual property on the other hand makes the categorization of computer programs as 'movables' (or 'goods') uncertain. And this uncertainty may have substantial implications for the law affecting computer programs".

For some further examples of this discussion see, Franken 1990, Bryde Andersen 1991b, Hirschback 1989 and Stuurman 1991 p 197-200.

This discussion leads to the conclusion that information *per se* is not a moveable, and that the connection between the information and the media carrying the same information, stresses the differences between this media and ordinary movables, and that it cannot be regarded as a moveable - the same way as "ordinary movables".

Another approach would therefore be to ask whether there is any reason to distinguish between information and movables. This answer might differ depending on the fields of law. There are severe differences between VAT-law, contract law, and criminal law, and this differences in the legal rules might lead to differences in the legal reasoning as to whether information is subject matter or not.

It should though be mentioned that even if information due to its nature not capable of being taken away, a medium containing the information⁷⁵ might be taken away, hence

⁷⁴ Bing 1981 p 225

⁷⁵ eg a book, a floppy disk or a cassette tape

fall within the scope of theft in most jurisdictions⁷⁶. This constitutes another problem since there might be a difference depending on whether there is a media being taken away or just somebody illegitimately accessing the information. One might ask if this is a reasonable result⁷⁷.

2.1.4 Information - concluding remarks

Information is loosely taken to be knowledge or new knowledge, it is the connection between this knowledge and the media carrying the same that in a legal context in many cases constitutes problems. It is the information, rather than the media that is interesting. The connection between the information and the media is not necessarily a relevant argument as to whether the criminal offenses relating to movables or goods should apply to information.

In addition to this problem, that has caused difficulties in applying existing criminal offenses (and other legal provision), there are some aspects of information, that has to be scrutinized, in the following. But before going on to that, it might be interesting to give a brief introduction to a model for communication process.

⁷⁶ Cfr Saxby 1990 p 219

⁷⁷ Regarding other fields of law, see Rt 1992 p 1629, *supra*.

2.2 Communication processes

Above, 2.1.2, is discussed some basic trends in the ways of communicating information. In this part communication process, based on Shannon and Weaver⁷⁸, as such will briefly be discussed. The model for communication process is shown in figure 5.

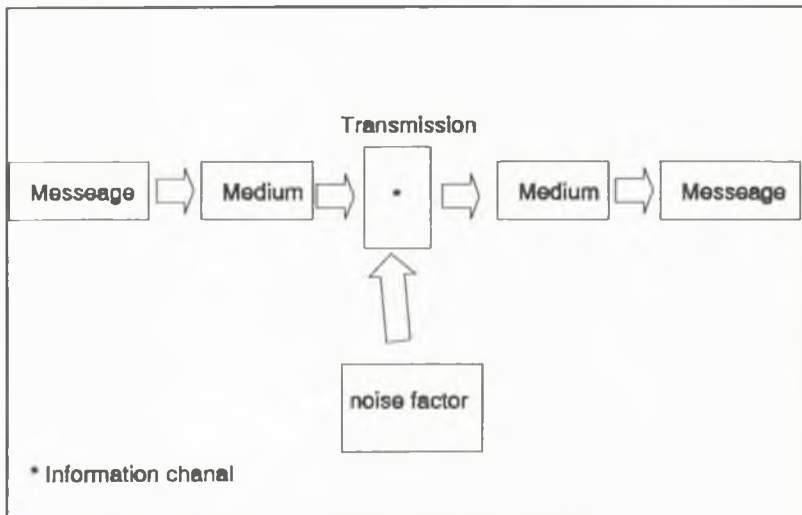


figure 5 A model for communication theory

There are some basic elements in a communication process. First the parties must have access to a medium for communication, next they must have a decided language for communication, and finally they must communicate, this also reflects the points made above.

⁷⁸ Cfr Bryde Andersen 1991a p 102

This model is general, hence supposed to cover any form of communication between two or more parties.

In our context it gives a starting point and a possibility for identifying what parts of a communication process it is desirable to regulate - or make subject for a criminal offence.

2.3 Information and secrecy

A different aspect, from above is the aspect of information and secrecy⁷⁹, hence the desire not to communicate the information. This aspect is that somebody tried to surround their information with a sufficient degree of secrecy, so it will not be available to outsiders.

The reason that this problem is discussed is partly that secrecy in some situations is the only mean of protecting information, and in some situation secrecy is one condition in order to obtain a legal protection. In the *de lege ferenda* discussion this will also be apparent, since it might put an obligation on the "possessor" of the information to keep it secret in order for a legal protection to occur.

This aspect might easily be summarized as a precaution to be taken, if one wants secrecy. It is also to be an argument in the legal discussion, *infra* 5.1.

It should be mentioned that there are levels of security, the security might be total, or partial, depending on whether

⁷⁹ Cfr Bryde Andersen 1991a p 285

the information is exclusive, difficult accessible or generally known⁸⁰.

2.4 Economics of information

There is a need to look at some aspects of the economics of information law, since the traditional economic models are based on movables, are not applicable to information. At the same time it should be kept in mind that *one* of the reasons for some of the traditional criminal offenses lies in some basics of economical theory.

The crime of theft is referred already in the Ten Commandments - you shall not steal. In any society this is a basic rule. If you take deprive someone of his sheep he cannot eat it. If you deprive someone of his cow he cannot get his milk, and if you steals somebody's flour he cannot make his daily bread. The same basic principles goes for more advanced products as well; a car, a boat, an electrical toothbrush or corkscrew. The same kind of reasoning is applied to a trades-man, if you steal his product, he is not able to sell them, because he has not got them.

Traditional commodity has its value due to its present, and depriving someone of that commodity at the same time deprives him of the economic value.

This is not so with information, as shown above, information by nature is not capable of being taken away. Information has to base its economical value on other elements.

⁸⁰ See Coleman 1993 p 175, in relation to breach of confidence.

This might be divided in two parts, the first what gives information its economic value and the other the aspect of return of investments in information.

2.4.1 The value of information

Information might be used in two different ways, one is to sell the information to somebody else, the other is to keep the information confidential and take advantage of it - typically in a production process⁸¹.

In the latter category the value of information lies in some kind of monopoly, that the information is not available to other parties, if it were the information would not give a competitive advantage. To keep this advantage the information must be kept secret⁸². Often this information is subject for trade secret (provided that other criteria are present)⁸³.

If the information is supposed to be sold, there has to be some exclusiveness in order to secure the profits, this might be a factual or a legal⁸⁴ exclusiveness. Since information may be expensive to create and costly to compile, once obtained it is cheap to reproduce there are no or rather very low variable costs the price of reproduction does not noticeably influence the market price.

⁸¹ Bull 1985 p 26 uses the term "Machwert" and "Geltwert"

⁸² if not protected by patent

⁸³ See Coleman 1993 p 176

⁸⁴ such as copyright and neighbouring rights

In some cases it is sufficient to have a lead time-wise (typically with factual information where the time is essential); "the first person who can end the uncertainty about share price trends can earn money. So can suppliers of semi-processed data."⁸⁵

It is not surprising to find that access to this two types of information differs, this should also be reflected in the legal norm regulating the access.

2.4.2 Protection of the investments in information

The problem with return of the investment involved in information is actually a very old problem, that prior to the post-industrialised society seems to have been *properly* protected by the intellectual property rights.

It is easily to demonstrate that some information is the result of a rather burdensome and expensive process, and that there is a desire to secure the return of profits from this process. It is also argued that without the possibility of a return of profits these investment will not be made.

Unlike traditional commodities it is rather easy to reproduce information (if available), how easy is partly based on the connection between the information and the media, *supra* 2.1.3. Copyright developed from the problems with copying books, several hundred years ago, so the problem is not quite new. But the developments in information technology and the new information services has addressed the problem in a new way.

⁸⁵ Dommering 1991 p 31

The problem is that there is a strong demand for a legal protection of the investment in the information, that up till now has not been present, and that copyright and other intellectual property rights alone are not capable of handling that demand properly in most jurisdictions today.

At least this is the case with the continental approach to copyright, with its emphasise on the writer or author - le droit de autor. The protection is different in common law jurisdictions and to some extent will protect the investment better. Even though the sanctions in most intellectual property legislation might seem insufficient for the values vested in the information. There is also a different approach as to whether infringement of copyright should be met with criminal sanctions.⁸⁶

2.5 Aspects of information law - why "ownership"-structure is not applicable

In addition to the points made above there are in many instances types of data where it is a desire to control the data in one way or another. It is emphasised that this must be taken into account in the *de lege ferenda* discussion⁸⁷. This is simply due to some characteristics of the piece of information in question, or a desire to give some communications confidentiality. Another aspect is the problems arising from some fundamental human rights (internationally accepted and based on the different constitutions), the question of access to information, the question of the workers right to organize etc.

⁸⁶ Sieber 1992 p 23

⁸⁷ Sieber 1992 p 17

2.5.1 Controlling data - due to its content

The starting point for this rather broad category is that some information is sensitive in one way or another, therefore a freedom of communicating is not desirable. This calls for a protection of some kinds information, where the access and communication should be limited. The problems regarding business secrets are discussed above.

In an attempt to divide this category, privacy and security of the state might easily be identified.

2.5.2 Privacy

Privacy may easily be viewed from this standing-point, as a way of making criminal certain ways of obtaining and using information. Depending on the jurisdiction privacy is defined in a variety of ways.

There seems to be a distinction between the common law jurisdiction⁸⁸ and the Continental European approach, where the former views this as some kind of a property right, while the latter is more concerned with the use of the "private" information.

The Norwegian approach is a good example where the essential is the use of the information. Chapter 23 of the Norwegian Criminal Code⁸⁹ deals with defamation. The crime is in s 246 and s 247 described as;

⁸⁸ Probably with the exception of England and Wales, that up till now has no efficient general protection for privacy, see Coleman 1993 p 176.

⁸⁹ Translation obtained from the Royal Norwegian Embassy in London

Anyone who unlawfully violates another's feeling or personal honor [sic] in word or deed.. and; Anyone who, in word or deed, behaves in a manner likely to harm the good name or reputation of another, or expose him to hatred, contempt or loss of the confidence required in his position or trade.... . This does not state anything if the accusations are true or, this is solved in s 249, that i subsection 1 states; "Punishment according to sections 246 and 247 shall not apply if the truth of the charge is proved". So far it seems to follow the lines of libel under English law, but subsection 2 goes on to state that "[e]ven if the truth is proved as indicated under No. 1, the charge is punishable if it is made without respectable reasons or is otherwise improper because of its form or the manner in which it is made, or for other reasons".

With the emerge of computerized systems the concept of data protection has emerged, and this is in some way linked to the concept of privacy. But it emphasises different aspects.

2.5.3 Security of the state

It seems obvious that there is a need to protect some information that is connected with the security of the state.

2.5.4 Professional secrecy

As a group of its own professional secrecy might be mentioned. This is to guarantee some canals of information that is free to use. Typically this is present with a doctor-patient situation, a lawyer-client situation and also in a number of other situations. This seems to fall within the broader scope of sphere of integrity as used by Sieber⁹⁰.

⁹⁰ See Sieber 1990 p 125

2.5.5 Freedom: right to information?

Freedom of speech is a basic civil right, in most western countries, and has a constitutional aspect in virtually all countries - with the exception of The United Kingdom⁹¹ - and is also granted in the European Convention on Human Rights, art 10. It might be argued that this right is connected with the right of access to information. To some extent this is covered by Art 10, but than only if the holder discloses it. The same is the situation with the German constitution⁹². The question of whether the European Convention gives the right of access to governmental information has been brought before the European Court of Human Right two times⁹³, and the answer is negative.

Even if this is not protected by the conventions on human rights there still seems to be a need for access to information. Mackaay⁹⁴ divides this question into different categories depending on who possess the information, and who the information concerns, as follows.

- Information Rights Against the State
- Information Rights against Private Citizens
 - Personal information
 - Information about criminals
 - Information about hazardous products and catastrophic risks
 - Information about competitors
 - Information on companies

⁹¹ Barendt 1992 p 13

⁹² Barendt 1992 p 21

⁹³ Leander v Sweden and Gaskin v U.K

⁹⁴ Mackaay 1992

It seems clear that the right of access to information held by the state, regarding the state is the case where the reason for giving access is the strongest⁹⁵, since this does not involve the same economical interest as with commercial information. This might also be illustrated by the fact that both Norway and Sweden in their introductory speech in the membership negotiations with the EC stressed this factor, and that they were interested in continuing their politics, and that they wanted it to govern in the EC as well. As a curiosity it is tempting to mention that the questions from the Commission to applicants are secret, but that under the Swedish principle of free access the answers given by the Swedish government are accessible.

The status differs between different nations today, where Sweden and The United Kingdom probably are the extreme points in western Europe today. Regardless of the current situation this is an argument in the discussion.

Whilst citizens does not have any general obligation to disclose information. Secrets might be kept⁹⁶, this is also demonstrated in *R v Stewart* - there was no underlying obligation to disclose the information. Nevertheless there might often be a public demand for disclosure⁹⁷

⁹⁵ with the limitations concerning the security of the state

⁹⁶ Mackaay 1992 p 171

⁹⁷ See also Coleman 1993 p 179, in relation to breach of confidence

2.6 Models for "information law"

Since information is not able of being taken away some attempts of making models for the information law has been made. I will discuss such a model⁹⁸, simply to emphasise some of the problems arising.

From the communication theory we may divide the processing of information into phases, and each of these phases might be regulated. It is also possible to focus on the information, and regulate some aspects of the information.

The phases, or functional division includes:

- creation
- communication
- storing
- processing

When focusing on the information, we find that the following aspects might be identified, and be subject of regulation;

- content
- form of the information
- the structure
- the media of the representation

The essence of this model is that under the functional division, the information must be created, it must (or might) be communicated, it must be stored, one way or the

⁹⁸ Based on Bing, Madsen, Myrland 1987 p 10 ff, see also Bing 1993 p 13 ff (in English).

other, and it might be processed. Each of these steps might be the basis for legal measurements⁹⁹, alone or together with other parameters.

With the focus on the information, we find that if it has a special content (ie security of the state), a special form (signed document), a special structure (ie a personal register), or connected to a special media (ie paper, computer storage medium) this might be regulated.

In some instances a combination of these aspects are made the basis of criminal (and non-criminal) offenses.

Espionage relates to the *communication* of information of a certain *content* that are being *stored* under certain circumstances, and not indented for communication. The same is the situation with industrial espionage, though the content are of a very different kind.

It should also be mentioned that Dommering¹⁰⁰ divides the subject for "information law" into the following four categories;

- a) the production and processing of information
- b) the storage of information
- c) the conversion, transfer and reproduction of information
- d) the use, consultation and storage of information.

It does not seem as there is any difference in the field, of study even though there are two different models being used. And it should be emphasised that the models are rather similar.

⁹⁹ Regarding "theft of information" the relevant aspect is the communication of the information.

¹⁰⁰ Dommering 1991 p 20

2.7 A temporary summary of this part

It has been demonstrated in this part that information, *per se*, is by nature different from movables, therefore it cannot *per se* follow the same legal rules as movables.

This point has also been noticed by the Norwegian Criminal Code Commission in a rather new proposal¹⁰¹. This Commission was set up in 1980 to make a draft for a new Criminal Code, the present proposal is for the general part of the Code. In the proposed sec 19 moveable is defined the same way as in the present Code. Regarding information the Commission makes it clear that this falls outside this definition, and goes on to state that¹⁰²; one could choose to extent the definition so it also would include data, but this would extend the crimes where the term movables are used in an undesirable way. Computer assisted crimes are so special that the existing criminal offenses should not be extended without further considerations.

Though this statement is with respect to computer crime¹⁰³, there is no reason why it should not be taken to include also non-computerised information crime.

It should also be kept in mind that "there are conflicting rights in respect of one and the same object to a far greater

¹⁰¹ NOU 1992:23

¹⁰² NOU 1992:23 p 67, my own translation

¹⁰³ It is rather unclear at this point since the Norwegian language uses the term "data-kriminalitet", hence data might refer to a computer (data-machine) or data *per se*. This dualistic meaning in the use of the term data in Norwegian makes any statement in this respect rather unclear, if not specified by the author.

extent than in the case of the ownership of material goods."¹⁰⁴

2.8 Intellectual property rights

It should be mentioned at this stage that due to some of the considerations in this part intellectual property rights has been developed. But it should be remembered that the principles of intellectual property rights "also modelled themselves upon the needs of a society whose wealth depended upon the development and manufacture of tangible goods. Proprietary rights were allocated, not to ideas as such, but to their embodiment in the written form or in physical plants with an industrial application."¹⁰⁵

These are basically drafted as a result of balancing interest between the "developer" and the society as such. It was considered necessary to give some reward for the useful arts and science.

This is also reflected in the American Constitution Art 1, Sec 8, cl 8; "To promote the Progress of Science and useful art, by securing for limited Timed to Authors and Inventors the exclusive Rights to their respective Writings and Discoveries".

Especially with patent this is a way of regulation the *use of* information or knowledge.

¹⁰⁴ Dommering 1991 p 21

¹⁰⁵ Saxby 1990 p 219

It should be mentioned that defining intellectual property rights as *property rights*¹⁰⁶, will not help to answer the problems of "theft of information". This was also pointed out by the Canadian Supreme Court in *R v Stewart* that the copyright cannot be stolen, only the copies of the work.¹⁰⁷

2.9 Some special problem with regulation of information law

Based on the model for information law regulation, *supra* 2.6, it is possible to make legal measurement in each of these elements. The problem is that traditionally there has been an emphasis on the media or a rather specialized way of communicating. In this part, more as an illustration to the general considerations to the discussion above, I will try to illustrate some of the problems in this area.

The last problem is easily illustrated with the development of new communication systems. Some decades ago the distinction between telecommunication services and broadcasting made no problem. It followed, in legal term, the way the information was *communicated* to the recipients. With the development of cable television, followed by pay-per-view television, on the one hand and the development of digital telecommunications network, able of carrying exactly the same information, on the other hand this distinction is getting more troublesome.

¹⁰⁶ Copyright, Design and Patents Act (UK) 1988 s 1; Copyright is a property right...

¹⁰⁷ p 15

An illustration on the legal problems arising from this might be found; under Norwegian law it is unclear if the prerecorded 0898-services¹⁰⁸ are covered by the broadcasting act or not - this simply due to the historical definition of broadcasting.¹⁰⁹

The same is easily construed as the problem with *computer crime*. As of today there are not any special problems as to whether a "thing" is a computer, hence covered by the computer crime legislation, or not. But in the future the problem may arise. And in some cases there are differences in the law affecting an action whether the action involves a computer or not.

This brings the attention back to the general problems of information law legislation. Traditionally we have been concerned with the media, or the way of communicating the information - not the information *per se*. This has opened for some loop-holes in the legislation - which in its turn has been covered. There has been a kind of competition between the technical development and the legal development, where the latter always is behind.

From this it seems as if there are two different ways of regulating information crime, either we discover new behaviours and make a criminal provision for them, based on the technical ways of communicating that are known today (which is the traditional approach) *or* we try to define the offence in such a way that it becomes not related to the

¹⁰⁸ 900-numbers in US, 020-number in Norway. The system is simply that the telephone subscribers pays more than the cost of the phonecall for the call, and that a certain amount of money, collected by the telephone-company is transferred to the information provider.

¹⁰⁹ Galtung 1992 p 8 ff, with further references

present information technology. The latter is a more difficult approach to the problem, firstly because it is difficult to define in non-technical terms what the crime is, secondly this approach would probably make the definitions of the criminal offenses rather broad. But with a part of common sense in the interpretation this problem might not be that serious. (In the common Law countries this might give a problem, though.) At the same time it is easy to loose the communicative aspect of the criminal offenses - that the members of the society shall know what criminal offenses that exists. There does not seem to be any easy answer to this problem.

3 Theft of information - a *de lege lata* overview

Applying criminal offenses to a fact is basically the same in all jurisdictions¹¹⁰. First the piece of legislation has to undergo a interpretation, to achieve the legal rule. This is followed by applying the norm to given fact.

Since theft is defined differently in the different jurisdictions the legal norm will also be different. In a criminal context most jurisdiction the rule of law is prevailing - you cannot punish unless there is a statute stating that something is a criminal offence.

¹¹⁰ With the exception of jurisdiction who has common law based criminal offenses, such as Scotland.

3.1 The general starting point

The general starting point will be the legislation. Most jurisdictions has defined theft as taking away from someone their property or belongings. In the context of information this rises two problems, the first is whether information might be taken away, the second whether information is property or belongings as defined in the statute.

Some illustrations found in legislation could be used as examples of this; Every one commits theft who ... takes, or ... converts to his use .. anything wether animate or inanimate, with intent ...¹¹¹; Anyone who carries away ... an object ... for the purpose of obtaining by appropriation of such object an unlawful gain ..., shall be punished for theft¹¹²; A person is guilty of theft if he dishonestly appropriates belonging to another with the intention of permanently depriving other of it, "property" includes money and all other property, real or personal, including things in action and other intangible property¹¹³;

Depending on the legislation it seams as if in many jurisdictions information, *per se*, will fit uneasily into the crime of theft, there is - at least in civil law jurisdictions - a limited possibility of construing an analogy by interpretations. It is argued that the courts should be careful with this since it in a democratic society is within the power of the Parliament to make new offenses¹¹⁴.

¹¹¹ The Canadian Criminal Code S 283 (1)

¹¹² The Norwegian Criminal Code (obtained in English translation from the Royal Norwegian Embassy in London), object includes electricity, s 6, but object is not defined in the Criminal Code.

¹¹³ The English Theft Act 1968 S 1 and 4

¹¹⁴ Franken 1990 p 137

3.2 Different jurisdictions - overview

This overview is two-fold, in some jurisdictions there is actual case-law dealing with the problem of information as subject matter of theft, and in other one has to base on the actual criminal codes (or other appropriate legislation) and legal theory.

For this part I will mainly base the discussion on legal literature and case-law, that addresses the problem of theft of information¹¹⁵. It seems rather clear that many aspects of information falls outside the scope of the national legislation - such as broadcasting, where it is more likely that other kinds of statutory rights are involved.

In most continental jurisdictions¹¹⁶ illegitimately accessing information is not within the scope of the crime of theft. In some jurisdictions, such as France and the Netherlands it seems possible at least in some cases that the *actus reus* of theft is broad enough to cover information. In some common-law jurisdictions there seem to be a strong tendency towards a "property theory"¹¹⁷

It is argued that the German Inkasso-case¹¹⁸ stipulates that the crime of theft is not the proper way of approaching this problems, but that it should be approached by trade-

¹¹⁵ It the case law the problem discussed has in all cases been the *actus reus*. There does not seem to be any cases acquitting the accused due to lacking *mens rea*.

¹¹⁶ Sieber 1992 p 18-19

¹¹⁷ Sieber 1992 p 19

¹¹⁸ 94 BGHZ 276 (1985)

secrets and intellectual Property Rights¹¹⁹. The argument in our context from this is that in Germany information in the form of computer programs is not subject matter for theft.

The Inkasso-case, did not address the problems of theft, it was concerned with the copyrightability of the computer program in question. Copies of a computer program was copied, and the person who has developed the program was in a situation where he wanted damages for the "unauthorized" appropriation. The Supreme Court (Bundesgerichtshof) found that the program was not protected by copyright.

Regarding software there is some case-law:

Probably the first case concerned with information as subject matter for theft is the American case of *Hancock v Texas*. Hancock photocopied 49 computer programs belonging to his employer - Texas Instruments - and tried to sell these to one of its clients. His counsel argued that no original documents had been stolen, no property had been taken, but the court found that the programs were in fact property. It should be mentioned though that under Texas law values of more than \$ 50 must be taken away to meet the *actus reus* for theft. Hancock admitted to have taken away \$ 35 worth of paper. This was more a case of whether the value of the media or the value of the media containing the information was the relevant aspect. Hancock made a petition for habeas corpus, which was rejected by the court of appeal 5th Circuit in *Hancock v Decker*.

It looking at the consequences of this case it must be remembered that it was decided before the American Copyright Act made specific reference to software, and at that time the applicability of copyright to software

¹¹⁹ Sieber 1990 p 124

was uncertain. The same uncertainty was probably present in the next case to be mentioned.

In October 1983 the Dutch Courts of Appeal found that a man who copied software from his employer to floppies owned by himself was guilty of theft. (A fact similar to the Inkasso-case, but unlike Hancock in that the defendant had not removed any property (except the software) belonging to his employer.) He later resigned his job and set up a competing company. The Dutch Courts of Appel based its decision on the similarity with electricity, which by a Supreme Court Case from 1921 was found to be subject matter for theft. Franken¹²⁰ is arguing that this case or *wrong*, but from his article it is not clear whether his argumentation is strictly *de lege lata* or not.

In non-software case-law the problem has related to confidential information of one kind or the other;

In *Oxford v Moss*, Moss - an undergraduate student had obtained access to an examination paper read it and was caught when returning it. To the question as to whether the obtaining of the information falls within the definition of property in Theft Act (1968) Smith J stated that as "we have to consider whether there is property in the information which is capable of being the subject of a charge of theft. In my judgement, it is clear that the answer to that question must be no." He was followed by the two other judges. This case was followed in *R v Absolom*, where a geologist was acquitted of theft after obtaining and trying to sell oil exploitation plans from Esso.

¹²⁰ Franken 1990 p 136

In *R v Stewart* the Canadian Supreme Court was confronted with the fact that a trade union tried to obtain a list of the employees of a hotel in Ontario. The hotel would not give them the list, and they contacted Mr Stewart, who acted as a private detective, and tried to bribe one from the security department into writing, from the rolls, a list of the employees. The Supreme Court, unlike the lower courts, found that this was not within the definition of theft.

This rather brief illustration of the applicability of the crime of theft illustrates that there are severe differences between the definitions of theft in different jurisdictions. At the same time it could be mentioned that the cases evolving software, today probably would be raised as cases of infringement of copyright instead.

4 Some general considerations as to information crime

As shown in the general discussion of information law, and the interest inherent therein makes new criminal (as well as non-criminal) measures necessary, but due to the differences between information and traditional commodities the existing criminal offenses should not be applied directly to information uncritically.

This has to some extent been met by legal measurements. Sieber¹²¹ identifies 4 waves of legislation, of which the first two up till now has been dominating.

¹²¹ Sieber 1990 p 120 ff

The first wave was the law reform in the western countries in the 70-ies and 80-ies concerning privacy and data protection. The second main wave was the reforms dealing with computer-related economic crimes in the early to mid 80-ies. In the course of the 80-ies a third series of law amendments improved the protection of intellectual property in the field of computer technology. The fourth - and up till now the last wave are the reform legislation bringing along a series of *new procedural law provisions*, to respond to the new developments.

The computer crime legislation is partly traditional offenses that would not be applicable in a computer context, in addition to this two new offenses is included in most jurisdictions - the criminal offence of hacking, and altering of data.

With the exception of hacking and unauthorized alteration of data computer crime legislation did not include totally different or new offenses, the concern was more towards the applicability of traditional offenses. For instance the crime of fraud would in most jurisdictions be defined as deception of someone. A computer system would fit uneasily into this definition. At the same time though with a problem according to the wording of the legislation acts like formatting a media (a floppy) was found to fall within the act of damages to property. In most jurisdictions it was found that the similarities to the traditional crime was so high that it did not make severe problems to include it.¹²²

¹²² Under English law this might be illustrated with *Cox v Riley*. For an overview of the international situation see Sieber 1992 p 28 et seq

It might be stated that the computer crime legislation of the 80-ies to a large extent brought the criminal offenses up to date with the development of information technology, but it was to a less degree interested in the problems of protecting the increased value of information. It seems as with the starting point - *computers* - this was not a strange result.

In this course of legal developments it is argued that the field of information crime is still lacking a "general theory on the criminal protection of information"¹²³.

5 Theft of information - a *de lege ferenda* discussion

A starting point in a discussion as to make criminal "theft of information" could be to start with an empirical analyses of the damaging results such behaviour has in today's society. Unfortunately we do not have such empirical data. There are large "dark numbers" in this field¹²⁴. But as stated by Franken¹²⁵ "we cannot avoid the conclusions that there has been an increase in the number and variety of these abuses." Due to this lack of empirical data this will not give a sufficient starting point for the discussion. The stress should be more on the possible harm that might be done, and what we actually know. On the other hand the need for and reliance on computer systems might be a useful starting point¹²⁶.

¹²³ Sieber 1990 p 123

¹²⁴ See Sieber 1992 p 7

¹²⁵ Franken 1990 p 132

¹²⁶ Cfr Sieber 1992 p 7-8

It is argued that a starting point should be a balancing of interest between free flow of information and the desire to protect data.

"But there's an inherent conflict. On the one hand we acknowledge the fundamental principle of the free flow of information, on the other hand society demands protection of data. The European Convention on Human Rights guarantees the freedom to receive and to gather information"¹²⁷ "There are three types of interest at which are at stake: availability, integrity and exclusivity."¹²⁸ "In the field of *substantive criminal law*, this new approach of "criminal information law" differentiates two fundamental questions: It first investigates how far the various national systems protect the holder of information (concentrating on the protecting information per se). It then investigates the privacy protection of "data subjects" concerned by the content of information."¹²⁹

5.1 Legal and other measures

It should also be kept in mind that legal measurements are only one of several that could be used in order to prevent the illegitimately accessing of information. Franken divides the preventive measures for risk avoidance into four basic categories¹³⁰:

- physical measures (as a safe place in the building)
- organizational measures (such as separation of functions between designers, operators and controllers)

¹²⁷ Franken 1990 p 133

¹²⁸ Franken 1990 p 137

¹²⁹ Sieber 1990 p 124

¹³⁰ Franken 1990 p 133

- logical measures (such as protection built into the program itself -encryption modules, for example)
- legal measures.

This point is also stressed by Sieber¹³¹ who states that it "is clear that a comprehensive strategy for the *prevention and control of computer crime* cannot only be based on legal measures."

It should be stressed that legal measures also includes contractual measures between parties, such as employer and employee, and not only new legislation.

Though these categories specifically deals with *computer security*, the same categories might easily be applied to other forms for information.

Take the case of *Oxford v Moss*, the University had not taken the simple precautions of protecting their information, or it did not work. This falls easily into the first category - physical measures. In the case of *R v Stewart* the organizational measures worked perfectly and Stewart did not achieve his illegitimately access to the files.

In the youth of the computer era the systems were made with a lack of security, and this lack of security is to be blamed the computer industry and the organizations purchasing computer systems. It seems tendentious that this lack of security should be balanced with legal measures, even though this has been much of the argumentation prior to the international initiatives in computer crime.

This might be illustrated with the definition of hacking found in some jurisdiction (Canada, UK, Denmark, Israel and some states in the USA), where the *actus reus* is unauthorized access, whilst in other it is a part of

¹³¹ Sieber 1990 p 119

the *actus reus* that some security measurements must be passed (Germany and Norway)¹³².

My initial argumentation is simply that if unwanted behaviour might be prevented by physical measures there is not a strong need to make new legal provisions dealing with the same problems.

I am not arguing that legal measures should not be made, but that they should not be used as arguments as to relax on the other, and in that respect it seems as only legal measures would relax on the other aspects. The aspect of information and secrecy supports this argument, in that if someone wants to keep something secret, he must make some precautions to obtain that secrecy.

5.2 To extend the present criminal offenses or create new offenses

The problem is obviously not addresses in the case-law approach, because it is solely a question for the parliament. The question is simply whether the existing criminal offenses - in casu theft - should be extended to cover information or not.

I have, above, argued that the existing criminal offenses should not uncritically be applied to new facts, simply since the offenses are different. If there are no reason to treat information and goods differently the same criminal offenses could easily be applied. This is in some jurisdictions, above, the case with damage to property. But

¹³² Schjølberg 1991 p 154

regarding the crime of theft there are serious differences between information and goods, hence they should be treated differently¹³³. In some cases, narrowly defined, the act of acquiring access to information should probably be a criminal offense, but this legislation must be drawn carefully.

5.3 A starting point for the discussion whether to make new criminal offenses or not

The starting point should be whether the behaviour is undesirable or not. If the answer is yes, the next question is whether it should be met by criminal provisions or not.

It should in this discussion be kept in mind that punishment is the societies strongest expression of displeasure due to a certain conduct. In many cases there are non-criminal sanctions at hand, or there can be construed new - to make an appropriate reaction to the conduct.

The case of *Oxford v Moss* may serve as an illustration. In this case the student could be expelled from the university due to his conduct. In such a case, one might easily argue that being expelled in itself is a reaction strong enough, and that there is no need for an additional criminal offence.

¹³³ See also Sieber 1992 p 19

5.4 The need for international legal harmonization

There has to be some sort of international harmonization in information crime, the major reason for this is the international dimension of information technology¹³⁴, and that the problems are international, not limited to one jurisdiction¹³⁵.

From the early days in the development of information crime there has been a large evolvement from organizations as OECD, COE, EEC, WIPO, and UN. For an overview of the initiatives of international organizations, see Sieber 1992 p 73 et seq.

This international framework is necessary, especially in the computer related parts of information crime, since it is no problem to move ones data to another jurisdiction, and at the same time assaults to ones data might easily occur from outside the jurisdiction they are located.

In a criminal context this might also raise problems with jurisdictions. This specially in those jurisdictions based on the principle of dual offence - that a crime might be punished if scene of the crime was within another jurisdiction, but the same act is criminal also in the other jurisdiction.

¹³⁴ Cfr Sieber 1990 p 127-128

¹³⁵ Saxby 1990 p 217

5.5 The balancing of interests. Whether to regulate or not

After formulating the problem as such "In considering the *interests of the "proprietor" or holder of information*, has to consider two main aspects: First, it must decide whether and in which cases the exclusive use and the secrecy of information should be protected. Second, the question must be solved as to how far criminal law should guarantee the integrity, availability and the correctness of information"¹³⁶ Sieber identifies the following elements that (in our context) should be protected:

- copyright protection for computer programs
- a "formal sphere of secrecy" by criminalizing illegal access to specific computer data
- a criminal privacy protection, but "it is essential to avoid an over-criminalization and imprecise criminal statutes which can be found today in many countries"¹³⁷

The starting point in my discussion is basically the problems and interest set out above. The results has to be based on a balancing of interest between the parties interested in the same information. This is to a large extent a question of moral standards, and might easily differ between different countries.

As an example of this, in *R v Stewart*, the interest of the employer would in other countries be to disclose the information or parts of it. This would probably be the case in the Scandinavian countries and some continental countries. The same is illustrated in the amended proposal

¹³⁶ Sieber 1990 p 124

¹³⁷ Sieber 1990 p 126

for data protection, where the classification of union membership as sensitive data in some countries is used as a good example of different social systems.

It should also be kept in mind that the relevant view is not the information *per se*, but the use of it. The obtained information itself does not make any harm, it is rather the use of it in one context or the other.

One starting point could be the way the information is obtained. If the information is obtained by *improper* means there is a stronger need for protection than if obtained in other ways. Eavesdropping, hacking, bribery and similar methods of gaining access to the information should be met with legal sanctions. If the information willingly is passed on to the acquirer for instance by an employee - the receiver of the information has not done any improper acts (or at least not that improper). But if the information is of a kind that needs protection, security of the state, privacy interests, or would damage a companies possibility of gaining return of the investments there might even though be a need to deny the use of it.

This must on its side be balanced with the legitimate reasons for accessing and disclosing the same information.

Regarding commercial information, about the production process, the illegitimate use would be competitors using it to improve their own production process. Other kinds of information held by companies might be used in an attempt to destroy the reputation of the company. In some cases this might be legitimate. If someone disclosed information that Bodyshop actually tested their products on animals there would be a strong public demand to disclose that information, simply since their marketing is based on the fact that they are the only company that never tested

anything on animals. But in many cases this disclosure would not have the same legitimate reasons.

From an economical point of view there should be a possibility of return on the invested capital, this no matter whether the information is kept (or tried to keep) secret or it is released for sale. The cases of theft of computer software illustrates this point. It was not tried to keep the software secret, in any way, it was simply the fact that the information if used freely would reduce the possibility of return. The same is often the case with databases offered to the public.

5.6 Whether to make a criminal offence or not

In the question whether to make new criminal offenses or not it should be kept in mind that other remedied will often be sufficient, and that other remedies often is needed in addition to the criminal charges¹³⁸.

If there is a legitimate reason for keeping the information confidential, this cannot alone be solved with criminal sanctions. There must be a possibility of getting an injunction that the information cannot be used, and if already used there must be a possibility of confiscating the improper income from the use of the information¹³⁹. At the same time these actions might be sufficient.

¹³⁸ See Sieber 1992 p 10; At least in theory, criminal sanctions should only be used as "ultima ratio".

¹³⁹ This is the present problem with the doctrine of breach of confidence in England (Coleman 1993 p 192)

My opinion is that only the most serious behaviour should be met with criminal sanctions¹⁴⁰. This would include the information that is most vital, is the relevant respect. There should also be some spheres that are secured from interception, already this includes in most jurisdictions professional secrecy, it should include free communication canals and storage media (if kept somewhat protected). However some security measurements should be passed before a criminal sanction might be justified. This will have to be drafted carefully.

If, on the other hand, it in an investigation by the police is necessary to obtain evidence by waving the rights of the individual sketched out here, this should be based on a court warrant, not the discretion of the police. This is nothing but another aspect of the principle of law.

There is a possibility that new offenses created will concur with existing offenses, but this will have to be solved by the theory of concurrence of offenses in the jurisdiction involved. I do not find this to be a serious problem.

¹⁴⁰ In relation to data protection, COE R (89) 9 p 78



Software and product liability

In 1985, a Department of Trade and Industry consultative document concerned with the application of the then proposed product liability directive to information based products commented:

"Special problems arise with those industries dealing with those products concerned with information such as books ... and computer software. ..."

Can software programs be considered products ? , when can they be considered to be defective and how do the provisions of the Consumer Protection Act 1987 and the EC Directive affect them ?

1 Introduction

Software does not fit easily into the legal system, and it never has. One of the problems arises with norms that requires subject matter to be "moveable" or "goods". Software needs some fixation to be communicates from one person to another, and it is this fixation that is confusing. Does this connection make software a moveable or not? There does not seem to be any easy answer to this question.

Already in 1981 Bing¹⁴¹ formulated the problem as such:

The similarity to a physical object on the one hand and to intellectual property on the other hand may make the categorization of computer programs as "movables" (or "goods") uncertain. And this uncertainty may have substantial implications for the law affecting computer programs.

This uncertainty still troubles the legal system, in more fields than the one discussed in this essay¹⁴² - such as in the applicability of sale of goods acts and theft of software. And any easy solution to this problem has not been given.

The question to be discussed in this essay is whether software is subject matter for product liability or not. Subject matter for product liability is "movables", is software such?

One starting point might be to look at these similarities and differences and draw a conclusion from this, as to whether software is subject matter or not. We find some examples

¹⁴¹ Bing 1981 p 225

¹⁴² see also my essay on Computer Crime

of this in the legal literature. But this approach is not sufficient to give any reliable answer to the question, and it also misses the core of the problem. The problem is actually a problem of description, and this ought to be the relevant starting point.

2 The relation between the Consumer Protection Act and the Product Liability Directive

The Consumer Protection Act 1987 is enacted to conform with the obligation arising from the Product Liability Directive 1985. The Directive is made as a part of the work to get the Internal Market into a reality. Its purpose is therefore to harmonize the product liability within the limits of the Directive.

The main implication of this is that it does not deny the Member States to regulate outside the scope of the directive. Another implication is that the Directive gives the European Court of Justice jurisdictions in the interpretation of the Directive¹⁴³.

The first question in this part is whether the definition of a "product" is wider in the Act than in the Directive, if it is not the interpretation might be based on the directive alone.

¹⁴³ The Treaty of Rome art 177

The directive governs *products*¹⁴⁴, which are defined as¹⁴⁵ "all movables, with the exception of primary agricultural products and game, even though incorporated into another moveable or into a immoveable ... Product includes electricity."

The Consumer Protection Act defines *product* as¹⁴⁶ "any goods or electricity and ... includes a product which is comprised in another product, whether by virtue of being a component part or raw material or otherwise".

Though differently worded it seems as the Consumer Protection Act in our context does not have a broader definition of the subject matter than the directive.

Therefore I will only discuss the Directive, and leave the Consumer Protection Act.

From a UK point of view it might be argued that this is not the correct approach to the problem, and that the UK courts has some discretion. This is a part of the general problem that national law of the member states does not fully accept the European dimension¹⁴⁷. These problem falls outside the scope of this essay, and I presume that UK will respond to their obligations under the Treaty of Rome (even though it does not necessarily do so).

¹⁴⁴ Article 1

¹⁴⁵ Art 2

¹⁴⁶ Sec 1, (2) a

¹⁴⁷ See Steiner 1992 p 42 ff

3 Approaching the problem

Since the interpretation falls within the Jurisdiction of the European Court of Justice, there is a necessity to give a brief overview of the jurisprudence of the Court. But before going on to that problem, I will briefly stipulate what is meant by the problems of description¹⁴⁸, in order to evaluate whether method is permitted under the jurisprudence of the European Court of Justice.

There is also a problem regarding the term 'software', to indicate what is meant by this term.

3.1 The problem of description in computer tort law

The problem of description is twofold, there is both a factual side and a legal side that needs a description¹⁴⁹. Such an approach is a necessity where there is a lack of general understanding and knowledge as to the matter.

The factual description is to describe what software is. This is to consider the aspects of software in relation to the norm given, what are the similarities and the differences, and it is also a necessity in order to give a factual background one might agree upon. In this respect it is argued by Bryde Andersen¹⁵⁰ that;

¹⁴⁸ This method originates from Bryde Andersen 1988, and is originally developed for Danish (and generally) Nordic law.

¹⁴⁹ Bryde Andersen 1991b p 124

¹⁵⁰ Bryde Andersen 1991b p 122

In ordinary "lawyers law" the necessary legal and factual knowledge is typically sufficient known by counsel. "Understanding" the case seldomly presents substantial problems. If it does, the remedies are usually at hand. In a case concerning liability for poisoning, counsel's own knowledge on the human organs etc. will suffice as a basis for additional knowledge to be obtained by expert testimonies etc.

In computer cases this is different. An equally sound basis of knowledge on how computers work etc. is rarely at hand for the average lawyer. Notoriously lawyers - like computer users - have great difficulty in grasping what a computer is and how it works. This difficulty seems to be more profound than in other areas of law with complex matters.

The legal description is necessary in order to verify the legal norms in a new context. The problem is merely that law is an old discipline, and for some rules there is a necessity to find that actual means of regulation in order to establish whether the rule will be appropriate in a software context or not.

3.2 The jurisprudence of the European Court of Justice

As I have stated above, the interpretation of the Directive, hence also the British obligations arising from this, is within the jurisdiction of the European Court of Justice in the last instance¹⁵¹.

Therefore it is the jurisprudence of the European court, as laid down by the Court in previous decisions, that is relevant in our context. The Court uses a teleological interpretation, rather than the literal interpretation found

¹⁵¹ Treaty of Rome art 177

in common-law jurisdictions. This point has also been noted by Lord Diplock who, in *R v Henn*, stated that¹⁵²:

The European Court, in contrast to English courts, applies teleological rather than historical methods to the interpretation of the Treaties and other Community legislation. It seeks to give effect to what it conceives to be the spirit rather than the letter of the Treaties; sometime, indeed, to an English judge, it may seem to the exclusion of the letter. It views the Communities as living and expanding organisms and the interpretation of the provisions of the Treaties as changing to match their growth.

The main aspect of a teleological interpretation is to aim at finding the spirit of the legislation, the Court tries to find what it regards to be the best way of applying any legislation¹⁵³. The actual words of the same legislation is of less interest in this context. But obviously, the wording of the Directive is the natural starting point for the interpretation.

In some cases the wording makes difficulties, due to the 9 different authentic versions of each community legislation. In this case, however, it seems as the term *moveable* does not make problems in this sense.

It seems as it is in accordance with the teleological principle and with the interpretation used by the Court to evaluate the consequences of applying a directive to software, hence the problems of description is permitted.

¹⁵² Quoted from Steiner 1992 p 18

¹⁵³ Arnesen 1992 p 27 ff

4 The factual side of the description - what is software

It is not possible, within the limits of this dissertation to scrutinize the factual side of the problem of description in detail. I will have to refer to Bryde Andersen 1991b¹⁵⁴.

However it is stressed that the starting point for the factual description have to be the communication theory and other underlying aspects.

4.1 Communication theory

In this part communication process, based on Shannon and Weaver¹⁵⁵, as such will briefly be discussed. The model for communication process is shown in figure 6.

There are some basic elements in a communication process. First the parties must have access to a medium for communication, next they must have a decided language for communication, and finally they must communicate, this also reflects the points made above.

This model is general, hence supposed to cover any form of communication between two or more parties.

In our context the main consequences of the communication theory are; firstly that the output from the software has to

¹⁵⁴ See also in Danish Bryde Andersen 1988 and Bryde Andersen 1991a

¹⁵⁵ Cf. Bryde Andersen 1991a p 102

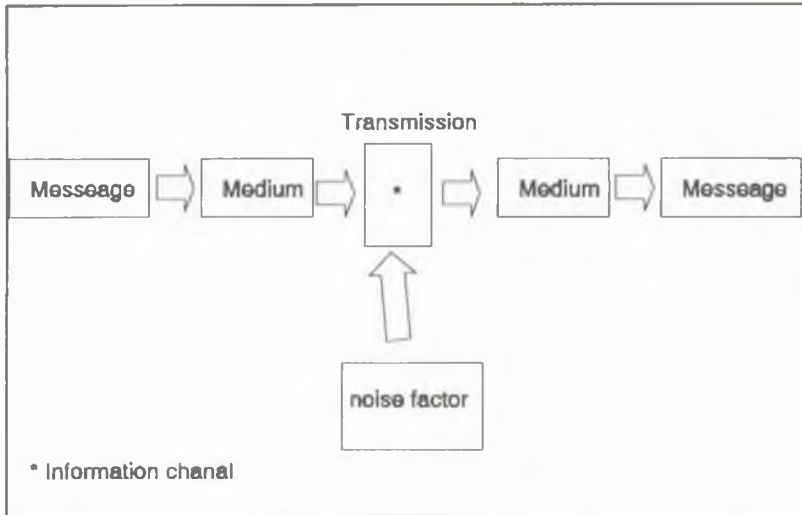


figure 6 A model for communication theory

be acted upon in one way or the other, this might be done in different ways; secondly that the way the software is communicated to the other party¹⁵⁶ does not change the substance of software.

4.2 Programming

It is claimed that it is not possible to make error-free software. This is due to the problems when programming. Some of the articles on this subject emphasises this problem, and argues that this seems to be a reason why product liability does not "fit" for software. Due to this it should be made some comments about this.

¹⁵⁶ see the opinion of Reed 1993, *infra*

Programming falls broadly in three phases. First defining what the program is to do and structuring it, secondly the programming, thirdly the testing of the program.

In the early days of the computer industry programming was rather unstructured, and more of an art than an industrial approach to the problem. These days are gone (though not completely).

Today the struggle is towards a more systemized programming, where the planning phase is divided and approach in a more structural way. In this approach the different tasks are separated, and the program-structure is based on this¹⁵⁷, and at the same time this approach shall make programs have less errors. At this step, at least in theory, it should be possible to make the structure next to error-free.

Before the actual programming it is possible to use a pseudo-code to get the program as optimal as possible, if this is used by groups of programmers the possibility of identifying error are larger.

The actual programming will than be based on the structure (or a pseudo-code).

After the programming phase the program has to undergo some testing to ensure that the program performs the way it should, and to test if there are errors that makes to program not perform the way it should. There are several ways of testing programs, but the basic element is to test if it behaves according to the defined requirements under all circumstances.

¹⁵⁷ See Bryde Andersen 1991a p 119 ff

The problem in the testing phase is that there are a number of parameters that might be used as input to the program, and that at some stage due to some unfortunate combination of parameters the program might give an output that is not in accordance with the requirements. The higher the complexity of the program (or rather the calculations in the program) the higher is the risk of such "unwanted outputs", and also the possibility of errors.

In order to test a complexed program fully there is a necessity of using a test-program, that gives the input to the program, and evaluates the output, to verify that the program behaves correctly. This will have to use the same algorithms and the same calculations as the program itself.

4.3 The software and the media

As shown by the communication theory there has to be some medium for communication of the software for one party to another. This might be that the software is embedded in a physical substance, in a floppy, or transmitted through the telecommunications network.

This connection between the software and the media makes problems when the media is the subject of regulation, or rather seems to be. This calls for a discussion on the relation between software and the media carrying the software.

4.3.1 General considerations

At a general level Bryde Andersen¹⁵⁸ points out three different ways information might be connected to its media. The first is where the information might easily be moved from one media to another or from one group of medias to another. This is the case with personal expertise, slogans, passwords, general ideas, etc. The second category is information that, according to its character or purpose, has to be connected to a certain *type* of medium - but it might easily be moved to another media within the same type. This is typically the situation with software. The third category is the information, that under normal use is inseparable from its media. This is the case with information embedded in a physical object, in our context this might be where some software is incorporated into a physical device. In most modern devices, such as cars, washing-machines and food-processor, there is some software controlling the operation of the object.

As mentioned above traditionally legal rules have been adjusted towards a moveable, not the information. There has for some time been discussions - in several fields of information law (and computer law) as to whether especially computer programs are to be considered as movables or not.

For some further examples of this discussion see, Franken 1990, Bryde Andersen 1991b, Hirschback 1989 and Stuurman 1991 p 197-200.

This discussion leads to the conclusion that information *per se* is not a moveable, and that the connection between the information and the media carrying the same information, stresses the differences between this media and ordinary

¹⁵⁸ Bryde Andersen 1991a p 282-283

movables, and that it cannot be regarded as a moveable - the same way as "ordinary movables".

Another approach would therefore be to ask whether there is any reason to distinguish between information and movables. This answer might differ depending on the fields of law. There are severe differences between VAT-law, contract law, and criminal law, and this differences in the legal rules might lead to differences in the legal reasoning as to whether information is subject matter or not.

4.3.2 The problem of software and media in our context

As stated above software is often incorporated into a physical product of some kind. In most modern day equipment there is some kind of software controlling the product.

It is argued strongly that this products fall within the scope of the Product Liability Directive, irrespective of the software included, since they to the user appear as a product. Bryde Andersen 1991b p 143 argues that:

Faulty software may cause personal damage in cases where the software functions inside a machine or a vehicle. In that case it seems beyond doubt that the machine or vehicle as such will be considered a product, although it functions by means of computer technology. The Machine or the vehicle *appear* as a product, not the chips and software inside.

But there is a problem inherent in this argumentation, when Bryde Andersen¹⁵⁹ on software states that "

¹⁵⁹ Bryde Andersen 1991b p 145

computers are not "dangerous" in the traditional sense, e.g. by causing explosions, poisoning etc. Only when someone takes action upon computer data, such damages will occur." - it seems as if he only is concerned with two of the three categories.

The middle category is where a computer containing software is connected to a machine of some kind, ie a medical scanner of some kind. There is a multi-purpose machine operating a machine. This does not seem to fit into either of the two categories Bryde Andersen is discussing. It seems to be strange that there shall be a different ruling depending on whether the software necessary to operate a machine is embedded in a chip in the machine or on the hard-disk of a multi-purpose machine connected to the same machine with a cable¹⁶⁰. This might lead to some problems, which will have to be discussed later.

4.4 The connection between software and a database - an attempt to illustrate that there is more than one element in some software

As a starting point it could be mentioned that traditionally there has been a diversion between - on the one hand - software - and on the other - hardware. However, "databases" are also an element of the soft side of the information technology. The reason for interpreting the term "software" narrowly is mainly historical. At an early stage when the concepts of "hardware" and "software" were

¹⁶⁰ Kirk 1988 does not seem to make any distinction at this point

coined, databases played a rather insignificant role as compared with computer programs."¹⁶¹

This problem comes also apparent in complexed systems, containing as well "software" and a compilation of facts. This is easily demonstrated with expert systems, which contains (among other elements) a program and a knowledge database.

Some of the examples discussed in the legal theory indicates that this distinction is not taken to seriously, but the problem will become apparent when the complexed system also includes a factual database or an access to another factual database. This problem is used as an illustration by Brannigan and Dayhoff¹⁶², who actually treats this as a software problem;

This process can be illustrated by the following example. In many hospitals the results of laboratory test performed on patient samples, such as blood or urine, are printed on reports by a computer. Certain test results may indicate an immediate danger to the patient. A computer program could be developed whose purpose would be, first, to determine when a test result for a particular patient, taking into account such factors as age, sex, other laboratory test results, and past history, falls within a "dangerous" range, and second, to notify the appropriate parties, whether physicians, nurses, or technicians, of the patient's "in danger" status and of specific aspects of his or her abnormality.

It is clear that such a system will contain of a computer program, a rule-base, and a factual base, and that it will also be connected to the hospitals general records of the patients. Here the fault might be within the program, the

¹⁶¹ Seipel 1992 p 125

¹⁶² Brannigan and Dayhoff 1981

rule-base, the factual base, or in the communication protocols on either side.

Traditionally it has been rather easy to separate a piece of software from a piece of "database", but this might become more and more difficult in the years to come.¹⁶³

I will adopt a more relaxed attitude in this essay, and will deal with the typical software, but will include the norm-base in (typically) expert systems, since they are integrated with the program in the every-day use. The factual base, fall outside the term software as I will use it in this essay. Due to this "definition" problems in communication protocols fall inside. It should be mentioned that the legal ruling will be the same in all cases, due to the differences in the "software".

5 Liability - general considerations

It could be relevant, at this stage, to make some general consideration as to the liability system as such, and also to look at the reasons for enacting the directive on product liability.

This will be a part of the legal side of the description problem, to evaluate the legal systems, and give a starting point in the discussion as to whether product liability in its basic form is fit to cover software.

¹⁶³ The applicability of the Directive to databases is discussed in Triaille 1991

5.1 Where does Product liability fit into the general liability scheme

The problem addressed in this part is generally how product liability fits into the general system of liability. This will be a brief overview of the liability system.

The starting point in discussions of liability, which often is overseen or forgotten; a loss is to remain where it occurs¹⁶⁴. From this starting point we have a system of liability rules to transfer the loss to another party. This is more visible with delictual liability than with contractual liability, in the latter category there is some contact between the parties prior to the loss (the agreement), and during the negotiation process it is possible to place the risk beforehand.

Already before the enactment of the Product Liability Directive there has been some case-law in some of the member states concerning the same issues as product liability, but rather based on negligence than the product itself to use the terminology of Bryde Andersen¹⁶⁵ this had been based on the liability for the computer strategy rather than on the liability for computer function, hence covered by negligence (or *culpa*).

Due to the information aspect it should also be mentioned that in some member states there is a liability scheme for information¹⁶⁶. Eg in England under a duty of care - doctrine, in Denmark under a very different scheme. The

¹⁶⁴ Cfr Bryde Andersen 1991b p 125

¹⁶⁵ Bryde Andersen 1991b

¹⁶⁶ See for a total overview Sieber 1991

latter is more based on the question as to whether there is a situation and surroundings as to whether the receiver of the information reasonably might have confidence in it¹⁶⁷. But there are differences, and not all member states has this field sufficiently covered.

If the hurt part is in a contractual situation with the producer or vendor of the software, he might be able to bring an action under the contract law of that jurisdiction. But also this differs between the member states.

Item	Contract	Delictual	Product liability
Goods	Sale of goods or similar legislation	Negligence or other	Yes
Information	Contract for services	some kind of duty of care - differs strongly	No

5.2 Why the Product Liability legislation

"From time immemorial the individual has sought to adapt the world around him to provide tools for the advancement of himself and the society in which he lives.¹⁶⁸" The problem is that this advancements might have undesired effect, they might be harmful - they may cause damage.

¹⁶⁷ Hagstrøm 1989

¹⁶⁸ Saxby 1990 p 221

This undesired effect of innovations is met with product liability. The implication of this new scheme is that a product should be tested so the risk for damages is so small as possible. And to make the producers test the product, they are met with a liability scheme if the product does not properly conform with the expected standard. This is substantiated with the fact that there are economical interests on the part of the producer, who should have the knowledge, to provide new products, and the consumers does not have the same possibilities of knowing what the dangers of (especially) new products are. This might be viewed as the legal response to challenges from the emerging technological innovations in the society.

In the field of information technology this implies that it "will be necessary to introduce higher standards of quality in hardware and software development for all products."¹⁶⁹

The same problem was found in many jurisdiction in the last half of the 19th century when the industrial revolution has come so far as to create new threats. Where the traditional doctrine of negligence or *culpa* has problems adapting to new threats in society.

In Norway this was the period where a strict delictual liability for dangerous machines and plants developed. The first case was a nitroglycerine plant who blew up, and harmed neighbouring property. The traditional scheme of *culpa* seemed insufficient to cope with this problem.

The Product Liability Directive was enacted due to a lack of harmonization in the Community, on this aspect. It should

¹⁶⁹ Saxby 1990 p 227

be mentioned that, however, "the introduction of this EC Directive does not imply full harmonization of the rules on product liability throughout the EC. On the contrary, the national rules on product liability in the member states (which differs substantially) remain fully in force and the Directive merely provides a basis for a gradual more extensive harmonization.¹⁷⁰ But this already existing liability is normally found within the law of tort, based on negligence or *culpa*¹⁷¹.

The balancing of interest between the industry on the one hand and the public on the other hand has resulted in this new liability scheme. It must be emphasized that though the product liability does not involve any negligence, hence is strict - its aim is not to force 100% secure products. It is aiming at a reasonable standard of security.

The concept of Product Liability governs two different types of damages, the first is where the standard of the product is acceptable, but there are some products that passes the production process with defect. The other is where the product as such is defect (in the meaning of the directive). Regarding software, only the latter category will apply, since there is no differences between the different copies of software.

¹⁷⁰ Stuurman 1991 p 191

¹⁷¹ Bryde Andersen 1991a p 429

6 Can software be regarded as *products* as defined in the directive?

After this broad introduction to the problem, having shown the general problems with software, and the reason behind and aim with the Product liability Directive, I will return to the question asked. Does the Directive cover software or not?

The Product Liability Directive governs *products*¹⁷², which is defined as¹⁷³ "all movables, with the exception of primary agricultural products and game, even though incorporated into another moveable or into a immovable ... Product includes electricity."

As already mentioned the relation between the software and the media carrying the software has caused some confusions, also in this fields. To start this discussion, it should be mentioned that argumentations in this direction is found in the legal theory, eg by Reed¹⁷⁴;

... defines "product" as any moveable. It seems likely, therefore, that the Act applies only to software which is marketed on some form of tangible medium (e.g., a tape or disk) ownership of which is transferred to the purchaser. Software which is installed by copying it on to the purchaser's system from a medium that remains the property of the supplier will lack the necessary tangibility to fall within the definition"

¹⁷² Article 1; The producer shall be liable for damage caused by a defect in his product.

¹⁷³ Article 2,

¹⁷⁴ Reed 1993 p 74

This kind of argumentation, however, does not take into account the problem of description, neither does it provide any reasonable results¹⁷⁵. The answer must therefore be found elsewhere, cfr above. It cannot be the intention of the Directive to apply differently depending on the way the software is delivered. See also Bown 1986 p 10:

It is unclear whether the definition of product was intended to include software or not. Clearly it would include software to the extent that it is a product - i.e. the disk or tape *on which the software is stored* would be a product. [my emphasis]

It should also be emphasised that the argumentation of Reed seems to find its starting point in English law, which regarding the Product Liability Directive is an error. The method of interpretation used by English court is *irrelevant* in discussion the extension of the Directive, hence also in discussing UK's obligations arising from that Directive.

Electricity is subject matter for product liability, this has urged some commentators to be taken as an implication that also software should be taken as such¹⁷⁶, but it must be emphasised that there still are severe differences between software and electricity firstly there are a limited number of "defects" inherent in electricity. The most probable defect is that it is not delivered in the right voltage and therefore causes problems. Furthermore, in some jurisdiction the similarity between electricity and movables in some context for the last century has been seen

¹⁷⁵ Which also is admitted by Reid

¹⁷⁶ Hirschback 1989 p 155

as a reason to treat them similarly in some contexts¹⁷⁷, and that this is not to be extended to include software¹⁷⁸

6.1 The media carrying the software

Software is normally delivered in floppy-diskettes, or other media¹⁷⁹ carrying the software¹⁸⁰. This media might be defect. There is no reason that such cases should not fall within the scope of the Product Liability Directive.

This question is probably of less practical interest. It seems less probable that a defect media shall cause damage. Triaille¹⁸¹ uses the example found in the Name of the Rose by Umberto Eco, where poison was applied to the pages of a book, and caused death.

6.2 Software, *per se* a product?

There is no direct answer to this question found in the reasons behind the directive, and the consequences will have to be taken into account. This I will do in a casuistical approach.

¹⁷⁷ the Norwegian Criminal Code s 6

¹⁷⁸ NOU 1992:23 p 67

¹⁷⁹ Such as a CD-ROM.

¹⁸⁰ Though this is not necessary, it may be "delivered" over the telecommunication networks.

¹⁸¹ Triaille 1991

6.3 The consequences of defining software as a subject matter for product liability

As shown above, the consequences of adapting the Directive to Software is a valid argument in the discussion - as to whether it should be adapted or not.

The questions arising in this context is mainly how the rules will be adapted to software - if incorporated. The question arising from this is whether this is a desirable result or not.

6.3.1 Damage - as defined in the Directive

Damage is defined as¹⁸²:

- (a) damage caused by death or personal injuries;
- (b) damage to, or destruction of, any item of property other than the product itself, with a lower threshold of 500 ECU, provided that the item of property;
 - (i) is of a type ordinary intended for private use or consumption, and
 - (ii) was used by the injured person mainly for his own private use or consumption.

This definition is without prejudice to national legislation regarding "non-material" damage¹⁸³.

Section 5, (1) - (4) of the Consumer Protection Act, uses the same definitions as the Directive (though worded differently).

¹⁸² Article 8

¹⁸³ Article 8, 2

There are two alternatives as to when a damage occurs, this will be dealt with in the following (but in the opposite direction of the directive);

Damage to property

It is stated clearly that if damage to property, is to fall within the scope of the directive, the damaged property must be of a type ordinary indented for private use. This implies that the any property that is not normally used for private use falls outside the directive. And also that the property, in question, must have been used for private use. These criteria are cumulative. There is on the other hand no requirement that the damaged product is for the same private use.

Death or personal injury

The other alternative is that the product leads to death or personal injury. Normally it would be rather easy to establish whether this is the case or not.

6.3.2 Different kinds of software

Before starting the discussion on the consequences of the Product Liability Directive on software, it should be mentioned the diversity of software that exist and the different problems they may lead to.

With the multi-purpose machine a modern computer is it seems obvious that many of the applications are incapable of making damage to persons or products. It does not seem likely that a word processing program is capable of killing or injuring somebody or making any physical destruction.

The problems will therefore arise with a limited number of applications. The aim of the casuistical approach, to follow, is to locate the possible cases where software might make damages, as defined in the Directive.

6.3.3 Casuistical approach

In this casuistical approach I will try to define when, if applicable, software might be defective.

It should be borne in mind that the similarities to immaterial products on the one hand and to movables on the other seems to be different depending on whether the software controls some kind of physical output or not. On this distinction it is pointed out that¹⁸⁴:

Prior to today, the written expression of ideas always remained passive until acted upon by human intervention whereas the machine embodiment of functional information remained fixed and ready to perform whatever precise function its mechanical construct ordained. Modern information technology has arguably broken that distinction with computers that can both read data and act upon instructions independently of human control.

Software - not controlling any physical output

If the software is not controlling any physical output it has to be relied upon and acted upon to cause physical damage outside the computer.

¹⁸⁴ Saxby 1990 p 221

It seems that this will fall outside the scope of the Product Liability directive, since the damage is not caused by the product itself but someone acting on it.¹⁸⁵

This has also similarities to traditional printed papers. In this respect it seems to be few differences between the information inherent in a book, a map, a database, a written advice of other kind and a piece of software. It should also be emphasised that the "fault" in such circumstances might appear in the programming logic of the software *or* in the knowledge or factual base in an expert system. In the latter case the similarities are even more obvious.

This seems to differ from the American situation, where there is some case-law that opens for product liability for information, at least in some states. It should though be mentioned that the approach to product liability in USA differs in the different jurisdictions, and that there is no general product liability scheme. For the American situation see Bender 1991.

It seems as if the question of liability might arise in the event that action has been taken on the output of the communication with the computer. If at all this is to be covered by product liability it seems as any liability might be reduced in many cases here. If the output is used as a part of a professional advice, typically from a lawyer or a doctor, the emphasis on his or her lack of care in the professional approach should be an element to reduce liability - if any at all.

An error in the programming structure implies that the output is an incorrect output from the input, because the algorithm is wrong. It might also be the case if the calculations are of other reasons not as

¹⁸⁵ Cfr Bryde Andersen 1991b p 145 ff

expected but the general public. An error in the database, is typically the case with an expert system where there is an error in the knowledge base, hence the program performs the way it should, but the output is wrong due to the parameters in the base.

The only physical damage the program itself can make is if it corrupts the machine on which it is installed. This will typically be the case if there is a virus on the floppy, or the program has some damaging characteristic¹⁸⁶ itself. But in such an event the damage would probably occur at the time of installing the program, and liability might easily be reduced due to the *culpable* action of the injured party¹⁸⁷ if there is no back up taken of the program.¹⁸⁸

Software - controlling a physical output

The problem stressed in this part is when software is controlling a machine, or any other product, that is connected to the computer.

This might easily be observed with medical equipment in a hospital, where some kind of an expert system is controlling the operations of a X-ray machine or a similar device.

In this cases the machine acting upon the output from the software might easily cause injury or even death.

¹⁸⁶ such as is the case with CHKDSK.COM in MS-DOS 5.0, which with the parameter /f under unfortunate circumstances will destroy the hard-disk of the machine

¹⁸⁷ Art 8, 2

¹⁸⁸ But if the damage occurs at a later stage, such as typically will be the case with CHKDSK.COM, this argumentation is not valid

There is also possibilities that the machine might hurt or damage some property, this might easily be the case with cars where the brakes are defect, or a washing-machine that lets the water out on the floor due to some error in the chip.

It could be mentioned that if an error in the software causes a nuclear disaster product liability is not applicable.¹⁸⁹ So if due to an error on the software nuclear missiles are launched or a nuclear vehicle explodes there are not claims arising due to the product liability.

The problems and possibilities for damage seems to be exactly the same if the software is an integrated part of the product.

The distinction between the two categories

It should be mentioned that the distinction between these two categories is not fixed, but to a large extent left open to the discretion of the programmer.

There are still systems that displays output on the screen and leaves it to some operator to give the same instructions to a machine of some kind.

6.3.4 Defect - as defined in the Directive

The Directive states that a defect is present when;¹⁹⁰

A product is defective when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, including;

¹⁸⁹ Art 14

¹⁹⁰ Art 6, 1

- (a) the presentation of the product;
- (b) the use to which it could reasonably be expected that the product would be put;
- (c) the time when the product was put into circulation.

The Directive goes on to state that¹⁹¹ a product "shall not be considered defective for the sole reason that a better product is subsequently put into circulation".

6.3.5 When is software to be regarded as defect in the meaning of the directive?

The problem arising after this casuistical approach as to when and how software might damage live or personal property we should return to the question of when the software might be regarded defect - as defined in the directive.

The general theme is whether the software will "provide the safety ... expect[ed]". The directive does not clearly state whether the starting point is the expectations of totally illiterate parts of society or whether the technical knowledge is to be a part of the evaluation. This is of less interest, though, since the development risk defence, paragraph 6.3.6, will cope with this problem anyway. So the evaluation of what is expected and the state of the art will to some extent fall together. It might in this respect be argued that the public cannot expect more than state of the art.

The special problems in the field of software engineering is that with several thousand programming lines it is not

¹⁹¹ Art 6, 2

possible to foresee all consequences that might arise with the problem. It should also be emphasised that when programming the programmer (or team of programmers) are not always able to foresee all possible inputs to the program - hence not able to foresee the possible output of the same. It is argued that with the state of the art it is not (economically) possible to make a program that is bug-free.

With this as a starting point one might argue that there should be balanced on a model of the possibilities for damage and the value of damages that might occur. So the higher the risk for damage to occur, and the more dangerous the damages might be - the more secure should the software be.

Litra b) might be of some interest in the software field, it states that the use which might reasonably be expected is a part of this argumentation. This seems to have some similarities with the problems of the unknown input to a program. However the use of the program is in most cases rather clear, the unknown input to the program seems not to be a valid argument. It might be an argument if the program has stipulated some fields of use and is used for others. An example might illustrate this problem, a machine for the use in hospitals might be based on standard inputs from adults, and should not be used with children, since the possible inputs that might occur, and the special mathematical calculations that is necessary, is not incorporated into the software.

6.3.6 The development risk defence

The member states have an opportunity of introducing a defence in the case "that the scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered".¹⁹²

The United Kingdom has adapted this defence as section 4, (1) (e), which actually is a interpretation of the Directive on this point. This interpretation is arguable, and is also disputed by the Commission.

Some of the problems arising in the forefront of technology may, due to this, be defended. Typically this calls for the problems inherent in programming - that a program can never be error free¹⁹³, there will always be one or more errors in the program.

It is arguable whether this is a relevant argument in the discussion. To start with the obvious - if the British interpretation of the Directive is correct any error that might not have been found by any other programmer would fall within this defence.

This defence is rather unclear, in s 4 (1) (e) this is defined as:

that the state of scientific and technical knowledge at the relevant time was not such that a producer of products of the same description as the product in question might be expected to have discovered the defect if it had existed in his product while they were under his control

¹⁹² Article 7 (e), cfr Article 15, 1. (b)

¹⁹³ see Hirschback 1989 with further references

If interpreted that it means that if the same defect had occurred in the program of another producer at the relevant time the defect would not have been discovered the implications for software is that any error in the program would fall within this defence. The problem with this wording of the defence is that it presumes that the error is present, and is then referring to the acts of error-checking and control of the program. This is not the relevant state of control, the emphasise in the software context is rather to be on the methods used in programming. This defence seems to be more concerned with the differences in products of a production process, which not is the case with software.

If the legislation had meant to put the emphasise on the state of the art in programming techniques they obviously would have said so. This they have not.

The defence in the directive is rather that the state of the art "was not such as to enable the existence of a defect to be discovered"¹⁹⁴. This emphasises both the programming process as such, the way the programming is organized, and it emphasises the control of the software when programmed.

However, there is a problem inherent in this argumentation as a total. The extent of the development defence risk is from the directive rather unclear. The underlying legislative intention seems to be that any defect that could not possibly be discovered should not be the risk of the producer. It must be remembered that this is an exemption from the general rule, that any defect should be the risk of the producer and that the reasons for this is the general problems producers have in today's society, cfr above.

¹⁹⁴ art 15, 1 (b)

There does not seem to be any general principles in the jurisprudence of the Court as to whether exemptions should be interpreted narrowly or not. But since the risk as a starting point is with the producer, it seems as if it should be a strong underlying reason to move the risk to the injured party. The actual wording of the Directive also seems to be built on this principle.

It must be remembered that for the producer this is a calculated risk or in most practical cases an annual insurance premium. The Directive also seems to be built on the principle that the producer is in a position to insure against this risks, and has a stronger urge to do so, more than the consumers.

6.4 The position of the Commission

As an answer to a question from Euro-MP Gijs de Vries, Lord Cockfield, answered¹⁹⁵:

Under article 2 of [the] directive ... on liability for defect products ... the term product is defined as all movables, with the exception of primary agricultural products - (not having undergone initial processing) - and game, even though incorporated into another moveable or into an immovable. Consequently the directive applies to software in the same way, moreover, that it applies to handicraft and artistic products.

This answer, it must be said, is rather unsatisfactory. The main reason is that does not stress the problems pointed out, neither does the comparison with "handicraft and artistic products" give any indications as to the consequences of the directive.

¹⁹⁵ Official Journal C114/42 8 May 1989

At the same time it could be mentioned that most answers from the Commission to questions from the parliament are rather unsatisfactory. It seems as if the Commission has a reluctance in answering clearly to any question from the Parliament. The reason for this might be found in the fact that the Commission has no power as to the interpretation of directives, this falls within the power of the Court.

6.5 Conclusion

It seems as all commentators¹⁹⁶ are concerned with the uncertainty of the applicability of Product liability to software, I cannot but join these ranks.

When some software, however, is controlling some physical output, this is covered by the Directive, since this should be regarded as a part of the product it is controlling, no matter if the software is incorporated into the product or not.

For the last category, where software is not controlling any physical output but must be relied upon by somebody and acted upon this should fall outside the scope of product liability.

¹⁹⁶ with the possible exception of Reed 1993

Tidligere utgitt i skriftserien CompLex

Alle heftene i skriftserien CompLex kan kjøpes hos, eventuelt bestilles fra Akademika (se kupongen bakerst). De kan også kjøpes fra Norsk forening for jus og edb, Postboks 7557 Skillebekk, 0205 OSLO 2. Her kan man også tegne abonnement eller abonnere på «vaskesedler» som gir en kort omtale av hver rapport etterhvert som de kommer ut, og som inneholder bestillings-seddel. Abonnement på «vaskesedler» er gratis.

CompLex 1/81

Johs Hansen

Et edb-system for analyse av rettslige avgjørelser

64 kr

CompLex 2/81

Johs Hansen (red)

Notater om deontiske systemer

47 kr

CompLex 3/81

Vidar Sørensen

Informasjonssystem mm for Norges Geotekniske Institutt

83 kr

CompLex 4/81

Kjetil Johnsen

Systemtekniske konsekvenser av persondatalovgivningen

111 kr

CompLex 5/81

Marit Thorvaldsen

Teledata og rettsinformasjon

65 kr

CompLex 6/81

Anne Kirsti Brække

Postmonopolet

27 kr

CompLex 7/81

Knut S Selmer (ed)

The LAWDATA Papers

28 kr

CompLex 1/82 Norsk forening for jus og edb & Svenska föreningen för adb och juridik <i>Nordiske personregisterlover.</i> <i>Council of Europe Convention og OECD Guidelines</i>	31,50
CompLex 2/82 Harald Brænd og Vidar Sørensen <i>Oljevern: Brukerbehov og kildemateriale</i>	55 kr
CompLex 3/82 Jon Bing og Dag Frøystad <i>Rettskildebruk</i>	90 kr
CompLex 4/82 Thomas Prebensen Steen <i>Post- og televerkets regulerte ansvar</i>	77 kr
CompLex 5/82 Datatilsynet <i>Årsmelding 1981</i>	44 kr
CompLex 6/82 Birger Eckhoff in cooperation with Jon Bing, Dag Frøystad and Anja Oskamp CATTS: Computerized program for teaching text retrieval systems	61 kr
CompLex 7/82 Jon Bing <i>Informasjonssystemer for Trygderettens kjennelser</i>	126 kr
CompLex 8/82 de Mulder, Oskamp, van der Heyden and Gubby Sentencing by Computer: An Experiment	123 kr
CompLex 9/82 Colin Tapper An Experiment in the Use of Citation Vectors in the Area of Legal Data	56 kr
CompLex 1/83 Arve Føyen <i>Utredning om endringer i pensjonregisterloven</i>	70 kr

CompLex 2/83 Stein Schjøberg Computers and Penal Legislation	140 kr
CompLex 3/83 John S Gulbrandsen og Terje Hoffmann <i>Rettigheter i idrettsarrangementer</i>	64 kr
CompLex 4/83 Sally Moon and Anja Oskamp The Law of Legal Information Systems: Two Essays	95 kr
CompLex 5/83 Datatilsynet <i>Årsmelding 1982</i>	utsolgt
CompLex 6/83 Olav Torvund <i>Betalingsformidling</i>	146 kr
CompLex 7/83 Else Ryen <i>Lov og lovmottaker</i>	103 kr
CompLex 8/83 Daniel Stripinis Probability Theory and Circumsantial Evidence	23 kr
CompLex 9/83 Frede Cappelen <i>Edb-basert informasjonssystem for forvaltningens praksis</i>	36 kr
CompLex 10/83 NORDIPRO Legal Acceptance of international Trade Data	utsolgt
CompLex 11/83 Jørgen Hafstad og Thomas Prebensen Steen <i>Teleksrett og merverdiavgift på programvare</i>	42 kr
CompLex 12/83 Kristin Kjelland-Mørde <i>Om forenkling av regler</i>	utsolgt

CompLex 13/83 Jon Bing <i>Edb: Mulighet og problem ved forenkling av regelverk</i>	92 kr
CompLex 14/83 Tarjei Stensaasen <i>Utvalgte emner i jus og edb (3. utgave)</i>	190 kr
CompLex 15/83 Anette Klafstad og Ulf Alex Samer <i>Plan for et forsikringsrettslig informasjonssystem</i>	60 kr
CompLex 1/84 Jon Erling Skjørshammer <i>Kabelnett: Bygnings- og ekspropriasjonslov</i>	utsolgt
CompLex 2/84 Tore Andreas Hauglie og Dag Wiese Schartum <i>Forslag til et helserettslig informasjonssystem</i>	120 kr
CompLex 3/84 Justisdepartementet <i>Den elektroniske grunnbok</i>	utsolgt
CompLex 4/84 Datatilsynet <i>Årsmelding 1983</i>	utsolgt
CompLex 5/84 Tove Fjeldvig <i>Tekstsøking: Teori, metoder og systemer</i>	90 kr
CompLex 6/84 Jon Bing <i>Offentlighetsloven og edb</i>	94 kr
CompLex 7/84 Gunnar Bach, Beate Jacobsen and Vidar Stensland <i>The National Social Insurance System of Norway</i>	51 kr

CompLex 8/84 Dag Frøystad Data Protection in Practice I: Identifying and Matching Elements	80 kr
CompLex 9/84 Tove Fjeldvig og Anne Golden <i>Automatisk rotlematisering - et lingvistisk hjelpemiddel for tekstsøking</i>	90 kr
CompLex 10/84 Elling Øyehaug Ose <i>Retstidene som informasjonssystem</i>	120 kr
CompLex 1/85 Jon Bing Data Protection in Practise II: International Service Bueraux and Transnational Data Flow	47 kr
CompLex 2/85 Jon Bing <i>Opphavsrett og edb</i>	176 kr
CompLex 3/85 Dag Wiese Schartum Codex, Calculation and Computers	utsolgt
CompLex 4/85 Olav Torvund <i>To informasjonsrettslige arbeider</i>	52 kr
CompLex 5/85 Datatilsynet <i>Årsmelding 1984</i>	utsolgt
CompLex 6/85 Hans Chr Aakre (red) <i>Utvalgte artikler i rettsinformatikk</i>	utsolgt
CompLex 7/85 Johannes Hansen <i>SARA: Brukerveiledning og programdokumentasjon</i>	150 kr

CompLex 8/85 Johannes Hansen Modelling Knowledge, Action, Logic and Norms	90 kr
CompLex 9/85 Thomas Prebensen Steen (red) <i>Kompendium i informasjonsrett</i>	utsolgt
CompLex 10/85 Tarjei Stensaasen <i>Opphavsretslovens § 43 («katalogregelen»)</i>	97 kr
CompLex 11/85 Jon Bing <i>Straffelovens definisjon av «trykt skrift» anvendt på datamaskinbaserte informasjonssystemer</i>	65 kr
CompLex 12/85 Magnus Stray Vyrje <i>Vanhjemmel, opphavsrett og datamaskinprogrammer</i>	161 kr
CompLex 1/86 Anne Kirsti Brække <i>Formidlingsplikt for kabeleier</i>	80 kr
CompLex 2/86 Dag Wiese Schartum <i>Stans av edb-tjenester i krigs- og krisesituasjoner</i>	80 kr
CompLex 3/86 Ingvild Mestad <i>«Elektroniske spor» - nye perspektiv på personvernet</i>	100 kr
CompLex 4/86 Jon Skjørshammer <i>Opphavsrett, databaser og datamaskinprogrammer: Kontraktrettslige aspekter</i>	205 kr
CompLex 5/86 Datatilsynet <i>Årsmelding 1985</i>	73 kr

CompLex 6/86 Johannes Hansen Simulation and automation of legal decisions	132 kr
CompLex 7/86 Stein Schjølborg <i>Datakriminalitet og forsikring</i>	54 kr
CompLex 8/86 Thomas Prebensen Steen (red) <i>Kompendium i informasjonsrett (2.utg)</i>	70 kr
CompLex 9/86 Peter Blume <i>Edb-rettlige foredrag</i>	77 kr
CompLex 1/87 Joseph A Cannataci Privacy and data protection law: International Development and Maltese Perspectives	170 kr
CompLex 2/87 Jon Bing og Jon Bonnevie Høyer <i>Publisering av rettsavgjørelser</i>	170 kr
CompLex 3/87 Hagen Kuehn The Social Security System in the Federal Republic of Germany	77 kr
CompLex 4/87 Hanne Plathe Maartmann <i>Personvern i sykepengereguleringen</i>	70 kr
CompLex 6/87 Jon Bing Electronic Publishing: Data Bases and Computer Programs	55 kr
CompLex 7/87 Ånde Somby <i>Selektiv gjenfinning av bestemmelser i bygningslovgivningen</i>	119 kr

CompLex 8/87 Jon Bing FOKUS: Knowledge based systems for public administration	125 kr
CompLex 9/87 Dag Wiese Schartum The introduction of computers in the Norwegian local insurance offices	230 kr
CompLex 10/87 Knut Kaspersen <i>Kredittopplysning</i>	75 kr
CompLex 11/87 Ernst Buchberger, Bo Göranson and Kristen Nygaard (ed) Artificial Intelligence: Perspectives and Implications	120 kr
CompLex 12/87 Jon Bing, Kristine M Madsen og Kjell Myrland <i>Strafferettslig vern av materielle goder</i>	118 kr
CompLex 13/87 Tove Fjeldvig <i>Effektivisering av tekstsøkesystemer: Utvikling av språkbaserte metoder</i>	175 kr
CompLex 14/87 Jon Bing <i>Journalister, aviser og databaser</i>	66 kr
CompLex 15/87 Andreas Galtung <i>Skatterettslig ekspertsystem: Et eksempel basert på skattelovens § 77</i>	82 kr
CompLex 1/88 Robin Thrapp-Meyer <i>Uvalgte emner i rettsinformatikk (4. utgave)</i>	228 kr

CompLex 2/88 Ernst Buchberger, Bo Göranzon and Kristen Nygaard (ed) Artificial Intelligence: Perspectives of AI as a social technology	178 kr
CompLex 3/88 Jon Bing og Anne Kirsti Brække <i>Satellittfjernsyn</i>	128 kr
CompLex 4/88 Jon Bing Journalists, Databases and Newspapers	68 kr
CompLex 5/88 Joseph Cannataci Liability and responsibility for expert systems	108 kr
CompLex 6/88 Datatilsynet <i>Årsmelding 1987</i>	58 kr
CompLex 7/88 Henrik Sinding-Larsen (ed) Artificial Intelligence and Language Old questions in a new key	290 kr
CompLex 8/88 Jon Bing Database for offentlige publikasjoner (DOP): Fremtidig organisering NORIS (87)	178 kr
CompLex 9/88 Jon Bing Conceptual Text Retrieval NORIS (77)	118 kr
CompLex 10/88 Henning Herrestad <i>Alderstrygden i et nøtteskall, eller skall, skal ikke, en studie av anvendelsen av ekspertsystemskall for PC innen dei juridiske domene</i>	108 kr

CompLex 11/88 Ingvild Mestad L'Informatique, la Liberté Individuelle et la Recherche Epidémiologique Data Protection and Epideminologic Research	98 kr
CompLex 12/88 Johs Hansen SAFE P: Sikring av foretak, edb-anlegg og personverninteresser etter personregisterloven TERESA (50)	178 kr
CompLex 13/88 Henning Herrestad & Dag Syvert Mæsel (red) Five Articles on Artificial Intelligence and Legal Expert Systems NORIS (83) FKUS	108 kr
CompLex 1/89 Dag Wiese Schartum En rettslig undersøkelse av tre edb- systemer i offentlig forvaltning NORIS (85)	178 kr
CompLex 2/89 Datatilsynet Årsmelding 1988	108 kr
CompLex 3/89 Dag Syvert Mæsel og Andreas Galtung XCITE NORIS(91)	238 kr
CompLex 4/89 Robin Thrap-Meyer Pantsettelse av datamaskinprogrammer og databaser TERESA(70)	118 kr
CompLex 5/89 Ellen-Kathrine Thrap-Meyer Forbrukerkjøp og EDB TERESA(58)	178 kr

CompLex 6/89 Andreas Galtung Rettslige aspekter ved miljøinformasjonssystem TERESA(72)	118 kr
CompLex 1/90 Dag Wiese Shartum IRIs SPECTRUM 20 artikler i anledning Institutt for rettsinformatikk 20 års jubileum	298 kr
CompLex 2/90 Finn-Erik Vinje (red.) Språket i lover og annet regelverk	188 kr
CompLex 3/90 Datatilsynets årsmelding 1989	108 kr
CompLex 4/90 Eirik Djønne (red.) Datatilsynet – 10 år som personvernets vokter	108 kr
CompLex 5/90 Rolf Riisnæs (red.) Elektronisk betalingsformidling og forbrukerinteresser I	238 kr
CompLex 6/90 Beate Heidenstrøm Hasseltvedt Rettslige normer og juridiske ekspertsystemer En vurdering av enkelte sider ved TAXMAN	118 kr
CompLex 7/90 Anne Oline Haugen Offentlig informasjon	138 kr
CompLex 8/90 Frank Iversen (red.) Nordisk rettsinformatikk – Foredrag fra Oslo-konferansen 21. og 22. september 1989	228 kr

- CompLex 9/90
Jon Bing
Merverdiavgift og Edb
TERESA (63) NOK 148,-
- CompLex 10/90
Jon Bing
Electronic Copying NOK 98,-
- CompLex 11/90
Karl Fr. Jarbo
Kabelnett i Oslo-området -
Rettslige aspekter NOK 98,-
- CompLex 12/90
Henning Berger Herrestad
Norms and Formalization NOK 158,-
- CompLex 1/91
Marek Sergot
**The Representation of Law in Computer Programs:
A survey and comparison** NOK 138,-
- CompLex 2/91
Jon Bing
The Portuguese Inforjur Project and Related Issues
NORIS (96) III NOK 128,-
- CompLex 3/91
Ola-Kristian Hoff (red.)
20 år med rettsinformatikk – 20 år i forvandlingens tegn
Institutt for rettsinformatikk jubileumsseminar NOK 148,-
- CompLex 4/91
Andreas Galtung
Paperless systems and EDI NOK 198,-
- CompLex 5/91
Rolf Riisnæs (red.)
Elektronisk betalingsformidling og forbrukerinteresser II
Rapport fra den nordiske konferanse 1990 NOK 278,-

- CompLex 6/91
Knut Rognlien
Forutberegnelighet og teknologisk utvikling
som juridiske argumenter
NORIS (89) NOK 198,-
- CompLex 7/91
Morten Daae
Lovdata – Historie, Lov og forskriftssystem NOK 138,-
- CompLex 8/91
Anne Kirsti Brække
Fjernovervåkning og informasjonstjenester
i telenettet
TERESA (83) NOK 238,-
- CompLex 1/92
Beate Hasseltvedt
Avskrivninger av mikrodatamaskiner med tilbehør –
en nordisk studie
TERESA (87) NOK 138,-
- CompLex 2/92
Nils Kr. Einstabland
Kringkastingsbegrepet
TERESA (78) NOK 208,-
- CompLex 3/92
Maria Strøm
Rettskilderegistre i Helsedirektoratet
NORIS (94) I & II NOK 228,-
- CompLex 4/92
Ditlev Schwanenflügel
Softwarepatentet – Imaterialrettens enfant terrible
En redegørelse for patenteringen af softwarerelaterede
opfinnelser i amerikansk og europæisk ret NOK 158,-
- CompLex 5/92
Lars Borchgrevink Grindal
Abonnementskontrakter for kabelfjernsyn
TERESA (78 II) NOK 248,-

CompLex 6/92 Rolf Riisnæs Implementing EDI – a proposal for regulatory form	NOK 118,-
CompLex 7/92 Morten S. Hagedal Deponering av kildekode «escrow»-klausuler TERESA (79)	NOK 128,-
CompLex 8/92 Ola-Kristian Hoff EDB i juridisk undervisning – med en reiserapport fra England og USA	NOK 228,-
CompLex 9/92 Jon Bing og Dag Elgesem Universitetens ansvar for bruk av datanett TERESA (94)	NOK 198,-
CompLex 10/92 Andreas Galtung Rettslige sider ved telenett	NOK 148,-
CompLex 1/93 Giovanni Sartor Artificial Intelligence and Law Legal Philosophy and Legal Theory	NOK 148,-
CompLex 2/93 Connie Smidt Informationsansvaret Erstatningsansvar for informasjonstjenester, særlig ved databasecydelser	NOK 138,-
CompLex 3/93 Ingvild Hanssen-Bauer Personvern i digitale telenett	NOK 178,-
CompLex 4/93 Joachim Benno Consumers Purchases through Telecommunications in Europe - application of private international law to cross-border contractual disputes	NOK 198,-



COMPLEX

Bestillingskupong

Ja takk, vi bestiller herved følgende eks.
av **COMPLEX**:

.....eks. av nr..... à kr

.....eks. av nr..... à kr

.....eks. av nr..... à kr

.....eks. av nr..... à kr

Av fremtidige **COMPLEX** utgivelser (se omtale foregående sider)
bestilles herved:

.....eks. av nr..... à kr

.....eks. av nr..... à kr

Navn:.....

Firma:.....

Adresse:.....

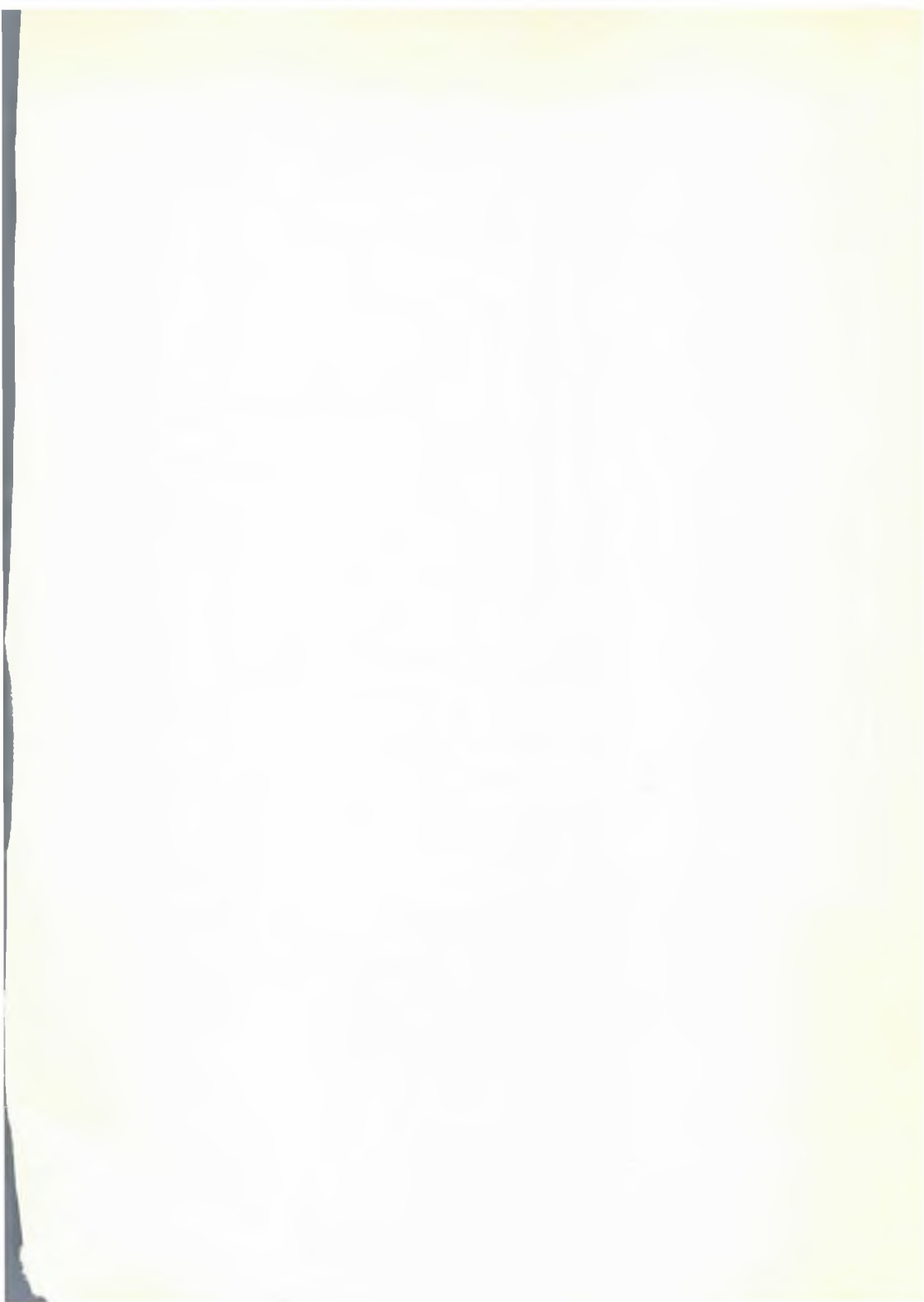
Postnr./sted:.....

Kupongen sendes til:

Akademika
INTERNASIONAL FAGBOERHANDEL

Karl Johansgt. 47
0162 Oslo 1









These four essays are all within the traditional field of computer and information technology law. They were initially written as a part of the authors LLM in Computer and Information Technology Law at University of Strathclyde.

The essay on *intellectual property right* is concerned with the interaction between (especially) copyright and the competition law of the EC. In the question of antagonism or peaceful cooperation the author is arguing that there is a peaceful cooperation in the field.

The essay on *privacy and data protection* deals with the underlying problems and the need for data protection. To some extent the European dimension is discussed.

The essay on *information crime* has its starting point in the problems with applying traditional (or existing) criminal offenses to information. The problems inherent in the fact that information, *per se*, as not an "ordinary" moveable is a major part of the discussion. A brief discussion *de lege lata* and *de lege ferenda* on the problems of theft of information is also included.

The final essay on *liability* deals with the problem of software and the Product liability directive. The question of whether software is subject matter of product liability is unfortunately unclear.



ISBN 82-518-3198-9

